# Journal Pre-proof


Survey on blockchain based smart contracts: Applications, opportunities and challenges

Tharaka Hewa, Mika Ylianttila, Madhusanka Liyanage

PII: S1084-8045(20)30323-4

DOI: https://doi.org/10.1016/j.jnca.2020.102857

Reference: YJNCA 102857

To appear in: *Journal of Network and Computer Applications*

Received Date: 20 February 2020

Revised Date: 11 August 2020

Accepted Date: 20 September 2020

Please cite this article as: Hewa, T., Ylianttila, M., Liyanage, M., Survey on blockchain based smart contracts: Applications, opportunities and challenges, *Journal of Network and Computer Applications* (2020), doi: https://doi.org/10.1016/j.jnca.2020.102857.

# Survey on Blockchain based Smart Contracts: Applications, Opportunities and Challenges

Tharaka Hewa

*Centre for Wireless Communications, University of Oulu, Finland*

Mika Ylianttila

*Centre for Wireless Communications, University of Oulu, Finland*

Madhusanka Liyanage

*School of Computer Science, University College Dublin, Ireland*

*Centre for Wireless Communications, University of Oulu, Finland*



**Abstract**

Blockchain is one of the disruptive technical innovation in the recent computing paradigm. Many applications already notoriously hard and complex are fortunate to ameliorate the service with the blessings of blockchain and smart contracts. The decentralized and autonomous execution with in-built transparency of blockchain based smart contracts revolutionize most of the applications with optimum and effective functionality. The paper explores the significant applications which already benefited from the smart contracts. We also highlight the future potential of the blockchain based smart contracts in these applications perspective.

*Keywords:* Blockchain, Smart Contracts, Applications, DLT, Hyperledger Fabric, Ethereum, Corda, Stellar

## 1. Introduction

The blockchain is a decentralized, distributed and immutable ledger comprised of a cryptographically linked chain of record collection. The collection of records referred as blocks and the records called transactions or events. The decentralized ledger is shared within all contributory members in the blockchain network. These transactions add to the ledger upon verification and agreement process between the parties on-board in the blockchain. The important features associated with blockchain are the **decentralization, immutability and cryptographic link.**

**Decentralization:**The decentralization of blockchain delegate the authority among the contributors of the network. It is a distinction of the blockchain which ensure redundancy in contrast with the centralized systems operated by a trusted third party. The decentralization ensures the service availability, reduce the risk of failure and eventually improve the trust of service with guaranteed availability.

**Immutability:** The records of transactions in the ledger, which remain distributed between the nodes are permanent and unalterable. The immutability is a distinguishing feature of the blockchain from the centralized database systems which elevates to the next level for the integrity of data on the ledger. The records are computationally tamper resistant with the existence of the cryptographic links.

**Cryptographic Link:** The cryptographic link between each record sorted in the chronological order and the block builds the chain of integrity in the entire blockchain. The digital signature verifies the integrity of each record using hashing techniques and asymmetric key cryptography. The alteration of block or transaction record violate the integrity and eventually make the record and block invalid.

In addition, cryptocurrencies enable seamless peer to peer payments and proliferate the financial context accentuating as the first generation of blockchain to the world. Cryptocurrencies are virtual and digital currencies secured with digital signatures. Bitcoin [1] is the first prominent cryptocurrency in the world which enables the peer-to-peer financial transactions without the intervention of trusted third party such as international payment channels. The system operates without a third party and the transactions committed to the network are verified by dedicated nodes called miners using the cryptographic techniques.

### *1.1. Significance of Blockchain based Smart Contracts*

Smart contracts are self-enforcing and self-executing programs which actuate the terms and conditions of a particular agreement or contract using software codes and computational infrastructure. Buterin et al. [2] instigated the concept of smarts contract emphasizing the key features with the inaugural deployment in the financial industry. The smart contracts are an

*Email addresses:* tharaka.hewa@oulu.fi (Tharaka Hewa), mika.ylianttila@oulu.fi (Mika Ylianttila), madhusanka@ucd.ie (Madhusanka Liyanage)

Table 1: Summary of Important Acronyms

| Acronym | Definition |
|---|---|
| 3D | 3 Dimensional |
| 5G | 5th Generation |
| ADS-B | Automatic Dependent Surveillance – Broadcast |
| AI | Artificial Intelligence |
| AIRA | Autonomous Intelligent Robot Agent |
| API | Application Programming Interface |
| AU | Application Unit |
| BFT | Byzantine Fault Tolerance |
| BTO | Basic Timestamp Ordering |
| CA | Certification Authority |
| CBRS | Citizens Broadband Radio Services |
| COAP | COnstrained Application Protocol |
| CVV | Card Verification Value |
| DAML | Digital Asset Modeling Language |
| dApp | Distributed Applications |
| DDOS | Distributed Denial of Service |
| DEX | Decentralized Exchange |
| DLT | Distributed Ledger Technology |
| eGovernment | Electronic Government |
| ERC | Ethereum Request for Comment |
| FAO | Food and Agricultural Organization |
| FSM | Finite State Machine |
| EV | Electric Vehicle |
| EVM | Ethereum Virtual Machine |
| FBI | Federal Bureau of Investigation |
| GDPR | General Data Protection Regulation |
| HIPAA | Health and Information Privacy and Portability Act |
| HDG | Health Data Gateway |
| HSM | Hardware Security Module |
| IAM | Identity and Access Management |
| ICO | Initial Coin Offering |
| IoT | Internet of Things |
| IT | Information Technology |
| KYC | Know Your Customer |
| LDAP | Lightweight Directory Access Protocol |
| LORA | LOng RAnge |
| MAC | Medium Access Control |
| ML | Machine Learning |
| MNO | Mobile Network Operator |
| NFT | Non Fungiable Token |
| OBU | On Boarding Unit |
| PBFT | Practical Byzantine Fault Tolerent |
| PA-DSS | Payment Application-Data Security Standards |
| PCI-DSS | Payment Card Industry-Data Security Standards |
| PKI | Public Key Infrastructure |
| PoS | Proof of Stake |
| STM | Software Transactional Memory |
| UAV | Unmanned Aerial Vehicles |
| VR | Virtual Reality |
| UTXO | Unspent Transaction Output |
| WAN | Wide Area Network |
| WBAN | Wireless Body Area Network |

extension of the utilization of distributed ledger. The smart contract operates as decentralized programs on the blockchain network. The program is immutable and cryptographically verified the immutability to ensure the trust of the program. The key features of the smart contracts are execution in peer to peer mode without the intervention of a centralized third party and service availability without any centralized dependency. The autonomous execution aligned to the predefined conditions makes the contracts smart rather than paper condition.

The smart contracts' features enable the pertinence of them to diverse domains. Many of such features inherited from the underlying blockchain technology. The key features of blockchain based smart contracts can be categorized as follows.

#### *1.1.1. **Elimination of Trusted Third Party***

The blockchain is capable to operating in collaboration with decentralized nodes. The smart contracts enable autonomous execution within predefined conditions. These are the key features to resolve most of the limitations in centralized applications. The decentralization eradicates the single point of failure which ensures the ceaseless service availability. The decentralization also eliminates the extensive data consumption and latency in operations when comparing with the round trip requests of the centralized systems. The decentralization provides transparency in the computational logic eliminating the centralized "Black Box" concept transferring the accountability to all the members.

#### *1.1.2. **Forge Resistance***

The integrity of each transaction and block in the distributed ledger verified with the digital signatures. The forge resistance is a key distinguishing feature which augments the value of blockchain. The transaction record and the computational logic of execution are cryptographically verified and remain persistently over the network.

#### *1.1.3. **Transparency***

Transaction transparency is another significant benefit of blockchain based smart contracts. The blockchain ledger and smart contract logic is visible to all parties in the blockchain ecosystem. The transparency is a differentiating feature of the blockchain which makes it lucrative among the centralized databases.

#### *1.1.4. **Autonomous Execution***

The programmed condition and flow of events defined to accomplished execute once the blockchain system reached to the triggering state. The triggering state can be defined in the smart contract upon agreement of all parties in the blockchain network. It can be any condition such as reduced funds, a node reaches a particular geographical location or the system receives a payment. The significant feature is that the execution is automatic and triggered on a condition of the peer without intervening a centralized third party. The service availability is guaranteed since the operation does not rely on a centralized third party.

#### 1.1.5. ***Accuracy***

The programmed conditions in the smart contracts are immutable and verified prior to the deployment in nodes in the blockchain network. The execution is automatic once the condition is met. The accuracy is guaranteed without any human or any other error on the execution. The autonomous accurate execution eliminates the biased operation and improves the trust through transparent accurate execution.

### *1.2. Paper Motivation*

The smart contracts facilitate the enforcement of contractual agreements with in-built transparency and forge resistance. The distinguishing features of smart contracts make it pertinent into many applications. A lot of research conducted in the industry as well as academia in order to investigate the strengths and applicability of smart contracts in different application domains. Furthermore, the improvements of technical aspects highly focused to fine tune the smart contracts for the enhancement of compatibility of the smart contracts. There are many smart contract platforms emerging in the market with associated distinguishing features which suits for specific applications.

Wang et al.[3] provided a comprehensive overview of blockchain-powered smart contracts spotting the distinguished challenges in the smart contracts along with future trends. Wright et al. [4] presented the benefits and drawbacks of the emerging decentralized technology and its requirement to the expansion of a new subset of law that termed as Lex Cryptographia and highlighted the requirement of the regulation of blockchain-based smart contract based organizations under legal theory. Udokwu et al. [5] provided a systematic review of previous studies such as frameworks, simulations, methods and working prototypes that demonstrated the application of smart contracts in the organization along with the main anticipations of smart contracts in the enterprise including the establishment of the trust. Seijas et al. [6] provided a high-level overview of the scripting languages utilized in the existing cryptocurrencies and smart contract platforms including Ethereum, Bitcoin and Nxt highlighting the strengths and weaknesses.

Aggrawal et al. [7] presented a comprehensive in-depth analysis in the smart community context with a comparative analysis with existing survey. Wüst et al. [8] critically analyzed the applicability of blockchain for a particular application scenario proposing a structured methodology to determine the relevant technical solutions and evaluated with some significant real-world applications. Clack et al. [9] explored the design landscape of potential formats for storage and transmission of smart legal agreements in association with blockchain technology specifically for the financial services context. Chen et al. [10] modeled smart contract execution over a decentralized network over an agent-based framework and introduced novel concepts including penalties and incentives to the agent-based model. Sousa et al. [11] proposed a Byzantine Fault-Tolerant (BFT) ordering service for ordering verified transactions in the Hyperledger Fabric with a novel consensus approach with successful results yielded. Xu et al.[12] proposed a classification method and compared blockchain and blockchain-based systems to assist with the design and assessment of their impact on software architecture. The significant design patterns of the blockchain also discussed in the paper. Marino et al. [13] developed a set of standards that enabled the smart contracts to alter or undo a contract made and conveyed its significance with applying on Ethereum smart contracts platform.

Norta et al. [14] illustrated the existing problems associated with non-machine readable classical contracts entirely based on trust. Luu et al. [15] proposed SMARTPOOL which is a novel protocol design for a decentralized mining pool. The authors implemented and deployed SMARTPOOL on Ethereum and Ethereum classic networks with constructive experimental results. Dai et al. [16] proposed Qtum-framework for a novel smart contract and blockchain-technology solution which uses Proof-of-Stake (PoS) validation. The framework aligned to the Unspent Transaction Output (UTXO) model which used in BitCoin. In contrast with Ethereum's account-based model since they highlighted that Ethereum's account-based model has scalability limitations.

Macrinici et al. [17] presented the problems and corresponding solutions in a broader perspective along with the research trends relevant to the blockchain based smart contract context and highlighted that the immature state of smart contracts. The authors also itemized the security, privacy, scalability, and programmability of the smart contracts highly focused in the conducted research previously. Zheng et al. [18] presented a survey on challenges and opportunities in blockchain. He et al. [19] presented survey on blockchain technology and its application prospect. Sankar et al. [20] focused on analyzing consensus protocols proposed with their feasibility and efficiency in the properties they proposed to facilitate for the significant blockchain platforms like Hyperledger Fabric, Stellar and R3 Corda. Singh et al. [21] presented the significance of the concept of sidechain, with a review upon examination, which has a future potential in blockchain context.

### *1.3. Our contribution*

The best of our knowledge, there is no single survey which considered the application of blockchain based smart contracts in broader and deeper perspective. Thus, this survey conduct with a deep focus on the applications of blockchain based smart contracts. The contribution of the survey include,

- **Background of blockchain based smart contracts** : An informative overview on the blockchain based smart contracts highlighting the core principles utilized in the blockchain.
- **Importance of blockchain based smart contracts**: The key features of blockchain based smart contracts which distinguish blockchain based architecture.
- **Overview on significant blockchain platforms**: The well known blockchain platforms with their key features discussed along with the real world applications.
- **Application domains of blockchain based smart contracts**: A broad illustration on each application domains of blockchain based smart contracts with related works, which is the core content of the survey.

Table 2: Previous Surveys on Smart Contracts

| Ref | Description | Comparison with our contribution |
|---|---|---|
| [17] | **Smart contract applications within blockchain technology: A systematic mapping study**: A systematic study which presents problems, corresponding solutions, and the research trends including numerical figures in a broader perspective. | Discussed the smart contracts and their role in concrete application perspective, identifying the application specific insights. |
| [22] | **An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns**: The usage of smart contracts analyzed on different platforms. There were 834 smart contracts analyzed by categorizing into their application domain. | The role of smart contracts analyzed distinguishing by the application domains. |
| [23] | **A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT**:A broad and comprehensive discussion on the blockchain solutions in the IoT and IIoT security context. | We discussed the smart contracts in the application perspective. |
| [24] | **A Survey on Privacy Protection in Blockchain System**: A comprehensive survey on the privacy protection including identity management. | We discussed the smart contracts mostly focusing in the applicability. |
| [25] | **Applications of Distributed Ledger Technologies to the Internet of Things: A Survey**: The applicability of smart contracts in different contexts along with IoT discussed including the challenges and future research issues. | We considered application contexts not limited to the IoT intervention. |
| [26] | **A Survey of Blockchain Applications in Different Domains** : An informative and brief high level survey on the blockchain for different application contexts including financial and healtchare. | We focused in detailed into the different sub contexts on each application and the associated issues with significant number of related works. |
| [27] | **Blockchain: A Survey on Functions, Applications and Open Issues**:Presents an analysis of blockchain and their applications along with different open issues. | We focused deeply on the application of blockchain. |
| [28] | **Blockchain and Its Applications – A Detailed Survey** : A high level discussion on blockchain and its applicability on different contexts. | We discussed in detail on the each application context. |

- **Technical challenges and solutions of smart contracts**: A high-level review on the significant challenges of smart contracts when they are applying to the real world use cases. Furthermore, a review on the corresponding solutions included as an elaboration.

- **Lessons learned and future works**: The insights of current applications and the future improvements required to address the existing issues of them discussed.

- **Future applications**: The application domains which have a potential in applicability of blockchain based smart contracts in future.

### *1.4. Outline of the Paper*

The rest of the paper is organized as follows. Section 2 provides a brief introduction to the paper with background information applicable to the smart contracts. The important acronyms with the definitions included in Table 1. A summary of important surveys related to the paper presented in Table 2. Table 3 projects the smart contract platforms with pointers to applications of current use. The different application contexts discussed in the Section 3. The Section 4 includes a review on the key technical challenges encountered in the smart contracts. The Section 5 discusses the lessons learned and future work. Section 6 concludes the survey.

## 2. Different Smart Contract Platforms and Their Applications

Smart contracts can transform the business rules into the computer programs. Different smart contract platforms have developed to address specific requirements in each industry. Each smart contract platform includes a set of specific features targeted to the particular application. For an instance, Ethereum is mainly developed for the applications which require tokenization. Almost all platforms contain the basic features of a smart contract system including the immutable program code, the decentralized ledger, and the consensus layer. Figure 1 reflects a few leading smart contract platforms. Table 3 summarizes the main application contexts and related works. Table 4 includes a relative comparison of the features of each smart contract platform.

### *2.1. Ethereum*

Ethereum [47] is defined as a distributed computing platform which is composed of a network of computers operating in a de-

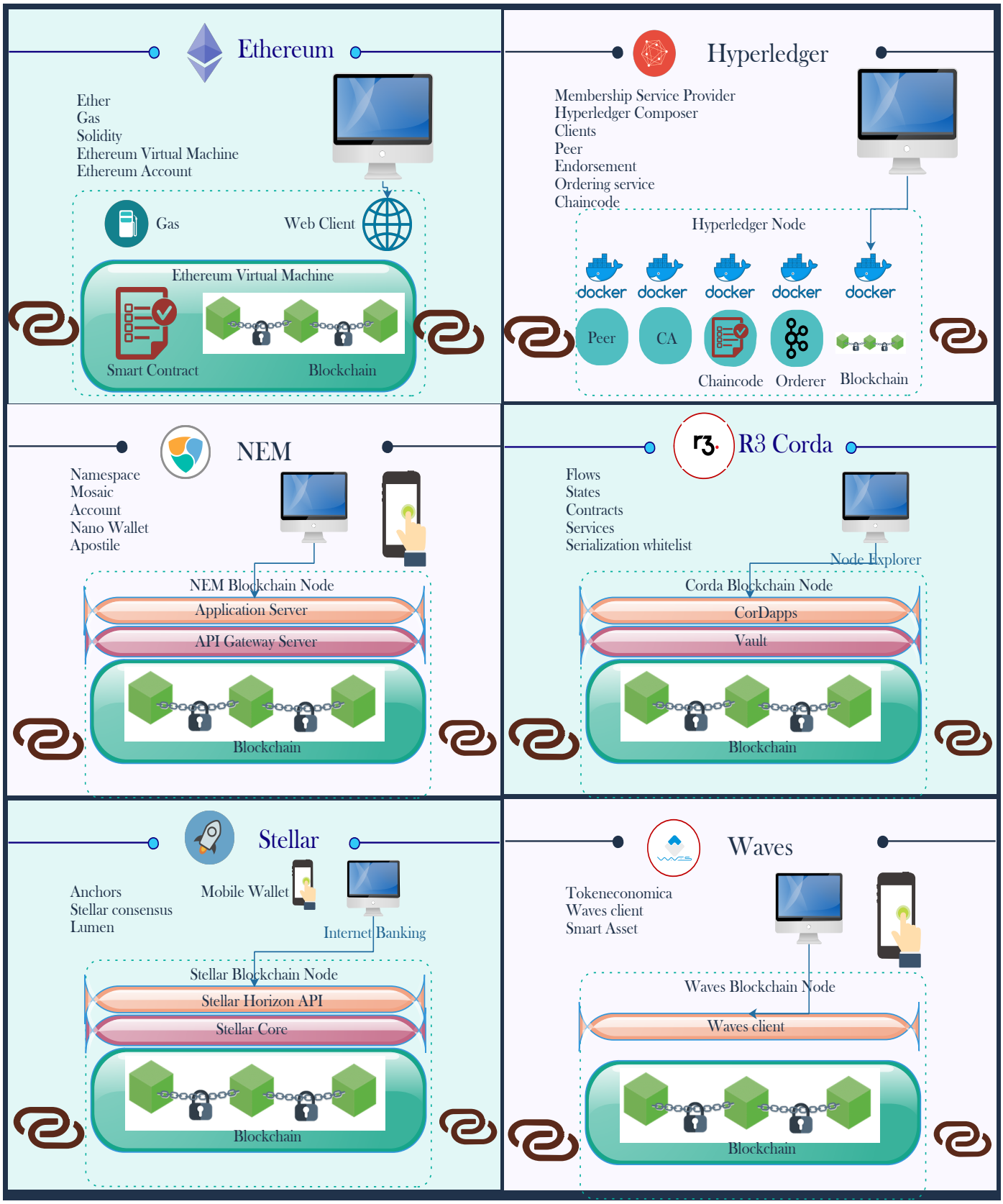


Figure 1: Important smart contract platforms

Table 3: Smart Contract Platforms and their Applications

| Platform | Main Application Contexts | Related Works |
|---|---|---|
| Ethereum | • Financial<br>• Asset trading | • DAI [29]<br>• Gitcoin [30]<br>• Cryptokitties [31] |
| Hyperledger Fabric | • Supply chain<br>• Trade finance<br>• Stock trading | • IBM Food Trust [32]<br>• Everledger diamond blockchain [33] |
| Corda | • Energy trading<br>• Insurance<br>• Retail markets | • Energy Block Exchange [34]<br>• TradeCloud[35]<br>• MonetaGo[36] |
| NEM | • Augmented reality<br>• Advertising and marketing<br>• Banking<br>• Gaming<br>• Music and entertainment | • DigitCoin[37]<br>• Bankera[38]<br>• Pantos[39]<br>• Verses[40] |
| Stellar | • Remittance | • StellarX[41]<br>• Tempo[42]<br>• TillBilly[43] |
| Waves | • Customized asset trading<br>• Ride sharing | • TokenEconomica[44]<br>• TradiSys[45]<br>• Multi Chain Ventures[46] |



centralized, self-governing and democratic manner. Ethereum executes smart contracts and deploys decentralized applications which is called dApp. The front-end can be deployed as web application with associated backend as a solidity smart contract. Ethereum uses token such as ERC-20 and ERC-721 to operate with the smart contracts. Ethereum Gas is the unit to measure the computational overheads in the smart contract execution. Gas cost is the monetary value to be spent by the user for a smart contract execution. Gas limit is the maximum price which is the blockchain platform user willing to pay for the smart contract execution.

*2.1.1. Advantages*

- **Open source system**: The governing body of Ethereum does not charge for the source codes. The source codes available publicly and open for the contribution of developers around the world.
- **A worldwide developer community in contribution**: Huge community of developers contribute to the evolution of Ethereum. The issues and improvements can be publicly handled with the involvement of different developers worldwide.
- **Availability in private and public mode**: The Quorum is the private mode of Ethereum blockchain. The users have the capability to decide the operational mode of blockchain as per their requirements.
- **Availability of native cryptocurrency** : The native cryptocurrency Ether is available to trade as well as incentivize the members as per the different requirements.

*2.1.2. Disadvantages*

- **Public ledger storage overheads** : The public ledger is expected to download when a member node required to connect the network. However, the storage is growing continuously which incur some overheads in the storage for the member nodes.

- **Transaction approval time :** The transaction approval time varies from seconds to minutes which will be not supportive to the realtime requirements of transaction processing. For an instance, the retail payments are hard to accept using the Ethereum due to the transaction time.
- **Transaction cost**: The computational overheads of smart contract execution determined as the gas cost. The gas cost eventually incur financial overheads to the members in the network.
- **Single programming language support**: The programming language of the smart contract limits to Solidity, which is mostly similar to Javascript. The single programming language restricts the experts of other programming languages.
- **Integration limitations**:The integration support of the Ethereum yet to be further evolved with different application contexts such as IoT.

### *2.2. Hyperledger Fabric*

Hyperledger Fabric is a permissioned blockchain platform which is designed for the enterprise-grade usage. Hyperledger Fabric was adopted to a micro-service based architecture for convenient deployment. The ledger developed on top of CouchDB no-sql database. The smart contract called ChainCode in Hyperledger terminology can develope using Java, NodeJs and GoLang programming languages. The microservices of a Hyperledger blockchain network includes peer, Certification Authority (CA) , CouchDB, orderer, and chaincode. Each microservice deployed as a docker container. They are interconnected using remote procedure calls. Hyperledger presents an array of specialized versions and utilzation tools for the blockchain platform. Hyperledger Fabric, Hyperledger Indy, and Hyperledger Sawtooth are the significant examples. Each version has developed with specialization in different contexts.

#### *2.2.1. Advantages*

- **Permissioned operational capability**: The permissioned operational capability provides a flexibility of the stakeholders to select which nodes to be operated, scope of ledger, and improved privacy. In contrast, the public blockchain platforms like Ethereum add transactions to the public ledger to make them publicly accessible which will raise privacy flaws.
- **Different modes of consensus (Solo, RAFT, Kafka)**: The Hyperledger provides different consensus mechanism integration capability which provides the flexibility to the users. The public blockchain frameworks such as Ethereum do not support custom consensus mechanisms as it will require to customize other member nodes.
- **No transaction costs**: There are no transaction costs for the Hyperledger blockchain. In contrast with public blockchain such as Ethereum, the transactions will not charge from the members as the blockchain will be deployed on the members' infrastructure.
- **Different programming language support (Java, JS, Go):** The Hyperledger provides SDK for a flexible integration in different applications.
- **Microservice adopted architecture:** The microservice architecture provides simplicity and flexibility with the containerization. The containerization provides convenience in the version controlling and other related operations. In contrast, the public blockchain networks are hard to upgrade upon identification of the software issues.
- **Rich queries in the ledger**: The transaction data stored in the CouchDB database. The ledger inherits a rich querying capability from the CouchDB.

#### *2.2.2. Disadvantages*

- **No native cryptocurrency**: There is no native cryptocurrency in the Hyperledger blockchain platform. If it is required, the cryptocurrency should be developed by the smart contracts.
- **Complexity in deployment** : The deployement of blockchain platform is relatively complicated in contrast to the platforms like Ethereum.
- **Number of proven usecases are relatively low**: The Hyperledger blockchain platform is still evolving by addressing different requirements.

### *2.3. Corda*

R3 Corda is a permissioned blockchain platform which can utilize to deploy legalized contracts with privacy preservation. The transactions of Corda platform performed in a legally enforceable manner. The platform is used in a vast variety of applications such as financial, healthcare and so on. The flows, which are the sequences of steps leading to a ledger update define the execution routing of the smart contract.The state of the R3 Corda platform represents the smart contract which corresponds to the real world contracts.

#### *2.3.1. Advantages*

- **Extended privacy prservation**: Corda was initially designed to cater the banking industry. The concept of notaries was intended to be operated by the banks. In contrast with the Ethereum, the notaries are the miners who verify the transactions.
- **A broad industrial compatibility**: Corda supports for different industrial applications with capability to enforce ordinary contracts as smart contracts.
- **Regulatory and supervisory node support**: Corda supports regulatory and supervisory nodes to align with the existing banking ecosystems.

- **Realistic contractual enforcement capability**: The corda is convenient for the enforcement of business logic as the smart contract. The platforms
- **Different consensus mechanism support**: Corda supports pluggable consensus mechanisms to enhance the flexibility of operations. The consensus mechanism of Corda is twofold, as transaction validity consensus and transaction uniquness consensus.

*2.3.2. Disadvantages*

- **No native cryptocurrency**: There is no native cryptocurrency included in Corda.
- **Verification only through trusted notaries**: The trusted notary service aligns the Corda system with the financial services requirements. It can be argued that notaries may drive the system towards trusted third party features, which is expected to be eliminated in blockchain principle.

*2.4. NEM*

The NEM is a blockchain-based cryptocurrency platform which is associated with significant value-added features. NEM has the extra capabilities such as identity proof, timestamping documents, and creation of customized digital assets. The NEM has strong potential to use in industrial applications when comparing with other cryptocurrencies. There are many potential usecases with NEM beyond peer-to-peer value transfer.

*2.4.1. Advantages*

- **Built in cryptocurrency**: The NEM has its own cryptocurrency XEM which can be used as an asset, like Ethereum.
- **High transaction throughput**: The transaction throughput of NEM is relatively higher than Ethereum and Hyperledger.
- **Improved Proof of Importance consensus algorithm**: The consensus algorithm Proof of Importance is encouraging the participants buy cryptocoins and remain active fort the contribution.
- **Delegated harvesting usage**: Delegated harvesting enables more members to contribute for the functioning of network

*2.4.2. Disadvantages*

- **Limitations of the documentation**: The documentation and other materials for the NEM blockchain are relatively low when compared with Hyperledger and Ethereum.
- **Comparably less number of tools available**: The number of tools for the NEM blockchain is relatively low when compared with the other platforms like Hyperledger Fabric. The Hyperledger platform provides a vast array of tools such as Hyperledger composer to easily created blockchain solutions.
- **Lacking of community contribution**:The developer community of the NEM is relatively low when comparing with the leading platforms like Ethereum and Hyperledger.

*2.5. Stellar*

Stellar is a blockchain platform that enables financial transactions beyond frontiers. The Stellar platform provides faster transaction processing time compared with other cryptocurrency platforms. The native cryptocurrency of Stellar is called Lumen. The transaction processing time in association with the concept called Anchors is always less than 5 seconds. The invention utilized the Stellar consensus based on the Ripple consensus algorithm. Even though the smart contract programming language is not Turing complete, the smart contracts can be used to multi-signature transactions and future executions. Turing completeness limitation was explicitly imposed in order to mitigate the security risks of Turing complete programming languages.

*2.5.1. Advantages*

- **Cryptocurrency support** : Stellar has its own cryptocurrency called Lumen which supports the different operations
- **Pre-generated cryptocurrency** : Stellar Lumens are pregenerated. Hence, there is no computataional overhead for mining, such as Bitcoin which will be more beneficial for the users
- **Faster transaction processing time**: The transaction confirmation time is 3-5 seconds, which makes it easy to integrate for retail payments
- **Enhanced security through non-Turing complete smart contract language** : The capabilities of the non-Turing complete smart contracts are limited.

*2.5.2. Disadvantages*

- **Integration issues with the existing banking systems**: The Stellar originally intended to use for the financial transactions. There are difficulties with the integration of blockchain with the existing systems such as SWIFT.
- **Regulatory difficulties with the legal frameworks**: Since the blockchain is still not evolved technology, there are some regulatory limitations as most of the legal systems do not define blockchain based transactions.

*2.6. Waves*

The Waves smart contract platform is a Scala programming language based open-source blockchain platform. It allows users to launch their own cryptocurrency token and facilitates with Decentralized EXchange (DEX). They have introduced the concept of custom application tokens, which is tailor-made for the user requirement. The platform enables users to create, issue, transfer assets, and exchange custom tokens within 5 minutes. The smart contract language used in Waves platform is a non-Turing complete language.

Table 4: Smart contract platforms relative comparison

| Features | Ethereum | Hyperledger Fabric | Corda | NEM | Stellar | Waves |
|---|---|---|---|---|---|---|
| **Operation mode** | Public | Private | Private | Public | Public | Public |
| **Smart contract programming language** | Javascript | Javascript Java/Go | Cotlin/Java | Custom | Custom | Custom |
| **Consensus mechanism** | PoW | Pluggable | Raft | Proof of Importance | Stellar consensus | Leased PoS |
| **Latency (Confirmation time)**[48], [49], [50], [51] | 15min | 1 second | Not published | 1-2 min | 1-5seconds | 10 min |
| **Throughput** [52], [53], [54], [55], [56] | 20tps | 20,000 tps | 15-1,678 tps | 4,000 tps | 1,000 tps | 500 tps |
| **Native cryptocurrency** | Ether | None | Corda coin | XEM | Lumens | Waves |
| **Smart contract Turing completeness** | Turing complete | Turing complete | Turing complete | Turing incomplete | Turing incomplete | Turing incomplete and basic functional smart contracts |
| **Transaction privacy** [57], [58] | No privacy on public ledger | Privacy through channels | Privacy through techniques such as partial data visibility | No privacy on public ledgers | No privacy techniques | Provides confidential data transfer and storage |

#### *2.6.1. Advantages*

- **Custom token creation capablity**: The capability to create custom wallets simplify the tokenization market to the new entrants. In contrast with the platforms such as Ethereum, the custom token creation is a distinguishing benefit of Waves.

- **Non-Turing complete language for better security** : The Non-Turing complete smart contract language limits the risk of utilization of smart contracts for attacks.

#### *2.6.2. Disadvantages*

- **Exposed to volatility in the monetary system through custom tokens**: The concept of custom tokens may create an artificial volatilty in the market.

## 3. Applications of Smart Contracts

The key application areas and the role of smart contracts are presented in this section. Figure 2 illustrates a quick overview of different smart contract based applications.

### *3.1. Financial Applications*

The self-executory, immutable, and distributed nature of the smart contracts revamp the financial industry in a few dimensions by solving many existing issues. Smart contracts guarantee the defined operation to be executed on a certain state of the system and it will be executed without any error. The competitive advantages of the blockchain-based smart contracts for the financial companies are highlighted in [59]. Figure 3 reflects these benefits of the smart contracts in the financial applications. Moreover, Table 5 summarizes the key challenges related to each financial applications and benefits of smart contracts to resolve them.

#### *3.1.1. **Currency management***

Currency is one of the most important elements in the financial industry. Currencies which are declared by a legal tender and controlled by a national central bank are called Fiat currencies. United State Dollars and Euro are well-known examples. Usage of Fiat currencies incurs the stakeholders a lot of overheads such as storage and transportation with high level of security. In the consumer's perspective, the centralized link with the central bank in fiat currency exposes the financial strength of each individual to the government. The government or bank can reverse a committed transaction without consumer's consent too. In addition to that, identity theft has become a major

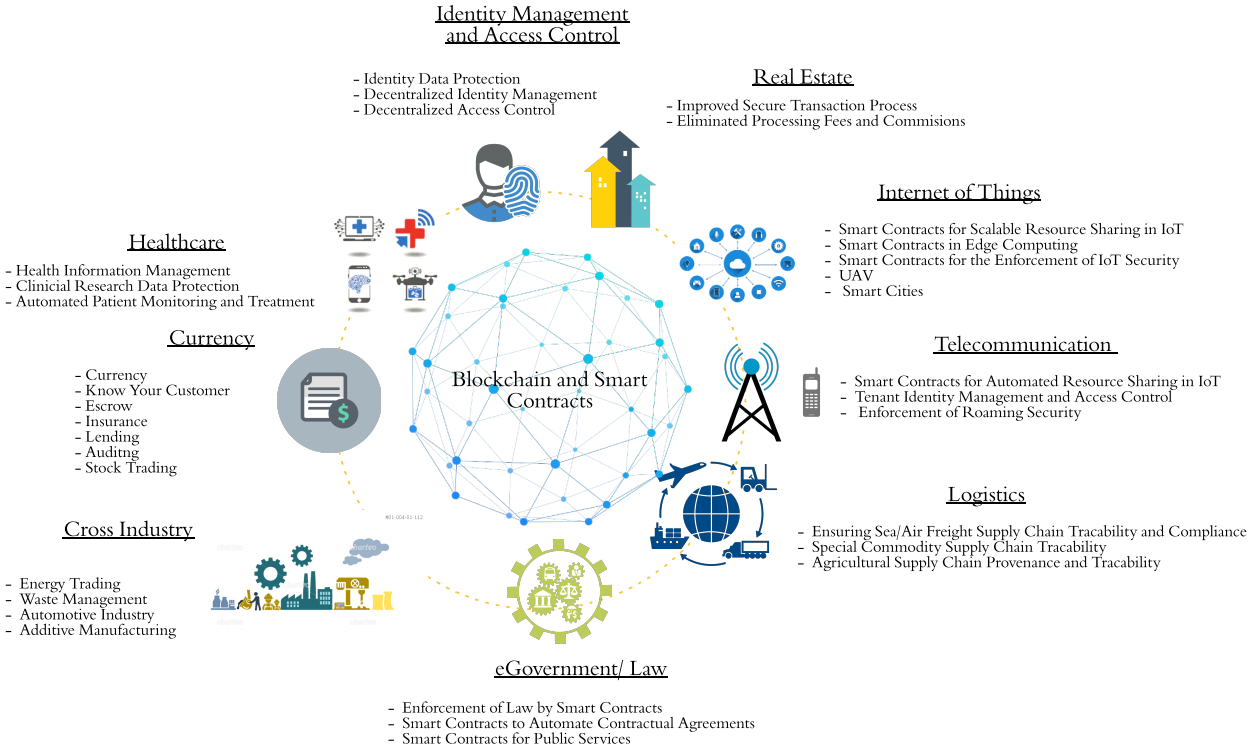


Figure 2: Different smart contract applications

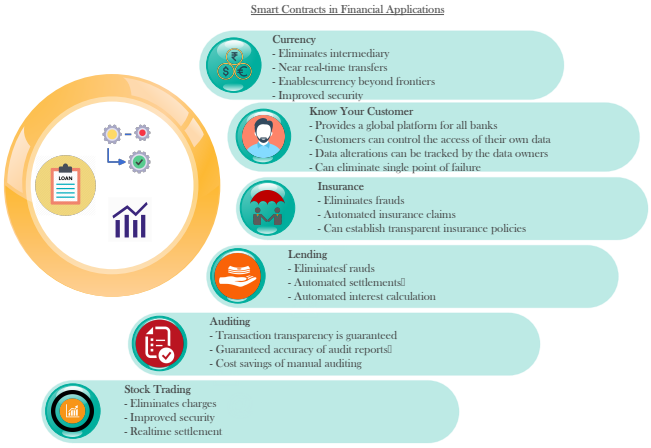


Figure 3: Benefits of Smart Contracts in Financial Applications

issue in today's financial world with Fiat currencies. The financial account information stored in the centralized systems in all leading payment organizations. The identity information such as Card Verification Value (CVV) of credit cards are vulnerable to domain expert hackers. The international remittance in Fiat currency is mostly not real-time and subject to commissions by the intervening banks.

Cryptocurrency is a revolutionary innovation of recent years to address most of these aforesaid issues. Powered by the blockchain technology, cryptocurrency is a digital asset secured with cryptographic techniques and operable with the smart contracts. Since the cryptocurrency is a "digital" asset, robust physical security is not required as the Fiat currency. Cryptocurrency transactions considered as psuedo-anonymous, since the complete identity of the sender and receiver not revealed by a third party, in contrast with the transactions routed through banks. Once committed, the transaction be recorded on a block and distributed among all the nodes in the blockchain ensures that any party cannot reverse the transaction as centralized banking transactions. The cryptocurrency transactions cannot be replayed when comparing with the credit card transactions.

Bitcoin by Satoshi Nakamoto is the first successful cryptocurrency in the world [1]. Eventhough Bitcoin does not di-

rectly support smart contracts, there are several approaches followed by researchers to incorporate smart contracts, such as [60] and [61]. Ethereum [47] is another prominent cryptocurrency innovation. Ethereum is not only a platform which provides a virtual computing environment called Ethereum Virtual Machine (EVM), but also Turing complete programming language to write smart contracts to run on the blockchain. In currency perspective, Ethereum declares its native token called "Ether" which is a bearable digital asset.

Hu et. al[62, 63] proposed Ethereum based payment solution for rural areas with non-persistent internet connectivity. The transactions were handled by the nodes connected to a local base station and transactions were processed by the miners and periodically connects to the synchronization of balances. Bowe et al. presented ZCash [64], which is an anonymous decentralized payment scheme that allows private transactions on a public blockchain using cryptocurrency. Duffield et al. [65] illustrated Dash which is a privacy-centric cryptocurrency based on Bitcoin. There are significant improvements in Dash when compared with Bitcoin, such as a two-tier incentivized network and which enables private transactions and instant transfers. Rosner et al.[66] identified Ripple as a seamless payment scheme that enables cross-border transactions seamlessly. The authors pointed out the significance of regulatory authorities to regulate the transactions committed on decentralized payment systems.

#### *3.1.2.* ***Know Your Customer***

Anonymous customers are restricted in almost all banks in the world to prevent money laundering and other illegal activities. Preliminary information such as names, addresses, social security numbers and contact numbers recorded by the banks after a formal customer screening process. If spurious activities are committed by the customers, those activities can trace and map along with their identities for further investigations. Every bank adhered to their own specification of Know Your Customer (KYC) process. This process includes a lot of paperwork and usually does not have a standardize way for cross-bank verification of an individual. The people conceal their identities in money laundering activities due to non-standardization and most of the times banks will be penalized for such criminal activities. In addition to that, the customers do not have authority to control the ownership of data.

In this regards, the incorporation of smart contracts can emancipate most of the awkward manual operations while enhancing the privacy preservation. Data alterations are traceable by both the bank and customers through the distributed ledger. Customers will have the ownership of data and can control the access to data to eliminate misuse of data. Anyone who need to access the data, has to request permission from the customer. Smart contracts can be used to enable such access dynamically. In addition, the distributed data storage enhances the single point of failure and risk of data loss as well. The blockchain based data storage ensures the availability of the service with its distributed service architecture.

Ye and Liang[67] discussed the benefits and how the smart contract transformation will revolutionize the banking industry. The author suggested that all data should store in the financial institutions in encrypted form and a summarized version of data should be shared to the public ledger. Moyano and Ross [68] proposed a Ethereum based KYC system to reduce the operational cost and enhance the customer experience. The authors also discussed the capability to incorporate permissioned blockchain such as Corda for the system. Alex et al.[69] proposed privacy preserving KYC scheme on Ethereum, which leverages the customer onboarding with compliance to the regulatory requirements. The system defined two smart contracts naming KycProvider and KyceToken. Each smart contract maintains access related information and functioning as standard ECR - 20 token for the KYC checks.

#### *3.1.3.* ***Escrow service***

Escrow is an essential service in the online international trading marketplaces. Escrow is a widely used technique to exchange funds in the international transactions. It acts as the trusted mediator in classical international trade ecosystems. Since there is no face-to-face meetings and physical contract establishment in the online international transactions, a trusted intermediary is a mandatory service. Escrow services require a service charge which a certain percentage of the transaction value. The present escrow services have non-realtime settlement processes with non-standardized dispute resolution mechanisms.

This requirement of a trusted third party in the escrow service is fueling the use of autonomous platforms such as blockchain based smart contracts. Application of the smart contract eliminates the transaction delays. The smart contracts enable near real-time settlements and the embedded rules will charge the penalties for delayed payments and delivery. The distributed service architecture of the smart contract will eliminate the single point of failure and ensure the service availability to streamline the business.

Peters [70] discussed the blockchain technology, smart contracts and its application in the global money remittance. The author discussed the possibility of multi-signature escrow services with smart contracts. The author also highlighted the key requirement of the smart contracts anticipated in the escrow including accuracy and trust. Bogner et al. [71] demonstrated a decentralized Ethereum based application for sharing tangible objects in everyday use. The solution implemented associating a web application and a mobile application that is capable of reading a QR code displayed on the objects. The system utilizes an escrow service to hold the associated fees as per the requirement.

#### *3.1.4.* ***Insurance***

Insurance is an essential service to the people for centuries. People insured numerous assets such as properties, vehicles, businesses and their own lives. Any insurance agreement composed of an insurer, organization which provides the insurance and the policy which are often formed as paper contracts have a longer process in agreements. In addition to that, the insurance frauds are accountable as more than 40 billion dollars a year, according to Federal Bureau of Investigations (FBI) statistics[72].

The claiming and settlement process takes time which is unfair customer experience.

The use of smart contracts in the insurance industry will be beneficial in multiple dimensions. The smart contract can be utilized to establish insurance policy terms and conditions in an immutable manner. No human intervention is required to settle a claim. Smart contract based auditing and verification process will be straightforward than the manual process with the globally distributed public and immutable ledger.

Hans et al. [73] emphasizes the usefulness of blockchain based smart contracts in the insurance industry. Authors stated that smart contacts can speeds up the claim processing and eliminate the administrative costs. The authors also highlighted that still there are some aspects including scalability, flexibility, and permissioned operation to be improved before integrate the smart contract into the insurance industry. B3i [74] is one of the most significant innovations to the insurance industry in collaboration with fifteen giants in the sector. The smart contract based systems improve the insure and re-insure value chain as well as improve customer experience in KYC process.In [75], authours illustrated the possible improvements in the insurance industry by using blockchain based smart contracts. The authors highlighted the enhanced customer satisfaction through unified KYC process, fraud detection since each claim transaction requires to verify by the number of parties to being approved, automation of claim processing, and innovative product integration capability such as micro insurance.

Guo et al. [76] proposed WISChain, which was intended for web identity security. They provide two insurance service models for web identity security and commercial website security, which enables the claim evidences to be uploaded automatically to the blockchain. [77] illustrated a convenient crop insurance for farmers in Ghana. The smart contracts have been defined to compensate the policyholders due to certain conditions such as drought or rainfall utilizing high resolution satellite images to identify the weather conditions to eliminate fraudulent claims. [78] illustrated Etherisc, which is a decentralized and smart contract based insurance system which defines two types of tokens for economic incentivization and to represent risks respectively. It was utilized Ethereum smart contracts to establish a standardized set of rules to define how stakeholders should function in the system. Vo et al. [79] presented a permissioned blockchain-based solution for the data provenance in car insurance. The system was implemented using the Hyperledger Fabric platform. The smart contracts were invoked in capturing events such as weather events, location variations of the car, and so on.

#### *3.1.5. **Lending and borrowing***

Lending, borrowing and loans are significant economic activities of a civilized nation which are important in the economic development. The economic development made the human needs sophisticated. The lending methods also diversified among different avenues as per the human needs. Peer to peer lending was a famous mode since the ancient economic ecosystems. This was transformed into flexible syndicated products presented by major financial institutions. Here, banks act as trusted third parties. Banks are the only authorized repository of money for lending and dominate the lending market. The current mortgage and loan processing often spans about 60 days[80]. This arduous process includes ascertaining loan applicants' credit scoring, and underwriters' profile verification.

| Application | Key challenges | Blockchain features | | | | | Key benefits |
|---|---|---|---|---|---|---|---|
| | | Decentralization | Forge resistance | Transparency | Autonomous execution | Accuracy | |
| Know Your Customer: [67], [68], [69] | Redundant data entry at all banks | ✓ | | | | | • Improved customer experience<br>• Cross bank verification capability for customer details<br>• Data alteration can be tracked through ledger<br>• Universal data sharing is possible<br>• Eliminated overheads<br>• Better customer experience<br>• Access to the data can be controlled by the data owner |
| | Administrative overheads | ✓ | | | ✓ | ✓ | |
| | Cumbersome customer experience | ✓ | | ✓ | | | |
| | Data security and user privacy issues | | ✓ | | | | |
| | Data alteration cannot be tracked | | ✓ | ✓ | | | |
| | Data duplication overheads | ✓ | | | | | |
| | Universal data sharing is impossible | ✓ | ✓ | ✓ | | | |
| | User cannot control access to his data | ✓ | | | | | |
| Escrow service: [70], [71] | Settlement delays | ✓ | ✓ | | | | • Transparency<br>• Non repudiation<br>• Settlement is faster |
| | Expensive service fees | ✓ | | | | | |
| | Non repudiation is hard | ✓ | ✓ | ✓ | | | |
| Insurance: [73], [74], [75], [76], [77], [78], [79] | Insurance policies and terms and conditions are mentioned as paper contracts | ✓ | ✓ | | | ✓ | • Immutable policies<br>• Transparent policies<br>• Reduced overheads<br>• Fraudulent claims eliminated |
| | Auditing and verification of claim is a separate process | ✓ | ✓ | ✓ | | ✓ | |
| | Fraudulent claims | ✓ | ✓ | | ✓ | ✓ | |
| | Claiming process is costly | ✓ | | ✓ | | | |
| Lending: [81], [82], [83], [84] | Time and cost intensive verification processes | ✓ | | ✓ | | | • Immutable policies<br>• Automated recovery process<br>• Reduced overheads<br>• Transparent credit scoring<br>• Transparent agreements |
| | Credit scoring is a manual and non-transparent process | ✓ | | ✓ | ✓ | ✓ | |
| | Administrative costs | ✓ | | ✓ | | ✓ | |
| Auditing:[85], [86] | Time and cost intensive verification processes | ✓ | ✓ | ✓ | | | • Improved accuracy<br>• Automated audit process<br>• Elimination of specialized human intervention |
| | Credit scoring is a manual and non-transparent process | ✓ | ✓ | ✓ | | | |
| | Administrative costs | ✓ | ✓ | | | | |
| Stock Trading: [87], [88], [89], [90], [91] | Centralization | ✓ | | | | | • Transaction transparency<br>• Decentralization and ensured availability<br>• Improved accuracy |
| | Transactions will be charged by centralized authorities | ✓ | | | ✓ | | |
| | Transparency is not available | | | ✓ | | | |

Table 5: Summary of Applications of Smart Contracts in Financial Context

In addition to that, the loans were subject to processing fees and few other surcharges imposed by the bank. Some hidden charges can surprise the customers too. Borrowers sometimes escape and refuse to pay back the loan.

The smart contracts circumvent the existing issues and promise a trust based ecosystem which streamlines the application and payment with automatic execution. The smart contracts can automate the different manual processes which hinder the loan processing, utilizing the distributed ledger. Credit scoring, expense history analysis are few possible solutions which can be ideally replaced with the smart contracts to improve the process. Salt Lending [81] is world's one of the largest lending platforms with market capital of USD 126 millions. The borrowers send collateral to Salt's multi signature wallet in according to enforced conditions automatically. EthLend [82] is an Ethereum based lending platform. The important attributes such as loan terms, fund transferring conditions, and collateral are being handled by smart contracts with ERC-20 tokens. Everex [83] is a Singapore based lending and remittance service. Everex provides a transparent platform for the unbanked customers in South East Asian countries. It uses ERC-20 token which can be pegged with fiat currencies. Debitium [84] is one of the Ethereum based crowdfunding platforms. It facilitates cross border deals and connects borrowers and investors.

#### *3.1.6. **Auditing procedures***

The Auditing is a significant activity in an organization. Due to regulatory requirements, the organizations have to undertake the audit through a trusted independent third party organizations. These organizations charge explicitly for their operations. The audit operation is a tedious manual process which requires substantial human intervention. The derived insights from the audits will depend on human accuracy.

Audit procedures associated with smart contracts automate the audit procedures and eliminate the additional costs and human errors. The accuracy is guaranteed by the autonomous execution of smart contracts in real-time. Due to the distributed and transparent nature of the smart contract, the regulatory authorities can trust the executory conditions are not being tampered. Also the smart contracts can customize to derive deeper insights for data analytics.

Zou et al. [85] proposed a blockchain based audit scheme to eliminate forging of audit records. Rozairo et. al. [86] explained the applicability of smart contracts in the auditing procedures. Still the auditing require some more contribution of the blockchain based solutions.

#### *3.1.7. **Stock trading service***

Stock exchange is one of the most prominent activity in a financial structure. Most of the countries trade stocks valued in millions of dollars per day within traders. These traders are ranging from individual investors to multi millionaire public listed companies. Each transaction executes by intervention of different parties including brokers of the buyer and the seller, clearing houses and transferring agents. The current setup imposes commissions and charges on each player and prone to human errors. Sometimes the settlement is not realtime. Furthermore, the fiat currency based architecture operates with centralized governance architecture which limits the market access restricted to the people. The stock trading market access controlled through the registered brokers, which introduced additional overheads of time and cost to the people who are interested in trading.

The centralized trading architecture can be eliminated by incorporating smart contracts and will enable peer to peer transaction capability for the traders. The terms and conditions can be established transparently by using smart contracts. There is no centralization of trust is required since the ledger is decentralized and the network guarantees the conditions are immutable over the network. Therefore, smart contracts will empower the next generation stock exchanges eliminating human errors, centralization and additional charges incurred on traders along with faster settlement.

Yermack [87] discussed the advantages of blockchain based smart contracts for corporate governance and how financial asset trading will be benefited from smart contracts. The author emphasized that the improvement of tracking the ownership with public ledger will be accurate in financial record-keeping with greater transparency as well as improve the liquidity. The author elaborated that countries including the USA and Australia started experimenting with smart contract powered security trading platforms. [88] presented TITA which is an Ethereum blockchain based system which supports commodity trading for manufacturers and consumers. The system defines a token to enable purchases and transfers and incentivizes the token generating contributors of the network. Smart contracts transfer assets or establish escrow conditions as required. [89] is a prominent application of permissioned blockchain based smart contract application for stock exchange in Australia. It provides automated clearing and settlement by smart contracts along with some significant post-trade activities. They provided Digital Asset Modeling Language (DAML) and run privately on a defined set of nodes.[90] and [91] in Hong Kong developed by following the Australian Stock Exchange implementation.

### *3.2. Health Care Related Services*

The research and development in the health care domain have increased the life expectancy. As a result, the number of elderly people in the world who will require periodical medical attention is gradually increasing. New insurance schemes such as Affordable Care Act enrollment in the USA increased the number of patients seeking preventive medicine who were previously reluctant on medical care due to financial constraints. These reasons increased the volume of patients significantly over the the past few decades. Handling such an unprecedented volume of patient data manually is a cumbersome process. Manual processes incur significant administrative overheads and prone to life critical human errors. The digital transformation will eliminate these issues associated with the manual process but exposed to an array of data security threats. If these information systems integrated with prescription drug operations, the complexity and security requirement of the ecosystem will be increased drastically.

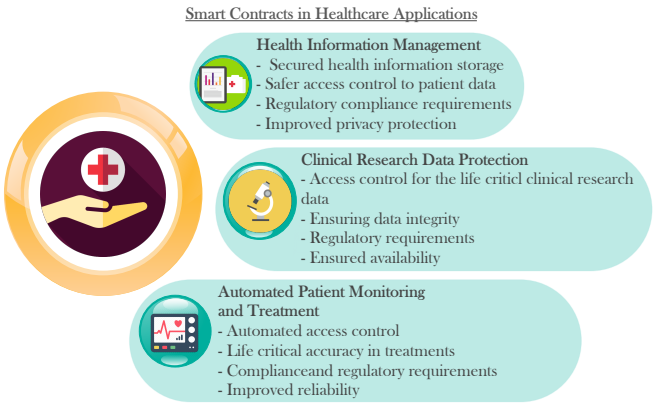


Figure 4: Smart Contract Applications in Healthcare

Therefore, incorporation of the smart contracts to the health care ecosystem will be significantly effective in different dimensions. A quick overview of smart contract applications on healthcare displayed on Figure 4. Table 6 summarizes the applications of smart contracts in the healthcare context along with the benefits and challenges. Candereli et. al [92] explored the opportunities in healthcare with a scientometrics analysis. McGhin et al. [93] presented a comprehensive review on research challenges and opportunities in the blockchain in the healthcare context.

### *3.2.1. **Health information management***

Modern medical institutions are mostly empowered with automation techniques to handle the myriad volume of patients. The IoT integration is a wider domain including remote treatments and real-time monitoring. These systems generate a massive amount of patient data which is confidential and life critical. But most of the systems in some countries are not compliant with international standards such as the Health Insurance Portability and Privacy Act (HIPAA). Some systems are still rigid and still may require some paperwork. The health information system must ensure data privacy and integrity, as well as availability. These services are indispensable in the health context rather than the other industries because the medical information is highly relevant in invaluable life assets. The blockchain technology and smart contracts can be applied to enable the health information management systems to ensure privacy, integrity and access control to achieve regulatory compliance along with the enhanced patient experience.

Azaria et al. presented MedRec [94] , a decentralized electronic health record management system which enables the patients to access their medical records across multiple treatment sites. The system is being leveraged by the blockchain and smart contracts, developed on Ethereum platform and manages authentication, confidentiality, accountability and data sharing with a crucial consideration on sensitive patient information. The system is interoperable with existing medical record ecosystems. Nichol and Brandt [95] presents a concept for co-creation of trust in healthcare, using three conceptualized postulations as interoperability, security, and payment. The authors explained with examples clearly how the blockchain based smart contracts will solve different problems in healthcare including the trust establishment and frauds. The authors defined blockchain based smart contracts will be a game changer in future of healthcare.

Kuo and Lucila [96] presents Modelchain, an adaptation of blockchain based smart contracts for the privacy preserving healthcare predictive modeling framework. The authors designed a framework to integrate online machine learning with blockchains and utilized transaction metadata for the predictive model dissemination. The authors designed a new proof-of-information algorithm on top of proof-of-work conesus algorithm to determine the order of online machine learning on blockchain. Dagher et al. [97] proposed Ancile, which enables secure, interoperable, and an efficient access control framework to medical records by the patients along with privacy preservation using Ethereum smart contracts. The solution transfers the ownership and control of the patient himself. The system developed with six smart contracts for operations including consensus, classification, ownership of data, permissions and re-encryption and maintains hashes of the records for integrity. The system enables data ownership transfer permission to the patient and compliant with HIPAA requirements. Yue et al. [98] proposed Healthcare Data Gateway (HDG), which is a blockchain powered mobile application allows patients to control the access of medical data by his own to ensure patient data privacy. The authors portrayed the application of Secure Multi-Party Computation on patient data to enable untrusted parties to compute patient data within privacy limits defined. The system used blockchain storage platform to manage data by the patient and the authors discussed about new hopes on 5G to faster data manipulation with enhanced network speed.

Novikov et al. [99] presents a blockchain based smart contract based distributed data register for creation of electronic medical card and an algorithm for the use of smart contracts. The authors have highlighted the establishment of reliability and transparency through blockchain and its significance on the medical information system. The authors suggested Ethereum platform for development of the suggested Integrated Electronic Medical Record register. Alexaki et al. [100] presented a conceptual medical record access and sharing mechanism powered by blockchain based smart contracts. The authors suggested development of the system based on either Ethereum or Quorum, which is the permissioned version of Ethereum blockchain. The authors applied smart contracts for significant roles including identity registration, patient record management and electronic patient record access agreement. Kuo et. al [101] presented an open discussion on the benefits, pitfalls and latest applications of blockchain based smart contracts to the biomedical and healthcare domain. The authors discussed the key benefits including improved medical record management, enhanced interfacing with insurance systems for the claiming process, accelerated clinical and biomedical research and data transparency and enhanced medical ledger with robustness and security. The authors discussed the key challenges of blockchain in healthcare is the publicly available health records.

| Application | Key challenges | Blockchain features | | | | | Key benefits |
|---|---|---|---|---|---|---|---|
| | | Decentralization | Forge resistance | Transparency | Autonomous execution | Accuracy | |
| Health Information Management: [94], [95], [96], [97] , [98], [99], [100], [101] | Attacks will affect the human lives | ✓ | ✓ | | | ✓ | • Accuracy of life critical operations<br>• Robust access control to the systems<br>• Data alteration trackable |
| | Human oriented programming errors | | ✓ | | ✓ | ✓ | |
| | Access control issues to the control systems | ✓ | ✓ | | ✓ | | |
| Clinical Research Data Protection: [102], [103], | Integrity requirements | ✓ | ✓ | | ✓ | ✓ | • Privacy enforcement<br>• Eliminated centralization<br>•Ensured availability |
| | Compliance requirements | ✓ | | | ✓ | ✓ | |
| | Access control requirements | ✓ | ✓ | | | ✓ | |
| Automated Patient Monitoring and Treatment:[104] | Attacks will affect the human lives | ✓ | | | ✓ | ✓ | • Accuracy of life critical operations<br>• Robust access control to the systems<br>• Ensured integrity of accumulated data |
| | Robust access control to the systems | ✓ | ✓ | ✓ | | | |
| | Ensured integrity of accumulated data | | ✓ | | | | |

Table 6: Summary of Applications of Smart Contracts in Healthcare Context

#### 3.2.2. *Clinical research data protection*

The data integrity of clinical trials is a major concern in medicine. The data integrity defined as the extent which the electronic and paper based data are complete, consistent, accurate, trustworthy, and reliable throughout the data lifecycle. There are guidelines such as International council for harmonization guideline for good clinical practice established to regulate the data integrity in different perspectives. The significant problems of the credibility of scientific data are data loss, endpoint switching, data dredging and selective publication. The treatments due to distorted data will expose the patients into a life risk. The paper based systems do not guarantee the integrity of data. The risk exists of losing the printed or hand-written papers where the data rests. Eventhough the computer systems utilized, still some robust security measures should be applied to prevent data loss and theft. Sometimes, the digital form of data will be more vulnerable than paper written data. The clinical research data repositories associated with smart contracts will be the ideal solution to enforce access control and regulatory compliance.

Nugent et al. [102] signified the enforcement of regulatory requirements and trust in clinical research data by blockchain based smart contracts using Ethereum platform. The smart contracts, naming as regulator contract and the trial contracts acted as trusted administrators of the system. The authors utilized two smart contracts. The regulator contract holds a data structure for clinical trial authorization while the trial contract is built using functions within the authorization contract. Zhang et al. [103] proposed a framework on managing and sharing electronic medical records of cancer patient care using Hyperledger Fabric blockchain platform along with symmetric and asymmetric encryption techniques as well as proxy re-encryption. The authors proposed that privacy, security, availability, and fine-grained access control over medical data ensured and mainly focused on the secured sharing of medical data, for research or treatment requirements between medical organizations. The smart contracts eliminated the requirement of trusted third party and ensures privacy and access control policy defined by the patient and used encryption techniques to store the data on the ledger. When comparing [103] with [102] , there are significant differences can be identified. [102] was built on Ethereum smart contract, which is a public blockchain. The public blockchain transactions are cost intensive with account management and mining contribution. In contrast, [103] implemented on Hyperledger Fabric private blockchain which provides flexibility for the stakeholders to regulate. For an instance, Hyperledger Fabric enables the nodes to define consensus policy according to their preference.

#### 3.2.3. *Automated patient monitoring and treatment*

The IoT and wearable devices have been embraced by people from smartwatch to Wireless Body Area Network (WBAN). The WBAN leverages IEEE 802.15.6 and IEEE 802.15.4j standards which were specifically standardized for medical WBANs. The core objective of WBAN is to improve the communication speed, accuracy, and reliability of sensors attached in the immediate proximity to the human body. The WBAN sensors may generate a massive amount of data such as blood glucose level, the pulse rate, blood pressure, and so on. The expansion of such systems raised the requirement of privacy, access control and integrity of data. Each device should be operated with robust automated access control mechanism to eliminate the risk of the patient. Rogue access to the automated patient monitoring and treatment system can kill the patient within few seconds by jamming the treatments. The smart contracts will be the next generation solution to eliminate the risks by controlling access and autonomous safe execution of the treatments in automated patient monitoring and treatment systems.

Griggs et al. [104] proposed a system which utilizes private Ethereum blockchain and master-slave modeled medical device deployment model. The sensors connected with the smart device, such as either a smartphone or tablet. The sensors can connect to apparatus such as insulin actuators and blood pressure monitors to execute smart contracts and eventually the records will transfer to the immutable ledger. The data received by the smart device is sent to the smart contract, along with the customized threshold values and smart contracts evaluate the data and trigger alerts to the patient, healthcare provider and instructs to the actuator nodes for automated treatment if required.

### 3.3. *Identity management and access control*

Identity management and access control are essential services in every enterprise. The classical identity management systems are mostly centralized and associated with expensive hardware such as smart cards and hardware security modules. Centralised systems will elevate the risk single point of failure and require a robust backup, recovery and disaster management procedures. There are scalability limitations exist in the centralized systems. Sometimes the latency in identity management and access control can be observed when they were connected to IoT devices due to computational power limitations.

The distributed ledger technologies will be the next generation of identity management and access control systems. Smart contracts based access control systems promise accuracy, high availability, and fault tolerance. Table 7 summarizes the applications of smart contracts in the identity management and access control context along with the benefits and challenges.

#### 3.3.1. *Identity Data Protection*

The value of personal identity information is proliferating with the association of modern technologies to the human life. The devices such as smartphones, wearables generate enormous amount of personal data such as location, identity information and so on. Most of the leading applications, including social media used by the people are centralized and the user has minimal rights to control the data. Still most of the users are unaware of the significance of their personal information. The incidents like Cambridge Analytica Scandal reflect that the capability to abuse the personal data without the owners' consent[105]. Data owners should be capable of controlling the access of their data to avoid such incidents.

The smart contracts are a blessing solution for the access control of identity information and eliminate data theft. The decentralized nature of smart contracts will enable the data owners to control the access of their own data with decentralized and transparent nature. The distributed ledger is applicable to record the access of the individual personal data, which ensures that the data did not access unnecessarily, such as for a third party.

Banerjee et al. [106] proposed a novel framework associated with blockchain based smart contracts for users to track how is their personal identity information is stored, used and shared by the service provider. The authors developed an automated access control and audit mechanism which enforces users' data privacy when sharing data across third parties. The authors also mentioned that their system can be adopted by big data users to automatically apply their privacy policy on the data flow and track operations. Ouaddah et al. [107] present a blockchain based privacy preserving authorization management framework which enables users to control their own data. The authors implemented the initial implementation on the typical IoT use case on Raspberry Pi. There are few types of transactions used to grant, get, delegate, and revoke access.

#### *3.3.2.* ***Decentralized identity management***

Classical identity management and access control systems such as LDAP (Lightweight Directory Access Protocol), IAM(Identity and Access Management) and PKI(Public Key Infrastructure) are aligned with common centralized architecture. The centralized identity management systems developed with privileged access management to the administrator(s) which enable the administrators to manipulate data, central point of failure and expensive perimeter security requirements for compliance. The access credentials associated with private keys will be vulnerable if they are stored in a centralized server, probably in the cloud. Perimeter security requirements will incur costs to the organizations to deploy expensive Hardware Security Modules and tokens with extensive administration and maintenance overheads. If a rogue user disables the centralized service, entire system will be affected.

Instead of the centralized access control systems, the decentralized system will heal many pains of centralized access control. The smart contracts will provide access to the individual user without invocation of centralized service and in network efficiency perspective, optimal than the centralized systems. The smart contract logic will be transparently deployed and the users can guarantee that their access control or identity information not manipulated by a privileged access management personal. The distributed nature will ensure the service is up and running and cannot be halted by attacking a single server.

Zhang et al. [108] investigated critical access control issues in IoT and proposed a smart contract based access control system with multiple access control contracts. The authors defined three contract types, as the access control contract, judge contract and register contract. The authors demonstrated the framework using IoT system and a desktop computer. Es-Samaali et al. [109] proposed a blockchain based access control framework to reinforce the security of bigdata platforms. The key features included the distributed nature and lack of central authority with transparency, light weight, fine granularity. They authors defined an authorization token which defines the access right by the creator of the smart contract. SCPKI [110] is an alternative PKI system with decentralized and transparent design used with smart contracts on Ethereum blockchain. The main advantage of the system is to identify the rogue certificates with he web-of-trust model when they are published. The model enables an entity or authority in the system can verify fine-grained attributes of another entity's identity.

Blendcac [111] is decentralized smart contract based access control solution for devices, services and information in large scale IoT systems. The authors proposed a robust capability token management strategy which utilizes smart contracts for registration , revocation and propagation of access authorization. The authors developed a PoC on private blockchain on the resource constrained devices which is raspberry pi and laptops and demonstrated the feasibility. Lin et al. [112] presented a blockchain based fine-grained access control framework for the Industry 4.0.

Ali et. al [113] proposed a decentralized access model using blockchain for IoT data using a network architecture naming as modular consortium architecture. The architecture has in-built privacy with adaptability for various IoT use cases. The feasibility and deployment considerations for the implementation analyzed in a performance evaluation of existing blockchain development platforms including Ethereum and Monax. Lee et. al [114] pointed that in the IoT environment, when data or device authentication information appended to the blockchain, there is a risk of the information leakage through proof-of-work process or address searching. They authors applied a zero-knowledge proof to a smart meter system and enabled the transaction processing through disclosing the information such as public key. They authors also studied the avenues to enhance the anonymity of blockchain for privacy protection.

#### *3.3.3.* ***Security policy in access control***

Security policy is a core regulatory component in any organization as well as Internet applications. The security policy defines the required security controls aligned with the organization's strategic rules and regulations. The depth of access of the users for the infrastructure or resources will depend on the security policy. The centralized security policy and governance architecture is one of the mostly adopted architecture for most of the organizations. With the centralized security policy management, the capability to customization is cumbersome. For an instance, if the employee promoted to the next level, the scope of accessible resources required to expand. Customization of the centralized security policy incurs additional overheads. If the organization deployed beyond frontiers, the overheads will be more. Furthermore, there is a risk of manipulation of centralized security policy without user's consent.

| Application | Key challenges | Blockchain features | | | | | Key benefits |
|---|---|---|---|---|---|---|---|
| | | Decentralization | Forge resistance | Transparency | Autonomous execution | Accuracy | |
| Identity Data Protection:[106], [107] | Risks cloud data theft | ✓ | | | | | • Decentralization<br>• Access control policy to the data can be defined by by data owners<br>• Transparent access log |
| | Central point of failure | ✓ | | | | | |
| | Data access and usage cannot be observed | | ✓ | ✓ | | | |
| Decentralized Identity Management: [108], [109], [110], [111] ,[113], [114] | Identity management service unavailability risk due to centralization | ✓ | | | | | • Privacy enforcement of clinical research data<br>• Eliminated trusted third party<br>•Ensured availability |
| | Data consumption is not efficient in centralized systems | ✓ | | ✓ | | | |
| | Scalability limitations | ✓ | | | | | |
| Security Policy in Access Control: [115], [116] | The stakeholders may claim security policy is biased and favorable due to lack of transparency | ✓ | ✓ | ✓ | | | • Improved perimeter security when comparing with the cloud<br>• Decentralization and ensured service availability<br>• Scalability |
| | Prone to human errors if a human intervention exists | ✓ | ✓ | | | ✓ | |
| | Performance limitations | ✓ | ✓ | | | ✓ | |

Table 7: Summary of Applications of Smart Contracts in Identity Management and Access Control Context

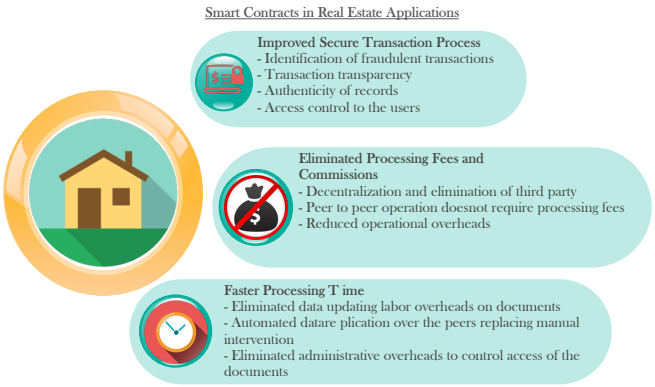


Figure 5: Smart contracts in Real Estate

The smart contracts promise the autonomous execution of the program once the predefined conditions met and an ideal solution for decentralized security policy management. The security controls can define as programs and deploy in the smart contracts. The autonomous execution eliminates the overhead of human intervention in the security policy. The distributed nature of the blockchain based smart contract guarantees that the execution logic is not being manipulated by either an administrator or any rogue user within the organization. The decentralization ensures the transparency as well as the availability of the security policy management system.

Cruz et al. [115] presented a role based access control using Ethereum smart contracts. The smart contracts used for the creation of user role assignments and eventually published to the blockchain. The smart contract provides significant features including managing and modifying information as required in a transparent manner. Outchakoucht et al. [116] proposed dynamic and fully distributed security policy implemented with smart contracts. In addition to that, the authors proposed to apply machine learning algorithms, particularly on reinforcement learning for dynamic, optimized and self-adjusted security policy. The smart contract learns from prior experience to adjust the optimal security policy. Lyu et al. [117] proposed blockchain based access control mechanism in the information centric networking context. Ali et al. [118] proposed blockchain based access control mechanism for conflict of interest domain.

### *3.4. Real Estate*

Commercial real estate industry composed of various transaction types such as leasing, rental and purchases with different asset classes including commercial properties, houses, lands and so on. The government authorities such as national land registry handle all information of the real estate ownership, leasing and so on. Transferring ownership and leasing transactions performed with the intervention of few trusted third parties. Such operations are manual and exposed to human errors, data manipulation risks and extensive processing time.

Smart contracts will be the next generation solution which will revolutionize the real estate trading industry by a storm with enhanced security and optimized processing time. An overview of smart contracts in real estate context displayed in Figure 5. Table 8 summarizes the applications of smart contracts in the real estate context along with the benefits and challenges.

#### *3.4.1. **Improved secure transaction process***

Multiple fraudulent transactions can be identified in the real estate industry. When the title of the asset, either a land or house is represented by a printed document, the authenticity of document cannot be easily verified. There are cases where a person can fraudulently duplicate the title document and submit to multiple banks as security asset to obtain a loan. The authenticity of paper title cannot verify in realtime by the current centralized systems. There are cases the land owner sells a land to multiple people using the duplicated paper titles. The key problem is that the authenticity of paper title issued by a trusted third party cannot be verified by the individuals.

Smart contracts eliminate the lead time for a title transfer and the transparent conditions will hiccup the fraudulent ownership transfer approaches. The ownership information stored in the public ledger and the parties such as banks can verify the ownership of the security.

Karamitsos et al. [119] examined design of Ethereum smart contract for the use cases of real estate, which is renting residential and business buildings. The authors proposed that the smart contract created between landlords/real estate owners and tenants which verifies that the rental agreement is signed, rental amount paid on time, and the contract terminated correctly. The authors also highlighted the improvement of the invoicing process through the smart contracts and stated that they need to asses the same use case with Hyperledger Fabric. Spielman [120] presented the blockchain application for the land title registry. The key advantages discussed the elimination of the centralized database in the land registry with enhanced security. Since all parties are involved in the consensus, the incapability of fraudulent transactions in the land title ledger was highlighted. Dijkstra [121] presented different possibilities and constraints for the blockchain in the real estate management process. The research conveys that blockchain is still required to improve different dimensions such as government regulation, standardization and so on. The interviews conducted in the research reflect significant insights such as digitally signing the lease contracts and monitoring the obligations via smart contracts are the most important applications of blockchain in the real estate management process.

#### *3.4.2. **Processing fees and commissions for transactions***

The trust establishment of real estate industry accomplished with the intervention of few trusted third parties such as government bodies and banks. These organizations incur processing fees and commissions such as stamp duties for their maintenance. The fees are not negligible when the transaction value is million dollars.

| **Application** | **Key challenges** | **Blockchain features** | | | | | **Key benefits** |
|---|---|---|---|---|---|---|---|
| | | Decentralization | Forge resistance | Transparency | Autonomous execution | Accuracy | |
| Improved Secure Transaction Process: [119], [120], [121] | Paper documents can be duplicated | | ✓ | ✓ | | | • Transaction authenticity<br>• Eliminates fraudulent duplication of ownership documents |
| | Central point of failure | ✓ | | | | | |
| | Authenticity is hard to ensure | | ✓ | | | | |
| Processing Fees and Commissions:[122] | Processing fees are higher making the transactions are expensive | ✓ | | | | | • Decentralization enables peer to peer transfer eliminating centralized systems<br>• Eliminated trusted third party<br>•Peer to peer operations |
| | The transaction costs are governed by centralized authorities | ✓ | | | | ✓ | |
| | Centralized operational overheads | ✓ | | ✓ | | | |
| | Central point of failure | ✓ | | | | | |
| | Ownership documents in paper can be forged | ✓ | ✓ | | | | |
| Extensive Processing Time: [123] | Processing requires updating on few centralized systems with extensive time for processing | ✓ | | | | | • Faster operations in peer to peer<br>• Transaction data stored in distributed ledger<br>• Faster verification |
| | Dependencies with multiple parties | ✓ | | | | | |
| | Costs for different data retrievels | ✓ | | ✓ | | | |

Table 8: Summary of Applications of Smart Contracts in Real Estate Context

Smart contracts eliminate the requirement of a trusted third party since the transfer executes the smart contract itself. Elimination of the trusted third party executes the ownership transfer in real time without processing fees and will reduce unnecessary costs to the consumers.

Oparah [122] highlighted the importance of smart contracts for elimination of costs incurred by the trusted third party. The cost is around 1-2% of the total value of the property which is not negligible. The importance of smart contract and the enablement to transfer the ownership between two homeowners legitimately without paying for third party verification.

#### *3.4.3. **Extensive processing time***

Current systems are mostly oriented with the centralized authorities. The centralized organizations handle the documents related to the ownership of lands such as titles. Sometimes the documents reside on owner's district or state local authority. This type of architecture consume time to deliver documents to each local authority and update information. In contrast, the smart contracts will execute in real-time or near real-time to transfer ownership which eliminates logistics problem and reduce costs.

Fernandaz et al. [123] proposed Evareium, which is a smart contract system for trading commercial property. The investors can trade ERC20 compliant tokens issued from Ethereum blockchain and utilize them to fractions of underlying property assets linked to the tokens. The system provides a faster, reliable and transparent platform for trading a plethora of real estate assets such as commercial properties and hotels.

### *3.5. eGovernment/Law*

Transformation of the government services and legal enforcement into the electronic genre grabbed attention by most of the nations including Europe, Asia, and many other regions. From the electronic services of government, the stakeholders anticipate different features. These include trust, accuracy and improved efficiency as well as user satisfaction. The increased population and complexity of the human needs escalated the requirement of automation to cope with enormous demand volume. Regardless of the service type, the eGovernment solutions handle personal data of the civilians. Uninterrupted service availability is also expected by the stakeholders. Blockchain based smart contracts are one of the most promising solution with significant features for eGovernment services as well as legal enforcement. Table 9 summarizes the applications of smart contracts in the eGovernment and Law context.

#### *3.5.1. **Enforcement of law***

The legal system of any country is complicated and consists of numerous terms and conditions. In a broader view, almost all conditions executed with the direct intervention of judicial personal after a certain assessment. For an instance, if a driver exceeded 10 percent of the speed limit, there is a predefined penalty. If he exceeded 20 percent, the penalty is even higher. The conditional execution intervened with a human. For more complicated cases, the assessment duration is exorbitant which can drag upto years. The human intervention exposes decision to human error. Therefore incorporation of the smart contract for legal enforcement is important because it enables the autonomous and accurate legal execution. However, all the legal terms cannot develop directly as smart contracts. Some straightforward terms are possible to deploy as smart contracts.

Raskin [124] examined the smart contracts' operation and its position in the existing contract law. The author distinguished the smart contracts as strong and weak, corresponding to the costs of their revocation and modification. The author also highlighted the significance of encouragement of smart contracts by the legislature as another form of agreement. Alexander [125] examined the key tensions between classic contract law and smart contracts. The author also analysed the alignment of powers of government on distributed ledgers without a central authority. The author suggested two main approaches to achieve the requirement. Sheilds [126] examined the potential use cases of blockchain based smart contracts along with their technical limitations and barriers. The author also described the legal and regulatory issues associated on the adoption of smart contracts. The legal changes which should be enacted to realize the benefits of technology also discussed in the article. Koulu [127] explained application of self-executory smart contracts and blockchain technologies along with their application to online dispute resolution. The author described the logic behind smart contracts with a more concrete example on a betting on weather of a given location. The article provides a further analysis of legal implications outside its application of virtual currency.

Levy [128] analyzed in depth the smart contract and its role to automatically execute the obligations without a centralized enforcement authority. The smart contract and its implication for social justice and fairness also discussed in the paper. The potential weaknesses of the smart contracts in the legal perspective discussed. Rosa et al. [129] presented application of the smart contract for the intellectual property protection for open innovation programmes targeted on small to medium enterprises. The users sign smart contracts as non disclosure agreement with timestamping with the corrective actions as required. The solution provides a smart contract based fine grained intellectual property management for open innovation programmes.

Tietze and Granstrand [130] presented a distributed ledger based approach to automate the intellectual propert y licensing payments. Lauslahti et al. [131] analyzed the smart contract from the perspective of digital platforms and the Finnish contract law. The authors also examined the formation mechanisms of the general principles of contract law in the application of smart contracts. The adaptability of smart contracts as the current legislation also evaluated. Watanabe et al. [132] proposed a method of recording the classical contracts. The authors utilized a transaction to evidence the contractor consent and information. The authors used encryption to keep preserve the confidentiality of the contracts.

| Application | Key challenges | Blockchain features | | | | | Key benefits |
|---|---|---|---|---|---|---|---|
| | | Decentralization | Forge resistance | Transparency | Autonomous execution | Accuracy | |
| Enforcement of Law by Smart Contracts: [124], [125], [126], [127], [128], [129], [131], [132] , [130] | Biased execution of law and order | | ✓ | ✓ | ✓ | ✓ | • Automated, faster, and accurate legal processes<br>• Transparency of execution and conditions<br>• Unbiased legal execution |
| | Human oriented assessments are cost intensive | ✓ | ✓ | ✓ | ✓ | | |
| | The time to conclude on a decision takes time | ✓ | | ✓ | | ✓ | |
| Smart Contracts to Automate Contractual Agreements:[133], [134] | Processing fees are higher making the transactions are expensive | ✓ | ✓ | ✓ | ✓ | | • Autonomous execution with improved accuracy<br>• Eliminated trusted third party<br>• Improved transparency of contractual conditions |
| | Time intensive operations for the conditional changes of contractual agreements | | ✓ | ✓ | | ✓ | |
| | The contract terms can be manipulated | ✓ | ✓ | ✓ | | | |
| | Central point of failure | ✓ | | | | | |
| Smart Contracts for Public Services: [135] , [136], [137] | Labor intensive administrative processes | | | ✓ | ✓ | ✓ | • Improved security<br>• Improved user satisfaction<br>• Eliminated overheads |
| | Administrative overheads | ✓ | ✓ | | ✓ | ✓ | |
| | Lower citizen satifaction | ✓ | ✓ | ✓ | ✓ | | |

Table 9: Summary of Applications of Smart Contracts in eGovernment and Law

#### 3.5.2. *Contractual agreements*

A contract is an agreement made between two or more parties with legal binding and enforceable by law. Contractual agreements in the business are composed with precisely defined terms and conditions. The terms and conditions are significant to the parties on the contract because they will set rights and obligations as well as price variation clauses for each. Classical contracts formed with the intervention of a trusted third party such as the notary. The on boarding of the trusted third party to form a contract incurs service charges. Most of the times, the trusted third party is a human and hence the risk of human error also exists. The terms and conditions can be manipulated by the third party if required.

The smart contracts are applicable to solve few issues associated with classical contracts. The smart contracts eliminate the requirement of trusted third party and it will eliminate the service cost of the notary. The terms and conditions can convert into programmable codes and deployable publicly. Terms and conditions are transparent and guarantee that they have not been manipulated. Furthermore, smart contracts can take their decisions of their own. For instance, the imposing penalties can be defined if the terms and conditions breached. Smart contracts are an ideal solution to replace the classical contracts and improve efficiency, effectiveness and security.

Frantz et al. [133] proposed a modeling approach that supports the semi-automated translation of human readable contract representations into computational equivalents to enable the codification of laws. The translated contracts are verifiable and enforceable computational structures reside within a public blockchain. The authors identified the smart contract components that correspond to real world institutions and explored capability based on selected examples. Scheid and Stiller [134] explained the application of smart contracts to automate the service level agreement process by eliminating any third parties during negotiations with guaranteeing terms agreed upon the service level agreement will not change. Through the smart contract, the bureaucratic and manual compensation process is replaceable by the autonomous contractual process which on board any untrusted parties together, such as subscriber and service provider. The PoC presented in the smart contracts for compensation of service level agreement using network function virtualization.

#### 3.5.3. *Public services*

eGovernment refers to electronic implementation of a broader spectrum of public services provided by the government to the citizens. eGovernment services include issuance of identification documents, taxation, insurance, utilities, border control and so on. To establish the trust, most of the eGovernment services developed adapting to a centralized architecture. For an instance, PKI is a vital component in most of the classical eGovernment service. PKI establish the root of trust as the root CA. The centralized eGovernment systems have all of the common issues associated with any centralized systems, including administrative overheads, the central point of failure, expensive perimeter security requirements and so on. The smart contracts will eliminate the major issues mentioned and will provide a decentralized highly available eGovernment system with extended transparency.

Mark [135] discussed multiple eGovernment applications integrated with smart contracts. The author illustrated significant use cases such as strengthening international aid systems with smart contracts. The author also highlighted the capability of integration of blockchain technology for other services such as finance and taxation. Chiang et al. [136] presented a blockchain and the smart contract integrated system to build the trust between immigrants and the government. The authors introduced ChainGov, a collaborative decentralized platform for immigrants, governments, and other institutions that can inform each collaborative individual about the flow of money as well as real time visibility of all transactions. They also indicate design implications and future directions of the work. Bodo et al. [138] presented a normative analysis of blockchain technology contracts along with the smart contracts and their applicability to copyright law. The extensive features of blockchain technologies including trust and decentralization as well as transparency was highlighted for the compatibility of blockchain with the fundamentals of copyrights. The authors discussed that substantial amount of transactions in the copyright domain could be modeled as if-then rules and eventually into smart contracts. Gheorghe et al. [137] presented the blockchain technology and its application for the governance of the music industry along with smart contracts and cryptocurrency. The authors highlighted the applicability of smart contracts for terms and conditions in music industry. In addition to that, the smart contract and its application for tracking the copyrights of digital content and its value discussed.

#### 3.5.4. *National democracy*

Voting is an important event in any democratic nation which requires the participation of every civilian. The election and counting process are computerized in some countries. Still, there are technical hurdles in implementation of entirely electronic voting systems in some countries. The reliability is a primary requirement in the voting systems along with the on-demand auditing and compliance assessment requirement. Furthermore, the scalability is a key requirement with ensured service availability. The data privacy and access control are also mandatory features in the electronic voting systems. However, there are some limitations in the service values in existing centralized voting systems. The data access control in the centralized systems prone the into security risks. The alteration of the number of votes will raise serious political issues in the country. The scalability limitations may occur since the number of concurrent voters may increase upto few thousands in peak time. The blockchain based smart contracts provide an extensive value addition in the electronic voting systems by ensuring decentralization, transparency and eliminating a single point of failure.

Garg et al. [139] presented an empirical review comparative analysis of the electronic voting systems based on blockchain. Ayed [140] proposed a blockchain based electronic voting system which ensures authentication, anonymity, accuracy, and verifiability. The solution connected to a database of regis-

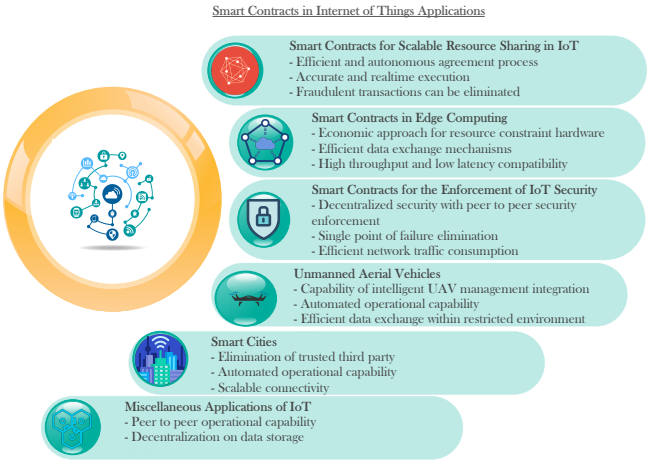


Figure 6: Smart Contract Applications in Internet of Things

tered voters and the committed vote stored in the blockchain to ensure anonymity and privacy. McCorry et al. [141] proposed Open Vote Network which ensures voter privacy using Ethereum for board room voting. The proposed system was tested on the public Ethereum network utilizing e-voting smart contracts. The voting operation incurs financial cost due to the blockchain network charge by the Ethereum public blockchain. Patidar et al. [142] proposed electronic voting system based on blockchain. The implementation was performed using Ethereum blockchain.

### *3.6. Internet of Things*

Internet of Things (IoT) is one of the hottest research areas in the recent ear of computer networking history. It is anticipated that billions of devices will be connected in future industries. Many new requirements are identified in different dimensions to facilitate these IoTs. The automation is an essential requirement with the IoT devices in future networks. Improvement of security is also challenging. The requirement of autonomous resource sharing will be a key feature of the next-generation autonomous systems. Blockchain based smart contracts will address many of these challenges in the future IoT systems with its in-built automated and decentralized nature. Smart contracts can be applied to fulfill many security requirements of IoT context. Fotiou et al.[143] illustrated the opportunities and challenges of the smart contracts for the Internet of Things. Figure 6 illustrates the applications of the smart contracts in IoT context. Table 10 summarizes the applications of smart contracts in the Internet of Things context along with the benefits and challenges.

#### *3.6.1. Smart Contracts for Scalable Resource Sharing of IoT*

Resource sharing is a significant requirement in the IoT network. The resource restrictive infrastructure arises the necessity of optimal resource sharing service. The resource sharing service should not be a resource intensive process. If so, the resource sharing process will incur another overhead on the system. The cloud-based resource sharing mechanism will incur additional network traffic and computational cost. The smart contracts will enable peer to peer resource sharing which is optimal in computation-wise as well as in the network traffic. Thus, smart contracts can be the next-generation resource sharing approach in the IoT context.

Wright et al. [144] introduced SmartEdge, Ethereum based smart contracts for the edge computing as a low-cost and low-overhead tool for compute-resource management. The smart contract consists with five different states for transition within its lifetime. The solution offloads the computation in verifiable manner. Zyılmaz et al. [145] described a fault tolerant standardized IoT infrastructure with distributed storage service. The data access managed using the trustless blockchain. The authors used swarm as distributed data storage and Ethereum as the blockchain platform. Liu et al. [146] proposed a blockchain-based framework for video streaming with mobile edge computing with adaptive block size for video streaming for mobile edge computing. The authors designed a customized incentive mechanism to facilitate the members including content creators, video transcoders and consumers. The details corresponding to the incentive mechanism encoded as a smart contract. Huang et al. [147] proposed a decentralized blockchain based solution of trusted IoT data exchange. The authors developed a prototype which can record transactions in an auditable, transparent and immutable manner. The prototype developed using Ethereum blockchain.

#### *3.6.2. Smart contracts in Edge computing*

Edge computing enriches the IoT systems in the restricted environment. The Edge nodes associated with IoT systems are capable of being offloaded with computationally expensive operations of IoT into themselves. In contrast with cloud computing, edge computing promises more resource economic operations. The centralized architecture of cloud computing generates more network traffic and contains latency. The blockchchain and smart contracts which operate in a decentralized architecture fit into the Edge computing context for future IoT systems. The peer to peer connectivity eliminates extensive network traffic and latency. The throughput can be increased with the deployment of blockchain based smart contracts with Edge computing deployment model.

Xiong et al. [148] introduced an economic approach empowered with a novel concept of edge computing for mobile blockchain. The authors pointed out that multiple access mobile edge computing is regarded as an auspicious solution to solve the proof-of-work puzzles for mobile users. The authors used Ethereum blockchain platform for the prototype system developed. Stanciu [149] presented ongoing research on application of blockchain based smart contracts for the platform of hierarchical and distributed control systems adopted to IEC 61499 standard. The author used Hyperledger Fabric as the blockchain solution and the smart contracts were used to implement the function blocks. The system adopted microservices architecture with utilization of docker and kubernetes. Yang

et al.[150] proposed a data exchange prototype for smart toys, which empowered with modern edge computing technologies. The solution developed as a prototype of Hyperledger Fabric v1.0. The authors used the smart contract to ensure the data exchange mechanism is efficient, secure and reliable.

Samaniego and Deters [151] presented a novel idea which proposed to encapsulate the features of blockchain, including smart contracts in software-defined components and distribute them towards edge devices. The smart contracts are deployed in deices called edge miners. The solution is ideal for the computational resource constrained environment. Xu et al. [152] proposed a blockchain based service provisioning mechanism for the protection of lightweight clients, such as the resource constrained IoT devices. The authors proposed to utilize the smart contracts to help the lightweight IoT clients to validate the acquired services and corresponding edge servers which will reduce the computational overheads for the IoT devices. The authors ensured high throughput and low latency by adopting efficient permissioned blockchain with the consensus engine which uses proof of authority. Ioni et al. [153] proposed a blockchain container based architecture which is aligned with W3C-Prov data model. The used Hyperledger Fabric as the blockchain platform. The significant activities such as the node joining, identity check and record provenance are implemented as smart contracts with the support of Hyperledger Composer.

#### *3.6.3. **Smart contracts for the enforcement of IoT security***

Security is a crucial requirement in the IoT context. With the resource restricted hardware, it is extremely hard to enforce security by increasing the key sizes with multiple cryptographic operations. The devices are constrained in the form of computational power as well as memory. Hence utilization of public-key certificates will be an expensive operation to the IoT devices. The PKI systems may require verification through the requests sent to the cloud servers which will generate the network traffic. The access control and privilege definition on the centralized servers will be vulnerable. Overall, the blockchain enables the stakeholders to embed access control policy on the smart contracts and deploy in a decentralized manner. The code is immutable and free of being modified in contrast with the cloud computing environment. The decentralized operation ensures that no extensive network traffic will be generated when the security is being enforced.

The trust management of IoT ecosystem is vital security consideration. The mission critical application contexts such as healthcare, smart cities, and vehicular networks require high end trust establishment for the IoT nodes in operation. The trust management includes the different services such as the trust establishment, realtime trust assessment, trust withdrawal upon the malicious practices and so on. The future IoT infrastructure will connect billions of devices in realtime and the trust management frameworks expected to scale up aligning the massive connectivity requirement. The centralized trust management is challenging with the future demand expectations. In addition to that, the computational resource restrictions shift the highlevel IoT infrastructure design decisions towards decentralized architectures such as edge and fog computing based designs. The distinguishing features of the blockchain based smart contracts promise significant value additions to the classical trust architecture, addressing the limitations of classical trust ecosystems in IoT.

Fortino et al.[154]initially proposed a method to measure trust of the automated guided vehicles in the smart factories and elaborated with a design of framework to exploit the measures for the formation of virtual, temporary and trust-based teams for the mobile intelligent devices. The included comprehensive experimental results which proves the efficiency and effectiveness optimization capability to improve the performance of the workshops. [155] introduced a reputation capital model for the multi-agent systems and integrated blockchain technology to certify the reputation capital of each agent in each federated environment. The comprehensive experimental results prove the usability of the proposed model to detect the misleading agents. [156] presented a reputation model with blockchain technology for grouping the agents in IoT. The reputation capital related operations, including the update of reputation capital managed through the smart contracts.

Dorri et al. [157] highlighted the significance of blockchain to overcome the security and privacy challenges of IoT. The authors stated that the resource intensive consensus operations of existing blockchain platforms are incompatible in the IoT context. The authors proposed a lightweight and scalable blockchain for IoT which utilized a distributed trust method instead of solving a puzzle in consensus. Yu et al. [158] illustrated that the IoT devices and data will be a trading capable commodity in near future and the infeasibility of the centralized trading platform for such a requirement. The authors stated that the blockchain based smart contracts will eradicate the requirement of the trusted third party. The authors demonstrated the establishment of trust by smart contracts and blockchain to enable end to end trading. Khan and Khaled [159] presented a survey on major security issues of IoT layered architecture. The authors outlined the security requirements for IoT as well as the existing threats, attacks along with the state-of-the-art solutions. The authors highlighted that the blockchain technology is a key enabler to solve many IoT security problems.

Lin et al. [160] proposed a blockchain based conceptual architecture and design to establish trust of the private LoRaWAN network servers. The proposed solution provides an irrefutable mechanism which verifies that the data of a transaction existed at a specific time in the network. The authors also stated the capability of smart contract technology to define an automated trading model in the IoT network. Pan et. al [161] designed and implemented a prototype named “EdgeChain”, which is an edge-IoT framework based on blockchain based smart contracts. The authors integrated a permissioned blockchain along with an internal currency system to link the edge cloud resource pool for each IoT device attached with account and resource usage. From the experiments and evaluation the authors highlighted that integrating EdgeChain is within the reasonable and acceptable range to gain the security benefits. Cha et. al [162] proposed the blockchain connected gateways to the protection of users from sending personal data to IoT devices without the users’ consent. The gateways proposed by them also store user

privacy preference on IoT devices within the blockchain network. The solution contributed to improving privacy and trust in IoT applications with legacy IoT devices.

Salahuddin et al. [163] proposed an agile softwarized infrastructure for IoT with secure and privacy preserving deployment in smart healthcare services with significant features such as enhanced security and virtualization techniques. The system employs smart contracts for seamless and transparent transfer of patient information from machine to machine. The authors have suggested that the integration of legal contracts as part of the deployed smart contracts can be used for proper enforcement and to control misbehaving members. Rantos et al. [164] proposed a blockchain integrated framework named "Advocate" which facilitates the GDPR-compliant personal data on the IoT environment. The smart contracts have been utilized to define the rules and penalties as well as automatically enforce the obligations. As future work, the authors plan to develop a policy-based access control system for the integrated personal data management system in IoT. Pinno et al. [165] presented a blockchain based architecture for IoT access authorization named as "ControlChain". The authors stated that the architecture is user transparent, decentralized as well as scalable and fault tolerant. The authors divided the database of ControlChain into 4 different blockchains and illustrated clearly. The authors also provided a secure way to establish the relationship between users and devices. Liu et al. [166] presented a blockchain-based data integrity service framework. The data integrity verification protocols were implemented as smart contracts in the Ethereum blockchain operated in the private mode. The framework has few advantages including enhanced reliability with decentralization, improved efficiency with multiple operating clients along with data trading capability.

Rathore et al. [167] presented blockchain based secure architecture in the IoT context. Alphand et al. [168] presented IoTChain, an improved blockchain based security architecture with key management and distribution framework. The system was implemented on Ethereum blockchain operated on the private mode. The resource owner describes the access rights in the smart contract, which will generate access tokens to the clients when the certain conditions have been met. Nagothu et al. [169] proposed a smart surveillance system with smart contract based access control system. The decentralized security mechanism was deployed to protect and synchronize data of the communication channel. The permissions on the data access enforced utilizing the smart contracts. Polyzos et al. [170] explored the potential of a blockchain assisted information distribution system for the IoT, along with the enforcement of the key security requirements using blockchain based smart contracts. The authors stated the contribution of blockchain based smart contracts to the sustainability of the IoT system and the enablements of new trust models. The proposed system designed for compatible with Ethereum client side architecture. Roy et al. [171] presents a secure transaction framework in association with the blockchain for the IoT QoS.

#### *3.6.4.* ***Unmanned Aerial Vehicles (UAV)***

The research and development of UAV evolved with a lot of strengths which are versatile and applicable in the future industries. UAVs can be utilized to complete tedious tasks that are risky and expensive to being fulfilled with humans. The operational accuracy is highly anticipated in UAVs intervention and efficient resource consumption is highly concerned. Especially the battery life is one the major concern in the UAVs. In addition to that, scalability is required in future UAV systems. The blockchain based smart contracts will enable decentralized and peer to peer operation of UAVs which will enhance efficiency and performance.

Mehta et al. [172] presented a comprehensive survey on the security issues of 5G enabled UAVs with a taxonomy in 5G-enabled UAV networks. Kapitonov et al. [173] presented the organization of a communication system between agents in peer-to-peer network with decentralized Ethereum blockchain based smart contracts for UAV. Their previously developed project AIRA (autonomous intelligent robot agent) takes care of the formalization of interaction and data exchange between robotic networks including UAV and smart contracts. The system uses its own token within the network as well as from the Ethereum network. Sharma et al. [174] presented the application of blockchain for drones which act as on-demand nodes for inter-service operability between multiple vendors. The drone smart contract includes the rules for initiating and regulating transactions between drones and the vendors. The features and threat implications of blockchain based smart contract based drones were also illustrated.

#### *3.6.5.* ***Smart cities***

Smart cities are one of major IoT innovations which will use in future town and country infrastructure development. Smart cities are anticipated to improve the quality of life. The enthusiasts have a lot of inspirations on significant contexts including entertainment, casinos, integrations with smart vehicles and so on. Since the smart cities consist of thousands of connected devices, the scalability of the operating platforms is a major anticipation. In addition to that, centralization will incur significant overheads with additional risks.

Smart contracts and blockchain will play a vital role in the future of smart cities. The operational capability of the smart contracts on the decentralized model will add more value with guaranteed service availability. The peer to peer operational capability of smart contracts will reduce the network resource consumption and improve the efficiency along with latency.

Yang et al. [175] proposed a framework of decentralized, secure and privacy-preserving eGovernment system for smart cities which utilizes the blockchain technology. The authors discussed the capability of application of smart contracts as a replacement of real contracts. The authors highlighted the adaptation capability of Ethereum platform as an open source blockchain solution. Liao et al. [176] illustrated the design and applications of future 5G wireless micro operators in casinos and other entertainment applications in future smart cities. The utilization of smart contracts in different use cases including Mega Jackpot. The authors introduced the concept of

Value Network Configuration model to illustrate the smart contract interoperability within devices, micro operator and service providers. Lazaroiu and Roscia [177] designed a smart district model which is a mandatory step to build a smart city incorporating new technologies and the role of energy management system integrated into a blockchain and IoT based platform. The setup utilized smart contracts for autonomous distributed power grid management by the local community along with the smart meter technology. The authors highlighted the blockchain technology as a key element for increased cost competitiveness for the rapid deployment of the smart city.

Leiding et al. [178] proposed to combine the vehicular ad-hoc network with Ethereum blockchain to enable the system with transparent, self-managed and decentralized. Each network entity, such as Road Side Unit(RSU), Application Unit (AU) or On-Boarding Unit (OBU) will identify with the Ethereum address. They stated the advantage of Ethereum's solidity programming language's Turing completeness to provide wider services including traffic jam updates and weather forecast. Sun et al. [179] proposed a conceptual framework including three important dimensions as human, technology and organization with fundamental factors for the smart city with sharing economy perspective as well as the application of the blockchain in the smart cities. The authors discussed the applicability of smart contracts in the shared economy. The authors highlighted the trust model based on blockchain based smart contracts will democratize the relationship between human and organization. Sharma et. al [180] proposed a vehicle network architecture based on blockchain in the smart city. The authors illustrated the application of the smart contract to commit autonomous payments. They expected to incorporate blockchain and wearable technologies as future work.

Sharma et al. [181] proposed a blockchain-based distributed framework for the automotive industry which will consist of autonomous and connected cars in the smart city. The authors applied smart contracts in significant phases of the vehicle lifecycle including registration, leasing, certification etc. The authors successfully performed a simulation with Ethereum blockchain platform in the private mode and the results conveyed that the proposed approach is effective and feasible to build a sustainable automotive ecosystem for the smart cities. Su et al. [182] proposed a contract based energy blockchain for the electric vehicle charging the smart community. The authors utilized smart contracts to implement the secure charging services once the valid trading conditions met and for the required cryptocurrency exchanges. The optimal contracts are analysed and designed to align with the customized EV(Electric Vehicle)'s individual energy requirements based on the contract theory.

#### *3.6.6. **Miscellaneous applications of IoT***

Internet of Things is one of the most promising technology enablers in the future industrial domain. There is a lot of research in progress by the academia and industry in multiple aspects of the IoT context. Most of the architectural designs are being adopted with decentralization and the peer to peer operational capability. The efficient resource consumption is highly anticipated and it is hard to yield significant efficiency when the devices are operating in a centralized architecture. The blockchain based smart contracts will resolve most of the issues associated with the centralization and adding a lot of value additions to the implementation. The IoT data sharing is a significant requirement in the different application contexts. The data sharing techniques expected to enforce access control and encryption techniques to protect the data over transit. The computational resource restrictions of IoT make the data sharing techniques challenging with different limitations. Niya et al. [183] proposed monitoring system integrated with Ethereum blockchain and LORA (LOngRAnge) technology. The authors used the blockchain to store and retrieve the data generated by the sensors. The authors utilized Ethereum lightweight client which only stores and synchronized the current transactions. Feng et al. [184] implemented a consortium chain-based outsourcing feature extraction scheme over encrypted images integrated with smart contracts and several other techniques in the device to device communication. The authors utilized smart contracts to transmission of the encrypted images. The authors utilized Hyperledger Fabric as the platform for smart contracts. Biswas et al. [185] proposed a security framework which integrates the blockchain technology with smart devices and provides a secure communication platform in the smart city. The authors highlighted the applicability of Ethereum smart contracts to enable the peer to peer functionality. The authors also stated that the integration of existing communication protocols with blockchain is challenging. Bahga et al. [186] presented a decentralized peer-to-peer platform named as BPIIoT for industrial internet of things which enables distributed applications for manufacturing. The platform enhances existing platforms in different dimensions such as enabling consumer-to-machine and machine-to-machine transactions without a trusted intermediary. The implementation was integrated with Arduino Uno and Ethereum platform in private mode. Ibba et al. [187] proposed CitySense, a blockchain based solution to solve the data storage and management. The authors applied smart contracts to enable the management sensor information and control logic. The authors used SCRUM methodology in development of the required software in the implementation.

Manzoor et al. [188] presented blockchain based proxy re-encryption scheme which stores the data in cloud without intervention of a third party. The system established a smart contract for the data users to control the access to the data. The proposed scheme evaluated using the Ethereum blockchain platform. Tharaka et al. [189] presented a blockchain based lightweight certificate management framework for 5G IoT. The proposed system utilized the smart contracts for threat scoring and revocation of the certificates of malicious IoT nodes. The system evaluated using Hyperledger Fabric blockchain platform. Some futuristic insights on the role of blockchain in 6G presented in [190].

| Application | Key challenges | Blockchain features | | | | | Key benefits |
|---|---|---|---|---|---|---|---|
| | | Decentralization | Forge resistance | Transparency | Autonomous execution | Accuracy | |
| Smart Contracts for Scalable Resource Sharing in IoT: [144], [145], [146], [147] | Resource intensive centralized operations | ✓ | | | | | • Decentralized service availability<br>• Peer to peer scalable operations<br>• Accurate agreements |
| | Lightweight cryptographic operations are vulnerable | ✓ | | | | | |
| | Scalability limitations | ✓ | | ✓ | | ✓ | |
| | Manual access control strategies are hard | ✓ | ✓ | ✓ | | ✓ | |
| Smart Contracts in Edge Computing: [148], [149], [150], [151], [152], [153] | Security risks for data in cloud | ✓ | | ✓ | | ✓ | • Improved perimeter security<br>• Reduced attack risk<br>• High throughput |
| | High risks in data transit over cloud | ✓ | | | | | |
| | Performance limitations | ✓ | | | | | |
| | Data access control limitations | ✓ | ✓ | | | ✓ | |
| Smart Contracts for IoT Security:[157], [158], [160], [161], [162], [163], [164], [165], [166], [168], [169], [170], [154], [155], [156] | Computational resource limitations | ✓ | | | ✓ | ✓ | • Decentralized security policy<br>• Efficient network consumption<br>• Scalability limitations |
| | Network traffic generated from eneromous number of nodes | ✓ | ✓ | ✓ | ✓ | ✓ | |
| | Scalable trust establishment | ✓ | ✓ | ✓ | | | |
| | Higher resource consumption for cryptographic operations | ✓ | ✓ | | ✓ | | |
| Unmanned Aerial Vehicles:[173], [174], [172] | Computational resource limitations | ✓ | ✓ | | ✓ | ✓ | • Guaranteed service availability<br>• Decentralization<br>• Optimal network resource consumption |
| | Concurrency requirements of UAV | ✓ | | ✓ | ✓ | | |
| | Higher throughput | ✓ | | | | | |
| | Central point of failure | ✓ | | | | | |
| Smart Cities:[175], [176], [177], [178], [179], [180], [181] | Computational resource limitations | ✓ | | ✓ | ✓ | | • Decentralized service availability<br>• Eliminated trusted third party<br>• Efficient network usage |
| | Throughput limitations | ✓ | | | | | |
| | Higher scalability requirements | ✓ | | | | | |
| | Higher data consumption | ✓ | | | ✓ | | |

Table 10: Summary of Applications of Smart Contracts in Internet of Things Context

### 3.7. Telecommunication Services

The telecommunication industry plays a vital role in almost all of the nations in the world. The customer volume inflated and the complexity of the services widened with the development. For the conformance of current and future demands, the network infrastructure and software modules require upgrading. The blockchain based smart contracts invigorate the telecommunication industry in different dimensions. The enhanced trust, autonomous execution of blockchain based smart contracts ensure security as well as scalability which is a mandatory requirement in modern telecommunication systems. Table 11 summarizes the applications of smart contracts in the telecommunication context along with the benefits and challenges.

#### 3.7.1. ***Autonomous and intelligent resource sharing in telecommunication***

The subscribers of telecommunication services are proliferating with the expansive utilization of mobile devices around the world. The sophistication of services emerges the complexity in different aspects of the telecommunication domain. The restricted resources in telecommunication required to allocate and utilize in a paradigmatic manner[191]. Furthermore, the subscriber-user agreements with their complexities must compatible with scalability requirements with future elastic demands. The blockchain based smart contracts are ideal solutions for the autonomous secure execution of service level agreements as per the customized subscriber need with scalability. There are many feasible use cases identifiable in the blockchain based smart contracts for optimal and accurate resource sharing in the telecommunication industry.

Raju et al. [192] proposed to use blockchain based spectrum exchange and smart contracts to implement elastic handoff, which is a composition of conventional cellular and voluntary spectrum handoffs. The authors proposed to enforce user and network accountability via smart contracts. The interactions between different components such as cognitive cellular users, cognitive cellular users and cognitive cellular networks and so on. Pascale et al. [193] proposed adoption of smart contracts to implement simple and effective service level agreement between small cell providers and mobile operators. The authors presented example contract based on Ethereum blockchain. They declared it as a smart contract as a service to individual users and retail venues. Backman et al. [194] presented blockchain slice leasing ledger concept with an analysis with its future application. The network slice trading is performed in the blockchain and its smart contracts order slice orchestration from slice broker autonomously. The next phase of the presented research will focus on the evaluation of slice leasing ledger from business, policy and legal perspectives. Valtanen et al. [195] presented blockchain network slice brokering use case along with value analysis and the results in the industrial automation application scenario. The authors applied the proposed resource configuration framework against blockchain based smart contract characteristics and capabilities to assess the use case value. The use case enabled industrial automation process to autonomously and dynamically acquire the slice required for more efficient operations. Fernando et al.[196] proposed a blockchain based wifi offloading platform for 5G. The smart contracts utilized for Wifi service provider rating and offloading decision making.

Yrjölä [197] discussed the unrivalled challenges of onboarding multiple stakeholders in future 6G ecosystem. A decentralized resource configuration prototype was proposed based on blockchain based smart contracts. The proposed prototype offered full autonomous resource configuration via blockchain as the resource orchestrator, which eliminated centralized resource orchestrator. Dai et al. [198] proposed a combination of blockchain and AI for resource sharing in the wireless networks. The proposed architecture provides services on resource management, flexibility in networking, and orchestration. The authors further proposed secure content caching environment utilized with advanced deep reinforcement learning to design caching scheme. Nag et al. [199] presented a comprehensive discussion on the security issues in the management of virtual network functions in the optical 5G networks. The work presented a high-level overview on the application of blockchain to eliminate the identified issues.

#### 3.7.2. ***User identity management and access control with smart contracts***

Identity management and access control is a significant security requirement in the telecommunication industry. The identity management system must be capable to coping with the futurstic demand inflations of the telecommunication industry. The identity theft is required to eliminate and essentially the service availability should be ensured. Blockchain based smart contracts already being adopted in multiple industries for access control. The telecommunication industry can empower with the blockchain based smart contracts for access control implementation. Furthermore, the decentralized nature will ensure the service availability with ensured scalability.

Raju et al. [200] proposed a privacy-enhancing user identity management system incorporated with blockchain based smart contracts. The two main purposes of the smart contracts are the enforcement of privacy compliance between cognitive cellular user and identity and credibility service and establishment of service level agreement between cognitive cellular user and cognitive cellular network. The experiments with the proposed system carried out on Ethereum blockchain on the private mode. Pop et al. [201] proposed augmentation of the protocol stack including application, transport, network, MAC and physical layer with the semantic plane, which provides a common interface for the users, actuators, sensors in one side as well as the protocol stack on the other side. The smart contracts were applied to control the access of physical resources in association of smart locks and application level aggregation of distributed ledger transactions. The key concerns were to reduce the overhead by incorporating smart contracts.

| Application | Key challenges | Blockchain features | | | | | Key benefits |
|---|---|---|---|---|---|---|---|
| | | Decentralization | Forge resistance | Transparency | Autonomous execution | Accuracy | |
| Automated Resource Sharing in Telecommunication: [192], [193], [194], [195], [197] | Centralization and single point of failure | ✓ | | | | | • Decentralized and efficient service availability<br>• Autonomous agreement<br>• Improved trust and scalability |
| | Operational overheads | ✓ | | | ✓ | | |
| | Manual agreements are slower | ✓ | ✓ | | ✓ | ✓ | |
| | Fraudulent transactions cannot track | ✓ | | ✓ | ✓ | | |
| Identity Management:[200], [201], [202] | Centralization and single point of failure | ✓ | | | | | • Decentralization<br>•Access control to data<br>• Reduced overheads |
| | Administrative overheads | ✓ | ✓ | ✓ | | | |
| | Data redundancy | ✓ | | | | | |
| | Data privacy issues | | | | ✓ | ✓ | |
| Roaming Services:[203], [204] | Fraudulent activities in roaming | ✓ | ✓ | ✓ | ✓ | ✓ | • Decentralized agreements<br>• Policy immutability<br>• Frauds can be identified<br>• Transparency |
| | Centralization and single point of failure | ✓ | | | | | |
| | Service unavailability | ✓ | | | ✓ | ✓ | |

Table 11: Summary of Applications of Smart Contracts in Telecommunications Context

Ling et al. [202] proposed a blockchain radio access network architecture which manages network access and authentication in a decentralized, secure and efficient mechanism among inherently trustless network entities. The authors applied smart contracts in multiple scenarios such as user equipment and host access point agreements on the terms of payments and digitization of spectrum assets. The authors also enforce the privacy protection as an additional term to the smart contract and highlighted the latency reduction and scalability requirement of the blockchain.

#### *3.7.3. **Smart contracts for roaming services***

Roaming is defined as the capability of accessing services offered by the telecommunication service provider outside the geographical area of coverage. The services include voice calls, SMS, data connectivity and so on. Preferebly the service charges should be lower than the remote call charges from the tenant's current geographical region. The smart contracts applicable to address some issues associated with roaming and related services.

Yrjölä [203] identified the impact of the blockchain technology in spectrum sharing concepts using the Citizens Broadband Radio Service (CBRS) concept as an example. The author suggested that the rules and agreements between the various asset providing networks can encode as smart contracts. The benefits of Inter-operator roaming connecting CBRS network by eliminating third-party clearinghouse by smart contracts was highlighted. Duru and Muhammad[204] emphasized the application of blockchain based smart contracts to fulfill the roaming requirements in maritime industry. The authors highlighted that there should be a global enterprise blockchain with governance is required for the success of future utilzation of blockchain including roaming. The authors highlighted of the establishment of policies and standards.

### *3.8. Logistics Management*

The logistics and supply chain industry complexified due to diversified customer requirements. The global production regulated according to the economic advantages and most of the countries contribute to import and export trade. The air and sea cargo are divers from the break bulk to commodities such as live crabs, fresh vegetables etc. When the commodities remodeled, the storage requirements and environmental condition in delivery, storage has become a vital consideration. The consumers usually focus whether the specific commodity delivered to the shelf within the required conditions such as regulatory requirements. Ensuring the delivery of commodities within the recommended conditions is a major challenge in logistics and supply chain. The smart contracts and blockchain technology promised to solve many problems with its distributed and autonomous executory nature. Table 12 summarizes the applications of smart contracts in the logistics management context along with the benefits and challenges.

#### *3.8.1. **Ensuring sea/air freight supply chain quality and compliance***

Supply chain compliance is a major concern in certain commodities such as edible items including vegetables, fruits and live crab. The standards established by organizations such as Marine Stewardship Council. The authorities execute robust audits to ensure that the certified seafood stakeholders ensure the standards. The extensive cost and effort could be eliminated by enabling smart contracts to takeover the required actions within the supply chain. For an instance, the specific conditions required to be met for a valid transfer of the custodian of seafood defined by the regulatory authorities and incorporate them as a smart contract. If so, the authorities can make sure the custodian transfers will be executed once the conditions defined by the regulatory authorities met. Therefore the requirement of the explicit audit eliminated. The smart contract, as an immutable program of conditions will ensure the transparency of conditional execution.

Wang et al. [205] presented the investigation of the way which will influence the future of supply chain practices and policies with blockchain and smart contracts. The establishment of trust and disintermediation, traceability and visibility of the supply chain, and improved data security identified as the key values added to the supply chain by the blockchain technology and smart contrcts. In addition to that, the socio-economic impact of the supply chain by the blockchain based smart contracts also discussed. Chen et al. [206] proposed the application of blockchain based smart contracts to supply chain quality manage . The authors highlighted that the smart contracts can use plethora of optimization techniques to improve the delivery such as using GPS coordinates and plan the route. They authors also highlighted the significance of confidentiality on the blockchain, which is corresponding to the sensitive business information. Angwei [207] Illustrated the applicability of blockchain based smart contracts to reduce the complexity of supply chain. The automated verification of the business transaction along with the decentralized distributed ledger ensures that all parties have the appropriate privileges on the supply chain. The PoC was developed using Ethereum platform and three smart contracts developed which included committing payments to the relevant parties as required.

| Application | Key challenges | Blockchain features | | | | | Key benefits |
|---|---|---|---|---|---|---|---|
| | | Decentralization | Forge resistance | Transparency | Autonomous execution | Accuracy | |
| Ensuring Sea/Air Freight Supply Chain Quality and Compliance: [205], [206], [207], [208], [209], [210] | Incompliant delivery conditions | | | | ✓ | ✓ | • Transparency of the milestones<br>• Automated and error free tax calculations<br>• Automated auditability |
| | Customers are not aware of compliance alignment | | | ✓ | | | |
| | Auditing of the compliance is cost intensive | ✓ | ✓ | | ✓ | | |
| | Forgery in trade documentation | ✓ | ✓ | ✓ | | | |
| Agricultural Supply Chain Regulatory Compliance: [211], [212], [213] | The suppliers can alter delivery conditions | | | | ✓ | ✓ | • Automated operations of environmental conditions<br>•Transparency<br>• Immutability of smart contract conditions |
| | Ambiguous compliance requirements | | | | ✓ | ✓ | |
| | Customers are unaware of delivery conditions | | | ✓ | | | |
| Special Commodity Supply Chain Tracability: [214],[215] | Fake validation certificates of the gemstones/diamonds | ✓ | ✓ | ✓ | | | • Reduced overheads<br>• Publicly available certificate information<br>• Automated compliance certificate generation |
| | Fake origin manipulations of gems | ✓ | ✓ | | | | |
| | Paper records can be destroyed/misplaced | ✓ | ✓ | ✓ | | ✓ | |

Table 12: Summary of Applications of Smart Contracts in Logistics Context

Yuan and Wang [208] conducted a preliminary study on blockchain based intelligent transportation systems. The authors considered blockchain as one of the secured and trusted architectures for development of parallel transportation management systems. The authors proposed smart contract powered ride sharing service. Nakasumi [209] illustrates the application of blockchain for information sharing and eventually identify double marginalization and information asymmetry, which are significant problems associated in the supply chain. The authors proposed to program the laws and regulations on the blockchain itself and enable data owners to access control on their own data in the supply chain. They also used homomorphic encryption on the data as required and plan to improve transaction search operation on blockchain. Komathy [210] introduced a five-layer framework to incorporate blockchain in cargo shipping along with role based access control methods and data analytics. The solution establishes the secure connectivity between financing stakeholders, banks, IoT, logistics and manufacturing as well as insurance globally in order to view the shipment. The users can view the transactions from anywhere in the world and reduce the delay in real time transactions.

#### *3.8.2. **Agricultural supply chain regulatory compliance***

Organizations such as Food and Agriculture Organization (FAO) by the United Nations(UN) established significant standards to maintain on food supply chain. For an instance, the thermal conditions of the reefer container with vegetables or foods inside should remain aligned to the predefined standards within the delivery in order to prevent development of bacteria and so on. Sometimes, the reefer stevedoring personals should manually adjust the temperature which is a human resource intensive operation. The cost of manual adjustments of the reefer temperature conditions eliminated when the smart contracts incorporated. The conditions established by the regulatory authorities and the accuracy of the temperature conditions guaranteed with the smart contracts.

Ge et al. [211] presents findings from Public Private Partnership programme, blockchain for agrifood, which targeted to derive insights of the implications of blockchain on agrifood, along with PoC on a use case of table grapes from South Africa. The PoC pilot demonstrated that the basic information concerning certificates can store in the blockchain based smart contracts. The authors used Hyperleder Fabric blockchain to develop the prototype system. Green [212] explores potential applications of blockchain to the agri-food market and over different sub domains including food safety. The author highlighted that the obstacles to the connectivity of the real world into the blockchain required to investigate properly. The author elaborated that the government intervention should be elevated in order to have a successful future incorporation of blockchain in the agri-food market. Kim et al. [213] introduced Harvest Network, a theoretical end-to end "farm-to-fork" food traceability solution with the integration of Ethereum platform along with IoT devices exchanging GS1 message standards. The authors proposed to tokenize the agricultural assets into ERC-721 tokens to transfer within the supply chain. The software designed of smart contracts on Ethereum blockchain builds a mesh network to improve food traceability, cost savings and improved efficiency within agricultural supply chain.

#### *3.8.3. **Special commodity supply chain tracability***

The provenance of history of some commodities is highly effective on its monetary value. For instance, gemstones and diamonds are significant examples. Consistent records of the movement from the mine to the showroom ensure that the gem was not altered or the records were not modified in transit. The certificates issued by government authorities are value-additions to the commodity. The decentralized and transparent nature of the blockchain are the ideal fit for the requirement of special commodities track and tracing.

Cartier et al. [214] provides significant insights of the applicability of blockchain based smart contracts to the gemstone, diamond, colored stone and pearl industry. The essential facts of a precious stone, such as geographical location and cutting and polishing specifications required to record in the ledger. When the monetization of precious stones, the business rules can define as the smart contract and the precious stones and asset ownership can transfer once the smart contract conditions met. Gutierrez et al. [215] illustrated Everledger which is a digital global ledger which can utilize to provide transparency for the open market places in the global supply chain. The authenticity of the asset stored among all industry participants. The solution developed with Hyperledger Fabric blockchain platform.

### *3.9. Smart Contracts in Cross Industry*

There are numerous applications in the smart contracts in various industries. The trust, autonomous execution, reliability and accuracy embraced the smart contracts by diverse industries. Significant applications of smart contracts in cross industry discussed. An overview of the smart contract applications in cross industrial applications displayed in Figure 7. Table 13 summarizes the applications of smart contracts in the cross industrial applications along with the benefits and challenges.

#### *3.9.1. **Smart contracts in enforcement of IT security in the industry***

Smart contracts are applicable to enforce the generic IT security standards of the organizations. Essentially, the organizations must ensure their service availability, alignment with the security compliance standards and so on. The organizations maintain the in-house IT security standards by installing firewalls, Intruder Detection Systems and so on. Mostly, the solutions like firewalls are expensive and operate in centralized manner. The distributed architecture of smart contracts can utilize to enforce the organizational security after proper customization. The distributed nature and some other features of the smart contracts ensure the guaranteed operability without any single point of failure. Rodrigues et al. [216] proposed a design to mitigate DDoS attacks applying blockchain technology and smart contracts. The authors used the smart contracts to store the source IP addresses required to block. The proposed architecture can deploy as an additional security measure for

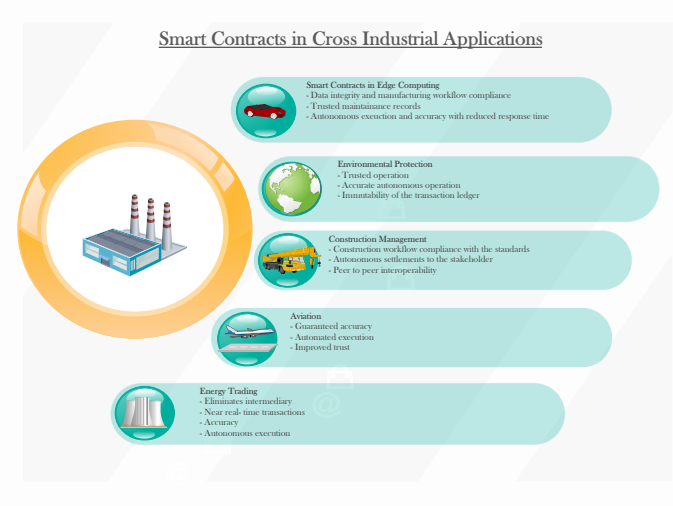


Figure 7: Benefits of Smart Contracts in Cross Industrial Applications

a particular system without interfering with the existing ones. Shao et al. [217] proposed a framework to enable self-adaptive log anomaly detection using the smart contracts.

### *3.9.2. **Smart contracts in energy trading***

The energy industry has significant benefits from the blockchain based smart contracts. The significant features including accuracy, autonomous execution, the peer to peer operations of the smart contracts empowers the energy market to enable peer to peer energy trading, smart metering, efficient renewable energy production, etc. The applications of smart contracts in the smart energy context emphasize the versatility of blockchain based smart contracts for the energy industry.

Pop et al. [218] proposed a blockchain based approach with a distributed ledger to store the energy prosumption information collected from IoT smart metering devices and enforcement of smart contracts to programmatically define the required energy flexibility on the individual prosumer. Furthermore, the smart contracts utilized to define the associated rewards or penalties and the rules required to balance the energy demand with the grid level production. The prototype of the system was implemented on Ethereum. Kounelis et al. [219] presented the conceptual design as well as the energy grid prototype and control layer running on the Ethereum platform. The authors proposed to facilitate the communication between two parties using a middleware application which interconnects the grid with the smart contract. The authors planned to extend more complex functions such as allow the use of coins and automated control of transaction fees from each user. Cutsem et al. [220] presented a blockchain based demand response framework for the smart buildings. Tanaka et al. [221] proposed a blockchain based electricity trading system in association with blockchain based smart contracts. The authors introduced a virtual currency called EnergyCoin to monetize the exchanged energy. The authors also stated the capability of smart contracts which enable micro-transactions between microgrids and further extensible for appliances.

Danzi et al. [222] proposed a Micro Grid(MG) proportional fairness control framework for energy trading using smart contracts. The authors utilized Ethereum blockchain platform operated in the private mode. The authors outlined the mining cost and the communication cost as potential limitations in the private blockchain architecture. Cheng et al. [223] a new transaction framework considering in the existing energy market. The framework is based on the blockchain technology and includes pricing methods, power transaction system architecture and few modules in the energy trading system. The smart contracts were incorporated to enable the system for decentralized trading when there is lack of trust between trading entities. Mangelkamp et al. [224] provides an energy prosumers and consumers a platform to trade local energy without an intermediary. They operate the blockchain in private mode. The real-life applicability and technological limitations were highlighted with their applicability in future research.

Mylrea et al. [225] explored utilization of blockchain based smart contracts in cyber resiliency improvement and enhancement of security in transactive energy applications. The significant benefits of blockchain were highlighted including trustworthiness and convenience in monetization. The application of blockchain which helps to optimize network data and recording residual energy at the substation level was one of the significant features expected of incorporation of smart contracts in the energy applications.Malik [226] developed a blockchain based smart grid for peer to peer energy trading. The performance compared using Ethereum and Hyperledger blockchain platforms.

| Application | Key challenges | Blockchain features | | | | | Key benefits |
|---|---|---|---|---|---|---|---|
| | | Decentralization | Forge resistance | Transparency | Autonomous execution | Accuracy | |
| Energy Trading: [218], [219], [221], [222] | Performance issues associated with centralized architectures | ✓ | ✓ | ✓ | ✓ | ✓ | • Decentralized scalable service availability<br>• Peer to peer operation<br>• Accurate agreements |
| | Scalability issues | ✓ | | | | ✓ | |
| | Security vulnerabilities | | ✓ | | | | |
| | Inefficient resource consumption | ✓ | | | | | |
| Automotive Industry:[227], [228], [229] | Lack of trust on the service records | ✓ | ✓ | ✓ | | | • Decentralized trust<br>•Transparent service records<br>• Interoperability |
| | Service record forgery risk | ✓ | ✓ | ✓ | | | |
| | Future interoperability requirements with smart cities | ✓ | | | | | |
| Environmental Protection: [230], [231], [232] | Scalability limitations due to resource restrictions | ✓ | | | | | • Scalability<br>• Improved accuracy on penalties |
| | Extensive network traffic | ✓ | | | | | |
| | High resource consumption | ✓ | | | | | |
| Construction Management : [233], [234] | Computational and power limitations | ✓ | ✓ | ✓ | ✓ | | • Scalability<br>• Establishment of trust through ledger |
| | Concurrent operational requirements | ✓ | | | ✓ | ✓ | |
| | Higher throughput requirements | ✓ | | | | | |
| Aviation:[235] | Risk of single point of failure | ✓ | | | | | • Autonomous and error free execution of operations<br>• Decentralized system with guaranteed service availability |
| | Perfect security requirements | ✓ | ✓ | | ✓ | ✓ | |
| | Seamless international integration requirements | ✓ | | | | ✓ | |

Table 13: Summary of Applications of Smart Contracts in Cross Industry

#### 3.9.3. *Smart contracts in automotive industry*

The automotive industry is highly focused on the research and development of applicability in new technologies. The key focused contexts include the accurate and compliant manufacturing process, automotive safety, traceability in periodic maintenance records, the immutability of records such as mileage and so on. In addition to that, the automotive safety and interoperability with smart cities also highly concerned in the future of automotive industry. The enthusiasts have a lot of inspirations on the blockchain based smart contracts which enable autonomous accurate execution and operate efficiently in the peer to peer mode.

Dorri et al. [227] proposed a blockchain based architecture for the privacy of the users and elevate the security of the future vehicular ecosystems. The authors presented the capability of blockchain for multiple utilities of the automobile industry including remote software updates, insurance and so on. The authors also discussed possible attack scenarios and the proposed architecture and its capability to mitigate these attacks. Brousmiche et al. [228] proposed a blockchain based smart contract empowered vehicle data and a process ledger framework to streamline the management of vehicle lifecycle and maintenance history. The solution enables transparency and improves collaboration between stakeholders. The smart contracts implemented in Solidity programming language, which is by Ethereum. Bohl et al. [229] reviewed an automotive road safety case study and demonstrated the feasibility of utilizing private blockchains in the automotive industry. The blockchain system utilized for monitoring and logging the behavior of the driver with in association with the map layers, geographical data as well as external rules defined by the local governing body. The significance of the private blockchain highlighted as the faster processing and enhanced data privacy comparing with the public blockchain.

#### 3.9.4. *Smart contracts in environmental protection*

Protection of the environment is a mandatory requirement for the future survival of human. There are numerous research approaches in progress with different avenues to protect the environment, natural resources and so on. The application of blockchain based smart contracts is a distinguishing approach to the future environmental protection context. The researchers expect to utilize the trust, accuracy, and immutability of the smart contracts for the environment protection.

Ongena et al. [230] evaluated the applicability of blockchain based smart contracts to solve problems in waste management. The results indicated the significance of preparation for blockchain based smart contracts for the organization and infrastructure for future waste management. The authors pointed out important problems which can be resolved by blockchain based smart contracts including payments for the weight of waste, wrong information etc. Fu et al. [231] proposed a blockchain-powered environmentally sustainable emission trading framework for the fashion apparel manufacturing industry. The proposed system framework was regarded as a reliable approach to reduce the carbon emission of the fashion apparel manufacturing industry. The immutability, automation, and transparency was regarded as the significant features for blockchain which are applicable for emission trading for the apparel industry. Lin et al. [232] utilized blockchain based smart contracts in association with artificial intelligence for the efficient management of water with climatic changes. The authors utilized the significant features of blockchain including decentralization and immutability to define a public water transaction record. The ultimate objective is to improve the trust and optimization of use on the water related data.

#### 3.9.5. *Smart contracts for construction management*

Construction of infrastructure is an essential requirement of the survival of nation. There are many types of research are in progress to efficient, collaborative, and effective construction and support services management. The important aspects of the construction management including compliance of building materials to the standards, accurate payments to the contractors are incurring administrative overheads to the stakeholders. The blockchain based smart contracts provide a wider scope of applicability to the construction management.

Cardeira [233] proposed possible significant use cases of the smart contracts for the construction sector. The author highlighted that the smart contracts with cryptocurrencies are applicable to develop an efficient method for expediting the payments of the intervening parties. Encryption of funds to enforce the privacy also discussed. Turk et al. [234] presented some insights of the potential of blockchain in construction management. The authors highlighted that the communication patterns between intervening parties are the peer to peer which is aligned with the peer to peer operational modes of blockchain. The requirement of further research into smart contracts for building information management discussed.

#### 3.9.6. *Smart contracts for air traffic management*

Aviation is an essential service that almost all nations of the world contribute. Air traffic management is the most important component of the aviation which incorporates a massive number of operations including flight directions, airport space allocation and so on. The air traffic management operations required to perfectly accurate since the lives on board of passenger aircraft are highly dependent on accurate air traffic management. Therefore, the privacy, availability, workflow compliance and realtime execution are the key requirements in the air traffic management context. The blockchain based smart contracts provide trust and accurate execution with its decentralized architecture. Therefore, the research organizations have a lot of anticipations on the applicability of blockchain based smart contracts for aviation.

Reisman [235] presented an engineering prototype that includes a design and methodology to mitigate Automatic Dependent Surveillance – Broadcast (ADS-B) related security issues using blockchain based smart contracts. The design innovation is using an open-source blockchain platform which is operating in private mode to achieve the privacy and anonymity of the aircraft. The framework featured with a certificate authority and higher-band bandwidth communication channels for shar-

ing private information between authorized parties such as aircraft and authorized members.

## 4. Technical Challenges and Solutions in Smart Contracts

Eventually, the smart contracts consist of computer programs and algorithms. The matters related to the computer programs as well as classical software developement life cycle are applicable to the smart contracts. The validation methodologies which are applicable to evaluate the computer programs and algorithms will be applicable to the smart contracts. In addition to that, there are some significant challenges identified which will leave gaps in the application functionality. These techniques will be focused in detail. The summary of the issues and corresponding solutions summarized in Table 14.

### *4.1. Verification and validation to resolve correctness issues*

The deviated behavior from their functional specifications of smart contracts will be a significant problem in the smart contract applications. The formal verification of a computer program ascertains that the particular program is functioning according to the formal behavior for the defined inputs and proves the correctness. Formal verification exists with two level language principles. The formal verification can perform on the language level and on the bytecode level. From unit testing to application of complex mathematical functions, there is a myriad of techniques utilized in the context. The formal verification of the smart contract is salient with its operational properties. The smart contracts are immutable once they are deployed and cannot patch easily. In addition to that, the smart contracts may hold financial values in different applications and will be accessible for anyone. Therefore, formal verification is paramount in the context of smart contracts.

Bhagavan et al. [236] outlined a framework to analyze and verify runtime safety and functional correctness of smart contracts written for Ethereum in Solidity programming language using F* functional programming language used in program verification. The tool verifies the smart contract in different perspectives including source level functional correctness, low-level properties such as gas consumption bounds and evaluation of the correctness of the output of Solidity compiler on a case-by-case basis applying relational reasoning. The authors assume that the verifier may only have the byte code in the verification. Bigi et al. [237] presented an approach with game theory and combined models of the formal methods for addressing future challenges in decentralized smart contract systems. The authors applied game theory to analyse how the smart contracts are settled through bargaining procedures and formal methods for the protocol validation. The combined analysis formally and quantitatively clarifies the anticipated behaviour of the protocol, which entrusted with a deposit scheme. Sergey et al. [238] outlined the design of Scilla, which is an intermediate level language for smart contracts and provides a clear separation between smart contract communication and programming components with a computational model based on the communicating automata. Their future work consists of defining formal grammar and semantics of language and implementation of Scilla and verifying number of contracts on a real-world blockchain platform. Abdellatif et al. [239] proposed a new formal modeling approach to verify the smart contract in its execution environment. The authors applied this formalism to concrete the smart contract for name registration implemented on Ethereum platform. The authors highlighted vulnerabilities to the smart contracts on the simulated executions and proposed alternative designs to eliminate the vulnerabilities. Nehai et al. [240] proposed modeling method of Ethereum application based smart contracts which apply a formal method named as ModelChecking. The method verifies that the application implementation is compliant with its predefined specification which is formalized by a set of temporal logic propositions. The authors illustrated the approach by applying to a concrete case study from the energy market. Lahiri et al. [241] present the evaluation of safety and security of smart contracts developed in Blockchain-as-a-Service offered by Microsoft via Azure Blockchain workbench. The semantic conformance of smart contracts formalized against a state machine model and developed an automated formal verifier for Solidity. The authors applied their verifier to VERISOL for the analysis of all contracts with Azure Blockchain Workbench.

| Technical challenges | Description | Solutions |
|---|---|---|
| Correctness issues | It is challenging to patch or version update of the smart contracts upon deployment. Therefore, it is essential to verify the behavior of smart contracts within the intended domain of inputs. The correctness issues identified should be fixed before deployment of smart contracts. | • Correctness validation [236],<br>• Formal verification [237], [238], [239], [240], [241] |
| Security vulnerabilities | The security vulnerabilities of smart contracts may expose the entire ecosystem into a massive risk. Especially, when a public blockchain is considered, fixing the security vulnerabilities may require to replace the codes in millions of nodes. In cryptocurrency perspective, the security vulnerabilities may cause losses of millions of dollars. Identification of such vulnerabilities save money, time and safeguards the entire blockchain ecosystem | • Security analysis [242], [243], [244], [245], [246], [247]<br>• Vulnerability identification [248], [249]<br>• Automated security testing [250], [251] , [252]<br>• Symbolic analysis [253]<br>• Security bug identification [254], [255], [256],<br>• Security auditing [257] |
| Software bugs | The software bugs are mainly focused to identify the functionality of smart contracts to fulfill the functional requirements. However, due to the distinguishing nature of smart contracts from the classical software systems, there are different techniques which utilize novel computer science concepts to identify the software bugs. | • Specialized testing frameworks [258]<br>• Automated software testing<br>• AI powered software testing<br>• Improved software practices [259],[260]<br>• Specialized bug detection tools [261], [262] , [263]<br>• Bug classification [48] |
| Data privacy issues | The data privacy is a vital concern in almost all application contexts. The distributed ledger publicly replicates all transaction data according to the principles of blockchain. However, such approach may raise privacy considerations on the transaction data when the transaction data is extremely sensitive. The different privacy and data access control mechanisms expected to be enforce in order to prevent data privacy violations. | • User privacy enforcement [264], [265], [266]<br>• Smart contract privacy enforcement [267], [268]<br>• Secure execution hardware integration [269]<br>• Secure multiparty computation [270], [271] |
| Performance limitations | The performance limitations hinder the applications of blockchain to the real world applications. There are many research conducted to optimize the performance factors, such as increased throughput and reduced latency to reduce the gap between the blockchain and real applications. | • Transaction throughput improvements [272], [273], [274]<br>• Shrading [275] , [276] |

Table 14: Summary of technical challenges and solutions in smart contracts

*4.2. Security vulnerabilities and prevention techniques*

The security vulnerabilities expose the systems into different risks. Since the blockchain systems for the corresponding applications built on computer programs, the security flaws common to computer systems expected to investigate and eliminate for the secure functionality of systems. The re-deployment operations after the fixes of security vulnerabilities are different from traditional software deployment lifecycle and challenging with extensive overheads. Especially, when a particular application integrated with a public blockchain network, the rectification of a fault will be an expensive operation. However, there are different technologies emerged in parallel to the blockchain evolution in order to find the software vulnerabilities of smart contracts.

Atzei et al. [248] analyzed the vulnerabilities of Ethereum platform, which is popular in the industry. The vulnerabilities grouped into three classes according to the level they are introduced, as Solidity, EVM bytecode, or blockchain. The authors highlighted that they expect the non-Turing complete, human readable languages will resolve some of the issues identified in future. Lin et al. [242] discussed the security issues encountered in blockchain and challenges needed to overcome. The significant security issues and challenges included majority attacks in consensus, forking issues as well as scalability issues. The authors also highlighted the role of government to define the corresponding laws for this novel technologies. Manjunath et al. [245] discussed the blockchain domain and focused on the possibilities of blockchain security analysis threat occurrences which is attracted more hackers' threats. The authors highlighted the significance of each issue and their impact. The authors expected that in future this will be resolved.

Parizi et al. [250] provided a comprehensive empirical evaluation on the open source automatic security analysis tools utilized to detect the security vulnerabilities of the Ethereum smart contracts written on Solidity programming language. The authors tested the tools on ten real world smart contracts. The results conveyed that SmartCheck [251] is statistically more effective in automated security testing than other tools evaluated. Tikhomirov et al. [251] proposed SmartCheck, a comprehensive analysis tool which detects the code issues of Ethereum smart contracts. The authors evaluated the tool on a massive dataset of real-world contracts and yielded potentially successful results. They also stated the capability of development of the tool in future directions including improvement of grammar.

Nikolic et al. [253] implemented MAIAN, which employs inter-procedural symbolic analysis and concrete validator to identify real exploits. The tool identifies three main types bugs as suicidial contracts, which can kill by anyone, prodigal contracts, which can send Ether to anyone and greedy contracts which does not allow to get Ether to anyone. The tool evaluated with analysis of one million contracts and flags 34,200 contracts vlunerable spending 10 seconds per contract. Liu et al. [254] presented the tool ReGuard, which are usable to identify reentrency bugs in smart contracts. It is a fuzzy-based analyzer which automatically detects the re-entrency bugs in Ethereum smart contracts. ReGuard iteratively generates random diverse transactions to test the vulnerability.

Jiang et al. [255] presented ContractFuzzer which is a comprehensive fuzzing framework to detect 7 types of vulnerabilities in Ethereum smart contracts. The authors identified few significant types of attacks s such as gasless send and reentrency vulnerability. The authors identified the false negative rate optimized when comparing with other platforms. Luu et al. [256] proposed a symbolic execution tool named as Oyente to find potential security bugs. The tool flagged 8,833 contracts as vulnerable out of the 19,366 including TheDAO bug which led to a 60 million USD loss. Liu et al. [257] proposed a semantic aware security auditing technique called S-gram which are applicable to Ethereum. The authors combined N-gram language modeling as well as lightweight static semantic labelling and to learn statistical regulatories of contract tokens and to capture high-level semantics such as the flow sensitivity of a transaction. The authors stated that S-gram is usable to predict potential vulnerabilities in identify irregular token sequences and possible to optimize existing in-depth analyzers. Brent et al. [246] provided a security analysis framework for Ethereum smart contracts. It provides an analysis pipeline for the conversion of the low-level EVM bytecode into semantic logic relations. The evaluation conveyed that Vandal is fast and robust as well as outperforming leading state-of-art tools with successful analysis of 95 of all 141,000 unique contracts with an average runtime of 4.15 seconds. Suiche [244] presented Prosity, which is a decompiler which generates readable Solidity syntaxes from EVM bytecode. The decompiled contracts can perform with static and dynamic analysis as required.

GRECH et al. [277] classified and identified the gas focused on vulnerabilities found in the Ethereum smart contracts. In addition to that, the authors presented MadMax, which are some static programming analysis techniques usable to detect gas related vulnerabilities with significantly high confidence. The approach included low-level analysis for decompilation in declerative program analysis techniques for higher level analysis which validated with 6.6 million contracts. Wust et al. [249] presented three vulnerabilities affecting Ethereum blockchain network and client. The authors described three vulnerabilities in consensus, block synchronization and block difficulty. The authors also suggested possible countermeasures to prevent the attacks discussed. Tsankov et al.[243] presented Securify, which is a security analyzer for Ethereum smart contract. It is scalable, fully automated and capabile of proving the contract behaviors are safe or unsafe corresponding to a given property and tested with more than 18k contracts. The analysis is a two stepped process which includes a symbolic analysis of contract's dependency graph to extract precise semantic information and checking for the compliance violation patterns. Grishchenko et al.[278] presented a complete small-step semantics of EVM bytecode and formalized a significantly large fragment of EVM using F*, which is a popular programming language used for similar verification programmed proof assistant. The authors also successfully validated it against official Ethereum test suite. The authors further defined number of salient security properties for smart contracts. Otte et al. [279] presented TrustChain, which is a permission-less and tamper proof data structure for the storage of transaction

records. Trustchain included a novel Sybil-resistant algorithm named as NetFlow which can determine the trustworthiness of agents online. The Netflow algo agreed upon higher-level business logic. The framework significantly outperforms Oyente with zero false negatives in their data set. Grishchenko et al. [252] presented EtherTrust which is an automated static analysis tool of EVM bytecode. This supports scalability up to larger contracts. The authors tested the tool with Oyente and observed outperforming results and EtherTrust showed better precision on a benchmark rather than state-of-art solutions. Mossberg et al. [247] introduced an open source dynamic execution framework named Manticore to analyse the binaries of Ethereum smart contracts. The framework provides analysis to find issues including logic bombs. The API provides flexibility to customize the utilization of framework. Mell et al. [280]presented usage of cryptocurrency smart contracts to create a distributed consensus protocol which can produce a stream of trustworthy timestamped public random numbers. The main objective is to eliminate prediction and control attacks. With the smart contracts, no one can change the published values. Popejoy [281] described Pact programming language which is developed for the Kadena blockchain platform. Kadena is a private blockchain platform that consists of the smart contract programming language in a human-readable form. The main feature is the Turing incompleteness which reduces the attack risk with restricted power of smart contracts.

### *4.3. Software bugs and software testing*

The software testing is an essential practice in the software engineering. The quality of software codes and their position with the specification expected to be evaluated prior to the production integration. There are different techniques and tools in the market to identify software bugs and evaluate the quality. However, some research conducted to develop tools and techniques for the quality assurance of smart contracts specifically.

Liao et al. [258] presented a behavior driven development framework for Ethereum smart contracts. The proposed work reduces the testing overheads and make the bug fixing process more convenient. Gao et al. [261] presented SmartEmbed which can be used to identify the clone related bugs in solidity smart contracts. The proposed solution supports identification of bugs in the individual scale as well as large scale. Delmolino et al. [260] documented some important insights from teaching smart contract programming to undergraduate students in the University of Maryland. The authors exposed common errors in designing safe and secure smart contracts. The authors highlighted the importance of fixing these errors in programming. Destefanis et al. [259] presented a study case regarding a smart contract library named as Parity. The problem was due to poor programming practices and 500,000 Ether which is equal to 150M USD freezed in 2017. The authors analyzed the chronology of events and identified that the problem occured due to negiligent programming practices. Wang et al. [262] introduced a methodological approach to identify the non-deterministic payment bugs of the Ethereum smart contracts. The proposed solution implemented as NPCHECKER and tested with 30,000 smart contracts to detect the non-deterministic payment bugs. The tool further developed to detect the known vulnerabilities of Ethereum. Torres et al. [263] proposed OSIRIS which is a framework that combines symbolic execution and tent analysis. The proposed solution evaluated with a significantly large smart contract dataset, which includes 42,108 Ethereum smart contracts to identify the integer bugs. Dingman et al. [48] proposed a formal classification for the known bugs in smart contracts using NIST's bugs framework. The proposed framework introduced two classes as Distributed System Protocol (DSP) and Distributed System Resource Management (DRM).

### *4.4. Privacy issues and enhancement techniques*

The data privacy is a vital concern in almost all applications. The core principles of blockchain include the public decentralized ledger which includes transaction data. However, these public transaction data may raise privacy issues in the perspective of data owners. These privacy requirements need to be addressed carefully without impact on the other features of blockchain, including performance requirements. The data privacy enforcement may reduce the gap between most of the present applications and blockchain for seamless integration.

[282] presented significant insights of different aspects blockchain technology including general data protection regulation and its applicability on blockchain as an enabler for data protection. The authors discussed application of permissioned and permissionless blockchain based smart contracts in association with appropriate data controllers. The authors categorized the two types of solutions in enabling compliance, as integration of different cryptographical functions and private computation schemes without revealing contents of transactions and application of blockchains as decentralized verification machines. Juels et al.[283] illustrated the emergence of the criminal smart contracts which will facilitate to reveal the confidential information. The authors illustrated a few issues including theft of cryptographic keys by criminal smart contracts. Their results highlighted creating policies and technical safeguarding measures against criminal smart contracts to ensure the smart contracts' beneficial objectives.

Kosba et. al[267] presents Hawk, a privacy preserving smart contracts, which dissipated the privacy hurdle encountered in Bitcoin and Ethereum as a currency. The authors propose a framework, which enables a non specialist programmer to write a privacy preserving smart contract. Hawk guarantees on-chain privacy, which cryptographically hides the flow of money and amount from public's view. Niya et al. [264] demonstrated a designing and implementation of a trading application which utilized Ethereum smart contracts. The application is developed with flexibility in requesting user identity directly by the seller and the buyer. The user privacy enhanced with other features such as time and cost. Chatzopoulos et al. [265] proposed a new architecture for the event based spatial crowdsensing tasks in association with the blockchain and technology with user privacy preservation. The architecture utilizes smart contracts to allow crowdsensing service providers to submit their requests, run cost optimal auctions and handle payments.

Liang et al. [266] designed and implemented ProvChain, which is a decentralized architecture for trusted cloud data provenance. Provchain provides significant security features such as tamper-proof provenance and user privacy. The main operational phases are provenance data collection, provenance data storage and provenance data validation which provides tamper-proof records to enable transparency and data accountability in the cloud. Al Bassam et al. [268] presents ChainSpace, which offers privacy friendly extensibility in the smart contract platform. The platform offers higher scalability than the existing platform achieved through sharding across nodes using a novel distributed atomic commit protocol named as S-BAC. It supports auditability and transparency as well. Kalodner et al. [284] presented Arbitrum, which is a cryptocurrency system with smart contracts. Arbitrum's model is compatible for private smart contracts which does not reveal the internal state to the verifiers who involve in the validation of transactions in certain circumstances. Arbitrum incentivizes the parties to agree off-chain on the VM's behavior which means that the Arbitrum miners only required to verify digital signatures without revealing the contract to confirm that parties agreed on VM's behavior.

Zhang et al. [285] presented an authenticated data feed system which is named as Town Crier. Town Crier provides a bridge between smart contracts and existing websites which are commonly trusted for non-blockchain applications. The frontend and hardware backend combined with the solution which is enabled with privacy as required. Cheng et al [286] presented Ekiden, which combines blockchain with trusted execution environment. The authors leveraged a novel architecture which separates the consensus from execution and enabled confidentiality preserving smart contracts in trusted execution environment. The authors planned to extend their work to enable secure multi-party computation in future. Yuan et al. [269] presented ShadowEth, which is a system that leverages a hardware enclave to ensure the confidentiality of smart contracts in public blockchain like Ethereum. The system also ensures integrity and availability. The authors implemented the prototype using Intel SGX on Ethereum network to analyse the security and vulnerability of the system.

Benhamouda et al. [270] presented a method for making Hyperledger Fabric blockchain platform compatible with private data using secure multi-party computation. The protocol implemented utilizing Yao's millionaire's problem and oblivious transfer. The authors associated a helper server, which separates multi-party computation into off-chain. Zyskin et al. [271] presented Enigma which is a computational model based on a highly optimized version of secure multi-party computation named as Enigma which guarantees a verifiable secret-sharing schemes and ensure confidentiality. The authors used a modified distributed hashtable to hold secret-shared data with an external blockchain as the controller of the network to control the access and identity management. The private components of the smart contracts run off-chain on Enigma platform and named as private contracts.

### *4.5. Performance limitations and performance improvement techniques*

The performance factors are essential considerations in the application perspective. The performance requirements of high volume transaction processing are mandatory for applications such as digital payment systems. The transaction verification times for the major blockchain platforms such as Ethereum and Bitcoin hindered the applicability to the retail payments. In contrast, the payment networks such as Visa provides 7000 transactions per second. However, a lot of research in progress to investigate techniques to enhance the performance features of blockchain.

Poon et al. [272] proposed Plasma, which is a framework for incentivized and enforced the execution of smart contracts which is scalable upto billions of state updates per second. The authors proposed to multiparty off-chain channels to hold the transaction state on behalf of others. The smart contracts held in the root chain and the Plasma chain maintains the set of balances in the main chain. Forestier et al. [273] proposed an architecture called blockclique, which shards the transactions in a block graph along multiple threads. A block in a selected thread only includes transactions assigned to this particular thread. The blockclique architecture reaches 10,000 transactions per second and provides protection against a wide range of well-known attacks.

Zamani et al. [275] proposed RapidChain, which is a sharding-based public blockchain protocol with a complete sharding of communication, computation and storage overheads. RapidChain utilizes an optimal consensus algorithm with block pipelining and a novel gossiping protocol for large blocks. The empirical evaluations suggest that RapidChain can process 7,300 transactions per second. Luu et al. [274] proposed Elastico, which is a distributed agreement protocol for permission-less blockchains which enables scalability. The solution automatically parallelizes the computational power for the mining service. The scalability evaluated by extending the number of nodes upto 1600 and focused on significant aspects corresponding to the scalability. Kokoris-Kogias et al. [276] presented OmniLedger, which is a scalable distributed ledger with long term security in permission-less operations. OmniLedger is designed to enhance the scalability up to the Visa payment network being adopted with hybrid consensus and sharding techniques. The authors introduced "trust-but-verify" concept to increase the performance.

## 5. Lessons learned and future work

The previous section discussed the significant technical aspects and features of smart contracts based applications. This section extends that discussion by elaborating learned lessons and future research directions for further improvements. The Figure 8 portraits an overview of the flow of lessons learned and future works.

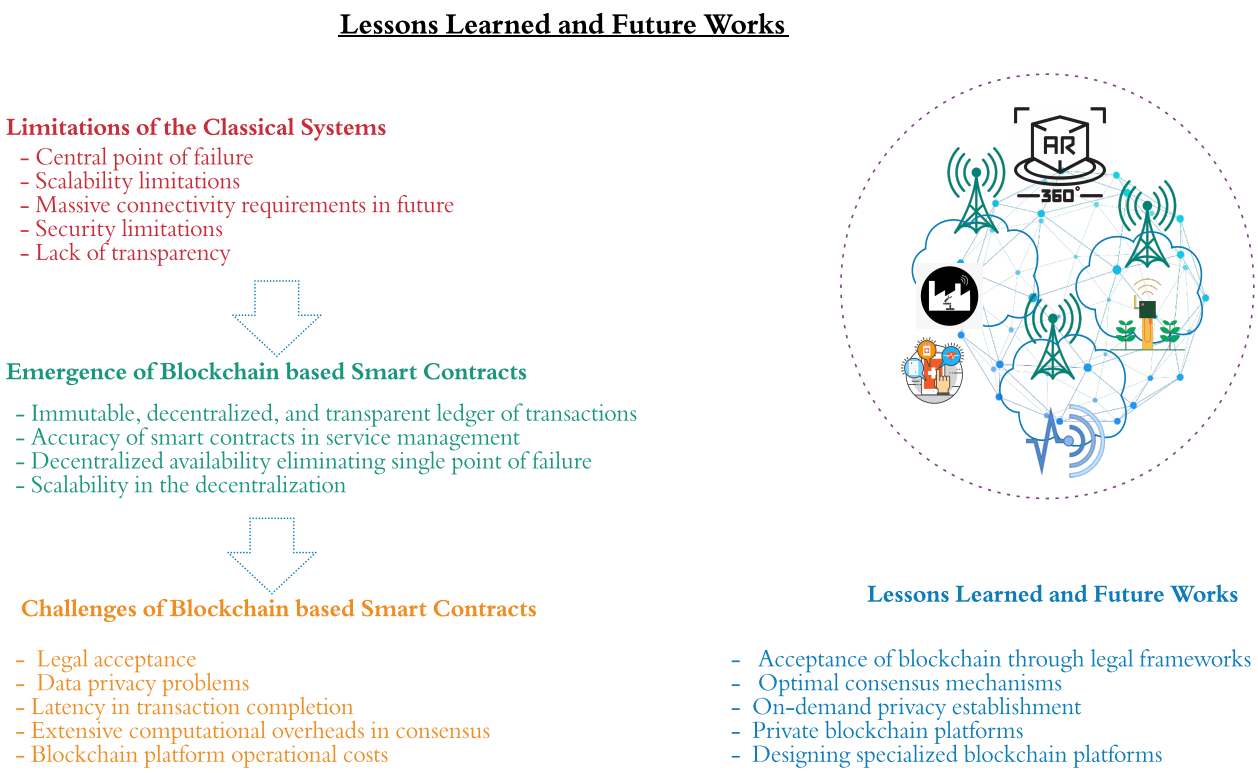


Figure 8: Lessons learned and future work

### 5.1. *Financial Applications*

#### 5.1.1. ***Lessons learned***

Different applications of blockchain based smart contracts in the financial context was discussed previously. However, several aspects of blockchain based smart contracts are still required to be improved further. Governments and governing institutes still do not fully recommend smart contracts for the utilization of fund transfers. The lack of regulating capability in decentralized systems is the main reason for the government bodies reluctant to fully approve the smart contracts in the financial context. Escrow services also have the same decentralization features and still not adopted by the government bodies for International fund transfers. Eventhough the Bitcoin and Ethereum are not fully adopted by the government bodies for fund transfers, the smart contract platforms like Stellar is still working for the fund transfers beyond borders.

It is essential to reduce the transaction processing time if the blockchain is used for retail merchant payments. For instance, Bitcoin and Ethereum take a few minutes for the completion of transactions which is not preferred to experience in the quick merchant transactions. The transaction validation time has to be retained as minimal as possible eventhough the ledger is evolving with the transaction count. It is mandatory to integrate blockchain platform with mobile devices in order to adopt more users. For the merchant retail payment systems with smart contracts, it has to compete with Visa or MasterCard like centralized high-end payment processing systems. Therefore, the further optimization of transaction completion requires to be considered before integrating the smart contracts for financial transactions. However, the smart contracts will be ideal for the financial transaction enablement of closed-loop financial ecosystems such as rural and undeveloped regions.

The decentralized smart contract based KYC systems will be attracted by the future banks as a single customer data sharing platform. However, if the legal policies can be defined to regulate the customer data, the trust of the decentralized KYC systems will be elevated and more customer satisfaction can be anticipated. For the stock exchange, the smart contracts will be an ideal candidate since it enables the autonomous operation. The improvement of the transaction processing time is required for further adaptation.

For lending and borrowing, smart contract systems can play a vital role since lending and borrowing does not require a realtime operation. The autonomous settlement which can be enabled with the smart contracts will be value addition and eliminates fraud. The insurance also will be benefited by the smart contracts by executing the claims autonomously by data inputs and eliminating frauds. The transparency of the transaction records will be advantageous when the auditing procedure of the smart contract integrated systems is considered. The trans-

parency can be a drawback also to the financial context since the transaction records are visible to the public and some customers can be discouraged to share the personal transaction details with the public. The traceability and autonomous execution will make the audit procedure independent and transparent. The main features of the smart contract systems are autonomous execution, elimination of third party intervention and transaction transparency in the financial context.

#### 5.1.2. ***Future work***

The future of financial transactions requires a robust intervention of the governing bodies to regulate the smart contract based financial transactions. Eventhough the decentralized nature preferred by the stakeholders, the government requires to monitor and establish rules and regulate to make the smart contract based financial transactions acceptable by the citizens. The improvements on the consensus anticipated when the smart contracts on board for the financial transactions. The transaction delays such as Bitcoin and Ethereum has required to eliminate if the smart contract based transactions are applying to retail merchant transactions. The computational resource consumption requires to optimize to eliminate the mining overheads in the financial transaction context. The future smart contract based financial systems required to design with formal auditing procedures and compliant with PCI-DSS(Payment Card Industry - Data Security Standards) and PA-DSS(Payment Application- Data Security Standards) standards for global acceptance. However, operating the smart contract based financial systems in a closed loop system such as a village, within an unbanked customer segment will help to identify the drawbacks in the real world operation. These drawbacks required to correct before the operation of smart contract based globally accepted payment systems.

### 5.2. *Healthcare Applications*

#### 5.2.1. ***Lessons learned***

The different applications of smart contracts in the healthcare context discussed previously. The patient data protection and health information management have a lot of inspirations on smart contracts. The access control to the patient data can implement with the smart contracts with decentralization. Elimination of the central point of failure is beneficial for the mission-critical healthcare systems. Health-information management applications with the smart contract incorporation must comply with health data protection standards such as HIPAA. Privacy highly considered in health data management systems. In addition to that, the data integrity of protected data required to ensure utilizing smart contract systems.

The smart contract based data sharing mechanisms must ensure privacy and integrity for the data in transit. The accuracy of the operation of automated patient monitoring and treatment systems required to improve since the smart contract applied with life critical operations. The smart contract developed for healthcare systems must be checked for the bugs, vulnerabilities, and accuracy. The formal verification can utilize to verify the operational accuracy of smart contracts for the healthcare systems. The different aspects of the smart contracts must consider such as the stability of the operations on a load, memory usage on the execution of the contract and so on. The smart contract systems for the future healthcare systems mostly expected to operate on private mode rather than public blockchain operation. The data integrity and immutability of transaction data are the major expectations of smart contracts for the healthcare systems.

#### 5.2.2. ***Future Work***

The future research of smart contracts focused on the improvement of privacy of health information management systems. The compliance with regulations is a major consideration of the incorporation of smart contract systems for healthcare. The privacy improvement along with the transparency requirement of blockchain based smart contracts is an important research direction. The secure data sharing schemes between third party organizations such as insurance companies required to improve the techniques such as oblivious transfer, secret sharing schemes. The next generation healthcare systems require synergestic operation with the services of smart city such as secured data sharing and eGovernment services. The data provenance respect to the sharing of private medical data is achievable with the immutable ledger. Since the accuracy of smart contracts developed for patient monitoring and treatment is highly anticipated, the applicability of formal verification was highlighted previously. The specialized formal verification methods for the healthcare systems are an important research area in the future.

### 5.3. *Identity Management and Access Control*

#### 5.3.1. ***Lessons learned***

Identity management and access control contexts have numerous applications with smart contracts. The data currently stored in centralized systems that have many issues associated. Elimination of the centralization is the main advantage that attracts smart contracts for identity management. The users' capability to control the access of their own data improves trust. The hardware costs for centralized systems such as HSMs can eliminate through the decentralization. However, the incorporation of national identity management systems with smart contracts will require further amendments in the legal systems. The legal systems which recognize the digital signatures and electronic identification are not compatible with decentralized smart contract-based identity management and access control systems. Therefore, the regulatory bodies required to enrich with the operational capabilities, strengths and weaknesses of the smart contract-based access control system and define them legally. Then the smart contract based access control systems are extensible even internationally. The identity data protection solutions empowered with smart contracts require to ensure that they have aligned with local identity management standards. The security policy definitions with the smart contracts are the ideal use cases since through decentralization, the trust can establish. The consensus mechanisms and other dependencies required to be further improved for the efficient operation of identity management systems with smart contracts.

#### 5.3.2. ***Future Work***

The Identity management system will be capable of automated identity management and access control in future. The synergetic operation with PKI based existing identity management systems will eliminate integration and adaptation hurdles. The decentralized identity management and access control systems must ensure the alignment with existing legal requirements in identity data protection. The data privacy must be guaranteed and it may be required to integrate with existing PKI systems which attached with HSMs. The smart contract based identity management systems are extensible as the national identity data repository of citizens. The access can be controlled by the users and the service providers such as banks, telecommunication services, and insurance can retrieve the data from the repository with the data owner's consent. The data usage records must transparently available in the ledger to ensure the data owner that his data was not transferred to third parties such as trade promoters and so on. The identity management systems must interface with the mobile devices which will enhance the usability of decentralized access control systems. The data access policy is a subject to define by the data owners. The consensus and storage systems must design with scalability provisions since the identity management systems will expand along with the number of users.

### 5.4. *Real Estate*

#### 5.4.1. ***Lessons learned***

The main objectives of smart contracts in the real estate domain are to eliminate the trusted third party and reduce the transaction time. The centralized automated systems may currently in use and the smart contract-based real estate systems required to integrate with the existing legacy systems. However, the real estate information owned by the property owners must restrict in availability to the public. The property ownership transfer operations required to execute immediately but do not require to be realtime such as retail merchant transactions. Thorough attention may not require to optimize the consensus for the enhancement of realtime transfers of property as per the merchant transactions.

However, the extensive transaction processing time in some of the legacy systems in the present required to eliminate. More improvements required on the enhancement of data privacy, secure data sharing with third parties such as banks and other regulatory authorities as well as customer-oriented decentralized access control to the property data. Since the systems are operating in decentralized mode, the computational and storage overheads as per the centralized systems required reduced and this advantage should be beneficial to the system users. The service fees required to reduce as encouragement to the customers for the usage of proposed decentralized systems. The legal recognition and regulation with the government body without charging fees will encourage the users to adopt the system. The smart contract systems for the next generation real estate domain may require to incorporate with PKI based eGovernment systems currently in use for the legal recognition.

#### 5.4.2. ***Future work***

The smart contract based real estate systems may need legal recognition in order to operate as a national real-estate management system. To legalize, the existing definitions must be identified and the smart contract system must be designed with the provisions for the legal recognition. The integration with existing PKI based electronic identity is a prudent solution to legally onboard the smart contract-based real estate system. The gap between the smart contract system and mobile devices required eliminated to increase usability. The mobile devices should be capable of instant verification of the property record such as the title report. However, the applicable use cases of mobile devices should be identified. Eventhough the system is decentralized, multiple ownership transfers required to eliminate. The response to the attacks and the availability of the system should ensure before deployment. The data backup and recovery procedures must verify for the functionality when the system is deployed in a production state.

### 5.5. *eGovernment and Law*

#### 5.5.1. ***Lessons learned***

The utilization of smart contracts for the eGovernment and Law related services is advantageous in different dimensions. Transformation of government services into the electronic form is one of the key strategic decisions in the national authorities in order to enhance efficiency and improve data security. The cost-intensive centralized solutions can eliminate with blockchain-based smart contracts integrated solutions. The distinguishing features such as transparency, fairness and autonomous execution will ensure the trust and attract the users as well as regulatory authorities for the smart contracts for eGovernment services.

The privacy of data requires to enforce and the access control policy to the data required to be controlled by the users to obtain true decentralization. The scalability of the system is essential consideration since the eGovernment services are national scale solutions. The systems require to design with the regulatory bodies also including the service nodes of the blockchain system. Furthermore, the branches of government authorities can further continue with their decentralized domination with the contribution of block generation. Since transparency is a major consideration in the smart contracts for eGovernment services, the programs must be developed with simplicity for a clear understanding of the users and regulatory authorities.

#### 5.5.2. ***Future Work***

The future of smart contracts for eGovernment services will improve the quality of human life in different aspects. Essentially, with the development of smart cities in the future, the blockchain-based eGovernments services will operate in association with the smart cities. The integration of mobile devices will be a major design principle in the future. The decentralization will enable the peer to peer operational modes for the simple services. The transparent distributed ledger will eliminate the requirement of auditing as an explicit attempt. The citizens will have a unique decentralized identity management system

that can be interfaced with other eGovernment services such as utility services, transport, banking. From the users' perspective, user experience requires improvement without repeating the data capture before a government service. The transparency of smart contracts is the most prominent feature of smart contracts for the enforcement of law. Through transparency, citizens can establish trust. Furthermore, through automation of smart contracts, will be the most promising solution for automated fine calculation in legal violations.

### *5.6. Internet of Things*

#### *5.6.1.* ***Lessons learned***

IoT will be one of the most prominent application contexts in the Industry 4.0 revolution. Billions of devices will connect in future industrial ecosystems. Blockchain-based smart contracts integrated architectures add a lot of values to the next generation IoT ecosystems which cannot be obtained by the centralized services. The scalability and decentralization anticipated in the future IoT systems. When the smart contracts integrated with the systems, the computational overheads required to reduce since the resources are constrained in IoT devices. The consensus functions required further optimization for the smart contract integration of IoT systems. The integrations of Edge computing nodes for the smart contract service deployment are an optimal and secured design principle. Furthermore, the security requirements including privacy should be properly identified and addressed for the massive data volume generated by the IoT systems. The robust security measures required to established on the IoT systems such as UAVs in operation to prevent the cyber attacks and eventually with optimal security.

#### *5.6.2.* ***Future Works***

The smart contracts with Edge computing nodes will be a significant design principle in future IoT ecosystems. The computational overheads of a smart contract system, such as block generation require to handle on the Edge computing infrastructure. The future blockchain systems required to design with enabling provisions for the Edge node connectivity. Edge computing integration interfaces should be designed with compatible protocols such as COAP for the existing blockchain systems. The existing connectivity protocols must be diversified with optimal protocols such as gRPC. The integration compatibility of future IoT systems must improve since IoT will be a major contributor in future smart cities.

### *5.7. Telecommunication Services*

#### *5.7.1.* ***Lessons learned***

The applications for the blockchain-based smart contracts for the telecommunication industry still require maturity. The computational overheads and the limitations of the real-time operation deviate the applicability of smart contracts for telecommunication. However, some services such as slice leasing, spectrum sharing mechanisms are still applicable since they are one-time operations. The smart contracts require further optimization if it requires to execute on the resource-constrained devices such as smartphones. Since the telecommunication services are large scale operational services, the reliability of the smart contract system requires proper testing. Once the realtime operational capability of the smart contract systems achieved, more opportunities can open in the telecommunication context for the blockchain-based smart contracts.

#### *5.7.2.* ***Future Works***

The blockchain-based smart contracts are a blessing solution for the future of telecommunication since the exponential growth of subscribers is anticipated with the industrialization. The enormous volume of mobile subscribers including the industrial sensors requires the scalability of communication infrastructure. Access control to the user data can ensure through blockchain based smart contracts. The access control system will enhance the user satisfaction of users. The data repositories are extensible as the globally accepted identity information system for telecommunication service in the future. If so, multiple MNOs can utilize the smart contract-based user data repository to eliminate repetitions in customer data capturing. This data repository can integrate with a smart city ecosystem and usable to track and trace the activities of users on-demand for scenarios such as legal actions. The 6th Generation (6G) is emerging with the promises of higher bandwidth and microsecond latency. The 6G will embrace the blockchain technology to utilize the decentralization and immutability of ledger in different use cases. The scalability requirements in the future 6G context will expect to divert from the centralized computational service architectures.

### *5.8. Logistics Management*

#### *5.8.1.* ***Lessons learned***

The main features of the blockchain-based smart contracts for the logistics and supply chain industry are the data provenance and decentralized autonomous operation. The data provenance is important to evaluate the alignment of the delivery with the regulatory requirements of a particular commodity beyond frontiers. The emergence of IoT infrastructure will increase the usability of blockchain based smart contracts in the logistics industry. The blockchain based smart contract systems required to improve further in order to integrate with the logistics systems. The systems required to incorporate with mobile applications to improve usability. For instance, the supply chain milestones of agricultural products such as vegetables, fruits, and fish can store in the blockchain and view the supply chain to the customers via mobile application. Instead of developing the blockchain alone, the integration is required to consider. The efficiency of smart contracts requires optimization in the autonomous execution enablement of smart contracts in the logistics context.

#### *5.8.2.* ***Future Works***

The blockchain-based smart contracts widely applied for the data provenance of the logistics and supply chain industry. The utilization of smart contracts for autonomous operation may require further optimization. The existing smart contract platforms require fine tuning for the optimal operation. If the smart

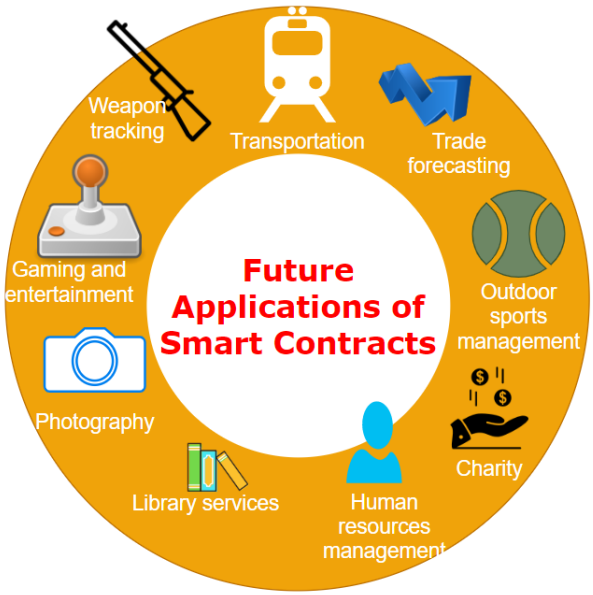


Figure 9: Future smart contract applications

contract nodes are operating with unstable network connectivity when the nodes are in the sea, the block synchronization functionality requires to identify. The error handling procedures for inconsistent blocks due to unstable network connections require further improvements. The leading smart contract platforms can fork a specialized version for the logistics-related services in future use.

### 5.9. Cross Industry

#### 5.9.1. ***Lessons learned***

Data provenance and autonomous execution are significant features that utilized widely in the industry. The blockchain based smart contracts and their utilization for IT security is a vital application. The decentralized operational capability distinguishes the blockchain-based smart contracts from centralized security solutions such as intruder detection and prevention systems. The failure risk is minimal with the smart contract integrated systems in contrast with the centralized solutions. The energy industry has a significant adaptation of blockchain based smart contracts since the autonomous execution can utilize for a lot of use cases such as smart metering, energy trading and so on. The supply chain use cases such as automotive industry and environmental protection are mostly dependent on IoT infrastructure. The improvements required for IoT will be effective for the agricultural and special commodity supply chain traceability and data provenance use cases. The lower response time with highest accuracy is required when the smart contracts are applicable to mission-critical services like aviation. The testing procedures such as formal verification, load testing, vulnerability assessment requires to conduct thoroughly when the smart contracts are incorporated to the industry like aviation.

#### 5.9.2. ***Future Works***

There are more opportunities in the industry for the blockchain based smart contracts. A lot of research-in-progress to explore more avenues of smart contract applicability. The improvements of smart contracts such as reduced latency, higher throughput and scalability will attract smart contracts to many industries. The industries such as space research and the military will have more opportunities for blockchain based smart contracts.

### 5.10. Emerging Applications of Smart Contracts

The applicability of smart contracts in the different sectors is an interesting research topic. The features of blockchain based smart contracts enable a great number of applications to be integrated with in future. The applications which have potential in future blockchain integration discussed. The Figure 9 portraits the future context of smart contracts.

#### 5.10.1. ***Transportation***

The blockchain based smart contracts have a disrupting applicability to the transport industry. The taxi and ride sharing is a significant example. When comparing with the centralized taxi services, the decentralized operational capabilities of the smart contracts provide scalability of the service with ensured service availability. The decentralized distributed ledger provides transparency of events which is eventually usable in dispute resolution. The autonomous execution provides efficiency and minimizes the human intervention in most of the operations such as booking and settlement processes. The transparent ledger provides accountability which is expected in the transport sector in some cases. However, the privacy and access control required to be implemented in the integration of the blockchain for ride sharing.

#### 5.10.2. ***Trade forecasting***

The trade prediction plays a vital role in the international foreign exchange and commodity markets. The prediction frameworks developed with the market insights and mostly integrated with machine learning techniques. The centralized machine learning techniques have limitations in the scalability and there are privacy concerns in the training data. The smart contracts can be incorporated for the trade prediction frameworks in future to eliminate most of the drawbacks encounter in the centralized techniques. The decentralization enhances the depth of crowdsourcing insights for sharp prediction frameworks. Furthermore, with the incorporation of decentralized machine learning techniques such as federated learning, the prediction frameworks can be further fine tuned for accurate predictions in the future.

#### 5.10.3. ***Outdoor sports management***

There are diverse hidden opportunities in the sports which can be utilized with the smart contracts for the improvement of service. The blockchain and smart contracts are applicable to the data provenance of the sports memorabilia, such as authentic jersey and head gears . The authenticity is verifiable using blockchain. The Non Fungiable Token (NFT), which is a non-interchangeable token is usable to represent the authentic assets. The blockchain based smart contracts are further applicable to store the historic performance data of the players.

This is important when the players transform from the national contests to the international events such as Olympic games. The historic records of the performance in games with ensure the compliance on the drug testing history of players along with the access control mechanisms powered by the blockchain based smart contracts. The indirect services, such as telecasting access rights can be managed through the smart contracts in sports.

#### *5.10.4.* ***Charity***

Charitable organizations operate to improve the social well-being for the needful people in the world. Mostly, the cost intensive requirements such as subsidizing the poor people, needs of the children fulfilled by the donations of the public. Public donations such as automated credit of the accumulated loyalty points is currently a widespread approach in fundraising for the charity. However, the blockchain based smart contracts improve the transparency in the automated credit of the loyalty points for charity. Furthermore, the blockchain provides fundraising through ICO (Initial Coin Offering) for the charity organizations. The establishment of smart contracts to utilize cryptocurrency for the expenses improve the transparency. The transparency is one of a major advantage in the smart contracts in the application perspective of charity since the public owes a right to transparently oversee the expenses of charitable organizations as the public funded them. In the form of dispute resolution and fraudulent commits of the charitable organizations can be eliminated through the blockchain based smart contracts.

#### *5.10.5.* ***Human resources management***

The capabilities of blockchain and smart contracts for the context of human resource management eliminate most of the current issues exist . The distributed ledger provides a on-demand accessible transparent record repository to track the significant events of the employees. The employers have on-demand access to the repository for the background checks of employees in the recruitment process. The access control to the data can be established using the smart contracts. Furthermore, the employee payments can be handled through the smart contracts with transparency and accuracy. The employee payment handling through the smart contract enhances the value of employee contracts based on commissions or any other performance evaluation criteria. Through the smart contracts, the employees and employers are visible on the evaluation criteria with convenience in dispute resolution requirements. The integration of in-house payment systems with the smart contracts streamlines the human resource and financial management workflow with guaranteed accuracy.

#### *5.10.6.* ***Library services***

Eventhough the world is moving towards the digital era, the reading of books remains sticked with the lifestyle of most of the people. The libraries play a vital role globally to enhance the reading. The libraries lend the books to the readers to share the knowledge. The blockchain based smart contracts have potential to enhance the value of services such as lending. Incorporation of blockchain based smart contracts can enable the peer to peer book sharing between members without the intervention of centralized authorities. The compensation for the delayed returns can be handled by the smart contracts transparently. The authors are capable of being rewarded as per the popularity of the publications. The inter-library lending processes can be enhanced with the incorporation of blockchain based smart contracts.

#### *5.10.7.* ***Photography***

The application of blockchain based smart contracts open up many opportunities for the photography. Especially, in the digital era, almost all the photographs uploaded and shared over the internet. The blockchain is applicable to store the metadata of photographs, such as location information, capturing hardware, and resolution of the photographs transparently. The smart contracts are applicable to access control the metadata for on-demand retrieval and exchanging as per the requirement, such as for the competitions. Furthermore, the photographs can be monetized by the integration of smart contracts and enable to trade in the marketplaces along with processes like auctioning.

#### *5.10.8.* ***Video streaming***

The video content and their sizes expected to be exponentially expand in the future with emerging technologies such as VR(Virtual Reality), 360 degree videos and ultra high definition in future. The number of video streaming service subscribers will be increased with diversified video content in the future. The centralized video streaming servers will have limitations in the scalability to serve the future requirements. The streaming from centralized servers will incur costs for the internet service providers. The streaming lags from the centralized servers may reduce the nature of the content. Furthermore, the access control and rights management of the content creators from centralized servers will expose to central point of failure.

The blockchain based smart contracts can facilitate the service with decentralization with efficient data consumption in streaming. The content rights management and subscription of the premium content are easily manageable with the decentralized smart contracts. The customized advertising based on user preference and the location efficiently managable through blockchain based smart contracts.

#### *5.10.9.* ***Gaming and entertainment***

The eSports market is expected to boom with millions of users in future. The eSports will encounter the scalability limitations in the incentivization, user identity management, and access control related operations with the rapid growth of demand. The blockchain based smart contracts will improve the player identity management, access control and provide transparency to eliminate dispute resolution in any case. The fan incentivization can be handled easily with the tokens supported by the blockchain. The tokens can be used to trade the monetized components of eSports. Furthermore, the entertainment techniques such as casinos can be regulated and audit with the incorporation of smart contracts. The dispute resolution is straightforward when the smart contracts incorporated.

#### *5.10.10. **Weapon and ammunition tracking***

Weapons and ammunition is utilized in domestic and national scale in some countries. The accountability of guns, volume of ammunition, their licensing information and the usage statistics are significant information on the establishment of national security. The blockchain based smart contracts provide transparency in the license information, usage statistics, ownership information of the guns with decentralized access control to the regulatory authorities such as Police, government administrative authorities and so on. The regulation of the usage in the national and international scope is also possible with the blockchain based smart contracts. The authorities such as United Nations can define the smart contracts to regulate the usage of ballistic missiles and rocket launchers as an international governing body.

## 6. Conclusion

The paper provides an extensive survey on applications of blockchain based smart contacts. The significance of smart contracts is distinguished due the rich set of features such as decentralization, forge resistance, transparency, autonomous execution, and accuracy. As a result, blockchain based smart contracts are used in wide rage of applications domains such as financial, healthcare, eGovernment, IoT, telecommunication, logistics, and different industrial contexts. Several blockchain platforms such as Ethereum, Hyperledger Fabric, Corda, NEM, Stellar, and Waves are available to deploy smart contacts with unique applicability features into the industry. Moreover, it is expected that more platforms will be emerged targeting specialized application domains. However, there are few challenges that smart contracts have to resolved before the large scale deployments. These challenges includes scalability, data privacy, lack of governance, computational overheads, storage overheads, and network overheads. Future research on smart contracts should be focusing on these challenges. The future research avenues are available to investigate the optimizations of consensus mechanisms, data usage efficiency, lower latency, minimal storage overheads with extremely lower latency in transaction processing.

## Acknowledgement

This work was supported in part by the Academy of Finland Project 6Genesis Flagship (Grant No. 318927), RESPONSE 5G (Grant No: 789658) and the European Union's Horizon 2020 research and innovation programme under the INSPIRE-5Gplus project (Grant No. 871808). The paper reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains.

## References

[1] S. Nakamoto, Bitcoin: A Peer-to-peer Electronic Cash System, 2009. URL: `http://www.bitcoin.org/bitcoin.pdf`.

[2] V. Buterin, et al., A Next-generation Smart Contract and Decentralized Application Platform, white paper 3 (2014) 37.

[3] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, F.-Y. Wang, An Overview of Smart Contract: Architecture, Applications, and Future Trends, in: 2018 IEEE Intelligent Vehicles Symposium (IV), IEEE, 2018, pp. 108–113.

[4] A. Wright, P. De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia, Available at SSRN 2580664 (2015).

[5] C. Udokwu, A. Kormiltsyn, K. Thangalimodzi, A. Norta, An Exploration of Blockchain Enabled Smart-contracts Application in the Enterprise, Technical Report, Technical Report, DOI: 10.13140/RG. 2.2. 36464.97287, Tech. Rep, 2018.

[6] P. L. Seijas, S. J. Thompson, D. McAdams, Scripting smart contracts for distributed ledger technology., IACR Cryptology ePrint Archive 2016 (2016) 1156.

[7] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, A. Y. Zomaya, Blockchain for Smart Communities: Applications, Challenges and Opportunities, Journal of Network and Computer Applications (2019).

[8] K. Wüst, A. Gervais, Do You Need a Blockchain?, in: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), IEEE, 2018, pp. 45–54.

[9] C. D. Clack, V. A. Bakshi, L. Braine, Smart Contract Templates: Essential Requirements and Design Options, arXiv preprint arXiv:1612.04496 (2016).

[10] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, W. Shi, Decentralized Execution of Smart Contracts: Agent Model Perspective and its Implications, in: International Conference on Financial Cryptography and Data Security, Springer, 2017, pp. 468–477.

[11] J. Sousa, A. Bessani, M. Vukolic, A Byzantine Fault-tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform, in: 2018 48th annual IEEE/IFIP international conference on dependable systems and networks (DSN), IEEE, 2018, pp. 51–58.

[12] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, P. Rimba, A taxonomy of Blockchain-based Systems for Architecture Design, in: 2017 IEEE International Conference on Software Architecture (ICSA), IEEE, 2017, pp. 243–252.

[13] B. Marino, A. Juels, Setting Standards for Altering and Undoing Smart Contracts, in: International Symposium on Rules and Rule Markup Languages for the Semantic Web, Springer, 2016, pp. 151–166.

[14] A. Norta, Designing a Smart-contract Application Layer for Transacting Decentralized Autonomous Organizations, in: International Conference on Advances in Computing and Data Sciences, Springer, 2016, pp. 595–604.

[15] L. Luu, Y. Velner, J. Teutsch, P. Saxena, Smartpool: Practical Decentralized Pooled Mining, in: 26th {USENIX} Security Symposium ({USENIX} Security 17), 2017, pp. 1409–1426.

[16] P. Dai, N. Mahi, J. Earls, A. Norta, Smart-contract Value-transfer Protocols on a Distributed Mobile Application Platform, URL: https://qtum. org/uploads/files/cf6d69348ca50dd985b60425ccf282f3. pdf (2017) 10.

[17] D. Macrinici, C. Cartofeanu, S. Gao, Smart Contract Applications within Blockchain Technology: A Systematic Mapping Study, Telematics and Informatics (2018).

[18] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain Challenges and Opportunities: A Survey, International Journal of Web and Grid Services 14 (2018) 352–375.

[19] P. He, G. Yu, Y. Zhang, Y. Bao, Survey on Blockchain Technology and its Application Prospect, Computer Science 44 (2017) 1–7.

[20] L. S. Sankar, M. Sindhu, M. Sethumadhavan, Survey of Consensus Protocols on Blockchain Applications, in: 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 2017, pp. 1–5.

[21] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, K.-K. R. Choo, Sidechain Technologies in Blockchain Networks: An Examination and State-of-the-art Review, Journal of Network and Computer Applications (2019) 102471.

[22] M. Bartoletti, L. Pompianu, An empirical analysis of smart contracts: platforms, applications, and design patterns, in: International conference on financial cryptography and data security, Springer, 2017, pp. 494–509.

[23] J. Sengupta, S. Ruj, S. D. Bit, A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT, Journal of Network and Computer Applications (2019) 102481.

[24] Q. Feng, D. He, S. Zeadally, M. K. Khan, N. Kumar, A Survey on Privacy Protection in Blockchain System, Journal of Network and Computer Applications 126 (2019) 45–58.

[25] Q. Zhu, S. W. Loke, R. Trujillo-Rasua, F. Jiang, Y. Xiang, Applications

of distributed ledger technologies to the internet of things: A survey, ACM Computing Surveys (CSUR) 52 (2019) 1–34.
[26] W. Chen, Z. Xu, S. Shi, Y. Zhao, J. Zhao, A survey of blockchain applications in different domains, in: Proceedings of the 2018 International Conference on Blockchain Technology and Application, ACM, 2018, pp. 17–21.
[27] Y. Lu, Blockchain: A Survey on Functions, Applications and Open Issues, Journal of Industrial Integration and Management 3 (2018) 1850015. Accessed: 2020-01-31.
[28] S. T. Aras, V. Kulkarni, Blockchain and its applications–a detailed survey, International Journal of Computer Applications 180 (2017) 29–35.
[29] 2020. URL: https://makerdao.com/en/, accessed: 2020-01-31.
[30] Gitcoin Whitepaper, 2020. URL: https://gitcoin.co/whitepaper, accessed: 2020-01-31.
[31] 2020. URL: https://en.wikipedia.org/wiki/CryptoKitties, [Online; accessed 2020-01-31].
[32] IBM Food Trust, 2020. URL: https://www.ibm.com/blockchain/solutions/food-trust, accessed: 2020-01-31.
[33] Everledger, 2020. URL: https://www.everledger.io/, accessed: 2020-01-31.
[34] Energy Block Exchange, 2020. URL: https://guild1.co/energy-block-exchange-ebx/, accessed: 2020-01-31.
[35] TradeCloud, 2020. URL: https://tradecloud.sg/, accessed: 2020-01-31.
[36] MonetaGo, 2020. URL: https://www.monetago.com/, accessed: 2020-01-31.
[37] DigitCoin, 2020. URL: https://www.digitcoin.world/, accessed: 2020-01-31.
[38] Bankera, 2020. URL: https://bankera.com/, accessed: 2020-01-31.
[39] Pantos, 2020. URL: https://pantos.io/, accessed: 2020-01-31.
[40] Verses, 2020. URL: https://verses.io/, accessed: 2020-01-31.
[41] StellarX, 2020. URL: https://www.stellarx.com/, accessed: 2020-01-31.
[42] Tempo, 2020. URL: https://tempo.eu.com/en, accessed: 2020-01-31.
[43] TillBilly, 2020. URL: https://tillbilly.com/, accessed: 2020-01-31.
[44] Token Economica, 2020. URL: https://wavesplatform.com/use-case/5e04c549513a210010a2c10e, accessed: 2020-01-31.
[45] Tradisys, 2020. URL: https://wavesplatform.com/use-case/5db6c3dd3f617e00127569e4, accessed: 2020-01-31.
[46] Multichain Ventures, 2020. URL: https://wavesplatform.com/use-case/5e00f274513a210010a2c105, accessed: 2020-01-31.
[47] G. Wood, Ethereum: A Secure Decentralised Generalised Transaction Ledger, Ethereum project yellow paper 151 (2014) 1–32.
[48] W. Dingman, A. Cohen, N. Ferrara, A. Lynch, P. Jasinski, P. E. Black, L. Deng, Classification of smart contract bugs using the nist bugs framework, in: 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA), IEEE, 2019, pp. 116–123.
[49] Cryptocurrency Deposit Processing Times, https://support.kraken.com/hc/en-us/articles/203325283-Cryptocurrency-deposit-processing-times (2017).
[50] J. Woods, Enterprise Blockchain Has Arrived (Part 2), https://www.blockchainbeach.com/enterprise-blockchain-has-arrived-part-2 (2018).
[51] A. Litke, D. Anagnostopoulos, T. Varvarigou, Blockchains for supply chain management: architectural elements and challenges towards a global scale deployment. logistics 3 (1)(2019), 2019.
[52] Transactions Per Second, https://medium.com/corda/transactions-per-second-tps-de3fb55d60e3 (2018).
[53] S. Williams, 3 Cryptocurrencies Processing 1,500 (or More) Transactions Per Second, https://www.fool.com/investing/2018/02/01/3-cryptocurrencies-processing-1500-or-more-transac.aspx (2018).
[54] C. Gorenflo, S. Lee, L. Golab, S. Keshav, Fastfabric: Scaling Hyperledger Fabric to 20,000 Transactions per second, in: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, 2019, pp. 455–463.
[55] LendLedger, Harnessing the Power of Stellar, https://medium.com/lendledger/why-lendledger-is-a-stellar-project-2403724b91d2 (2018).
[56] S. Ivanov, waves legitimately reaches 500 TPS on the mainnet. Meaning you can go and send 500 transactions per second, no strings attached., https://twitter.com/sasha35625/status/1064470221594009601 (2018).
[57] R. G. B. Mike Hearn, Corda: A distributed ledger, https://www.corda.net/wp-content/uploads/2019/08/corda-technical-whitepaper-August-29-2019.pdf (2019).
[58] Waves Data Privacy, https://docs.wavesenterprise.com/en/1.1.2/how-the-platform-works/data-privacy.html (2018).
[59] N. Vovchenko, A. Andreeva, A. Orobinskiy, Y. Filippov, Competitive Advantages of Financial Transactions on the Basis of the Blockchain Technology in Digital Economy, European Research Studies 20 (2017) 193.
[60] Btc, Yes, Bitcoin Can Do Smart Contracts and Particl Demonstrates How, 2020. URL: https://bitcoinmagazine.com/articles/yes-bitcoin-can-do-smart-contracts-and-particl-demonstrates-how/.
[61] S. Lande, R. Zunino, SoK: Unraveling Bitcoin Smart Contracts, Principles of Security and Trust LNCS 10804 (2018) 217.
[62] Y. Hu, A. Manzoor, P. Ekparinya, M. Liyanage, K. Thilakarathna, G. Jourjon, A. Seneviratne, M. E. Ylianttila, A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain, CoRR abs/1801.10295 (2018). URL: http://arxiv.org/abs/1801.10295. arXiv:1801.10295.
[63] A. Manzoor, Y. Hu, M. Liyanage, P. Ekparinya, K. Thilakarathna, G. Jourjon, A. Seneviratne, S. Kanhere, M. E. Ylianttila, A Delay-Tolerant Payment Scheme on the Ethereum Blockchain, in: 2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), IEEE, 2018, pp. 14–16.
[64] D. Hopwood, S. Bowe, T. Hornby, N. Wilcox, Zcash Protocol Specification, Tech. rep. 2016–1.10. Zerocoin Electric Coin Company, Tech. Rep. (2016).
[65] E. Duffield, D. Diaz, Dash: A Privacy-centric Cryptocurrency, No Publisher (2015).
[66] M. T. Rosner, A. Kang, Understanding and Regulating Twenty-first Century Payment Systems: The Ripple Case Study, Mich. L. Rev. 114 (2015) 649.
[67] Y. Guo, C. Liang, "Blockchain application and outlook in the banking industry", Financial Innovation 2 (2016) 24. URL: https://doi.org/10.1186/s40854-016-0034-9. doi:10.1186/s40854-016-0034-9.
[68] J. Parra Moyano, O. Ross, "KYC Optimization Using Distributed Ledger Technology", Business & Information Systems Engineering 59 (2017) 411–423. URL: https://doi.org/10.1007/s12599-017-0504-2. doi:10.1007/s12599-017-0504-2.
[69] A. Biryukov, D. Khovratovich, S. Tikhomirov, Privacy-preserving KYC on Ethereum, in: 1st ERCIM Blockchain Workshop, 2018.
[70] G. W. Peters, E. Panayi, Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money, in: Banking beyond banks and money, Springer, 2016, pp. 239–278.
[71] A. Bogner, M. Chanson, A. Meeuw, A Decentralised Sharing App Running a Smart Contract on the Ethereum Blockchain, in: Proceedings of the 6th International Conference on the Internet of Things, ACM, 2016, pp. 177–178.
[72] Insurance fraud, 2020. URL: https://en.wikipedia.org/wiki/Insurance_fraud, accessed: 2020-01-31.
[73] R. Hans, H. Zuber, A. Rizk, R. Steinmetz, Blockchain and Smart Contracts: Disruptive Technologies for the Insurance Market, in: 2017 Americas Conference on Information Systems, 2017.
[74] Allianz — B3i to Present Smart Contract Management System at 2017 Monte Carlo RVS conference, 2020. URL: https://www.allianz.com/en/press/news/commitment/sponsorship/170719-b3i-to-present-smart-contract-management-system.html.
[75] M. Crawford, The Insurance Implications of Blockchain, Risk Management 64 (2017) 24.
[76] Y. Guo, Z. Qi, X. Xian, H. Wu, Z. Yang, J. Zhang, L. Wenyin, WIS-Chain: An Online Insurance System based on Blockchain and DengLu1 for Web Identity Security, in: 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), 2018, pp. 242–243. doi:10.1109/HOTICN.2018.8606011.
[77] J. Bird, 'Smart' Insurance Helps Poor Farmers to Cut Risk, 2018. URL:

https://www.ft.com/content/3a8c7746-d886-11e8-aa22-36538487e3d0.
[78] Etherisc White Paper, Technical Report, Etherisc GmbH, 2017.
[79] H. T. Vo, L. Mehedy, M. Mohania, E. Abebe, Blockchain-based Data Management and Analytics for Micro-insurance Applications, in: Proceedings of the 2017 ACM on Conference on Information and Knowledge Management, ACM, 2017, pp. 2539–2542.
[80] Average Loan Processing Time, 2020. URL: https://themortgagereports.com/19487/how-long-does-it-take-to-close-a-mortgage-gina-pogol, accessed: 2020-01-31.
[81] Salt Lending White Paper, 2020. URL: https://www.cryptoground.com/salt-lending-white-paper.
[82] ETHLend, Ethlend/documentation, 2020. URL: https://github.com/ETHLend/Documentation/blob/master/ETHLendWhitePaper.md.
[83] Blockchain-Powered Money Transfers and Microfinance Services, 2020. URL: https://www.everex.io/cn/everexhow-it-works.
[84] Debitum Network (DEB) Price, Chart, Info - CoinSchedule, 2020. URL: https://www.coinschedule.com/cryptocurrency/debitum-network.
[85] X. Zou, X. Deng, T.-Y. Wu, C.-M. Chen, A collusion attack on identity-based public auditing scheme via blockchain, in: Advances in Intelligent Information Hiding and Multimedia Signal Processing, Springer, 2020, pp. 97–105.
[86] A. M. Rozario, M. A. Vasarhelyi, Auditing with smart contracts., International Journal of Digital Accounting Research 18 (2018).
[87] D. Yermack, Corporate Governance and Blockchains, Review of Finance (2015). doi:10.3386/w21802.
[88] TITA Project Whitepaper, 2020. URL: https://icosbull.com/eng/ico/titaproject/whitepaper.
[89] ASX Details Timeline, Features for New Blockchain-inspired System, 2020. URL: https://www.computerworld.com.au/article/640596/asx-details-timeline-features-new-blockchain-inspired-system/.
[90] Hong Kong Stock Exchange and Digital Asset Partner to Create New Blockchain Trade Platform, 2018. URL: https://www.ccn.com/hong-kong-exchange-prepares-for-blockchain-trading-platform, accessed: 2020-01-31.
[91] World's First Blockchain-powered Diamond Trading Platform to Launch in Hong Kong, 2019. URL: https://www.ccn.com/hong-kong-exchange-prepares-for-blockchain-trading-platform, accessed: 2020-01-31.
[92] Z. O. Candereli, S. Burmaoglu, L. B. Kidak, D. O. Gungor, Applying blockchain technologies in healthcare: A scientometric analysis, in: Multidimensional Perspectives and Global Analysis of Universal Health Coverage, IGI Global, 2020, pp. 69–92.
[93] T. McGhin, K.-K. R. Choo, C. Z. Liu, D. He, Blockchain in Healthcare Applications: Research Challenges and Opportunities, Journal of Network and Computer Applications (2019).
[94] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, MedRec: Using Blockchain for Medical Data Access and Permission Management, in: 2016 2nd International Conference on Open and Big Data (OBD), 2016, pp. 25–30. doi:10.1109/OBD.2016.11.
[95] P. Nichol, J. Brandt, Co-Creation of Trust for Healthcare: The Cryptocitizen Framework for Interoperability with Blockchain (2016). doi:10.13140/RG.2.1.1545.4963.
[96] T. Kuo, L. Ohno-Machado, ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks, CoRR abs/1802.01746 (2018). URL: http://arxiv.org/abs/1802.01746. arXiv:1802.01746.
[97] G. G. Dagher, J. Mohler, M. Milojkovic, P. B. Marella, Ancile: Privacy-preserving Framework for Access Control and Interoperability of Electronic Health Records using Blockchain Technology, Sustainable cities and society 39 (2018) 283–297.
[98] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control, Journal of medical systems 40 (2016) 218.
[99] S. P. Novikov, O. D. Kazakov, N. A. Kulagina, N. Y. Azarenko, Blockchain and Smart Contracts in a Decentralized Health Infrastructure, in: 2018 IEEE International Conference" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS), IEEE, 2018, pp. 697–703.
[100] S. Alexaki, G. Alexandris, V. Katos, E. N. Petroulakis, Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions, in: 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE, 2018, pp. 1–6.
[101] T.-T. Kuo, H.-E. Kim, L. Ohno-Machado, Blockchain Distributed Ledger Technologies for Biomedical and Health Care Applications, Journal of the American Medical Informatics Association 24 (2017) 1211–1220.
[102] T. Nugent, D. Upton, M. Cimpoesu, Improving Data Transparency in Clinical Trials using Blockchain Smart Contracts, F1000Research 5 (2016).
[103] P. Zhang, J. White, D. C. Schmidt, G. Lenz, S. T. Rosenbloom, Fhirchain: Applying Blockchain to Securely and Scalably Share Clinical Data, Computational and structural biotechnology journal 16 (2018) 267–278.
[104] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, T. Hayajneh, Healthcare Blockchain System using Smart Contracts for Secure Automated Remote Patient Monitoring, Journal of medical systems 42 (2018) 130.
[105] Facebook Cambridge Analytica, ???? URL: "https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal", accessed: 2020-01-31.
[106] A. Banerjee, K. P. Joshi, Link before You Share: Managing Privacy Policies through Blockchain, in: 2017 IEEE International Conference on Big Data (Big Data), IEEE, 2017, pp. 4438–4447.
[107] A. Ouaddah, A. Abou Elkalam, A. Ait Ouahman, FairAccess: A New Blockchain-based Access Control Framework for the Internet of Things, Security and Communication Networks 9 (2016) 5943–5964.
[108] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, J. Wan, Smart contract-based access control for the internet of things, IEEE Internet of Things Journal 6 (2019) 1594–1605. doi:10.1109/JIOT.2018.2847705.
[109] H. Es-Samaali, A. Outchakoucht, J. P. Leroy, A Blockchain-based Access Control for Big Data, International Journal of Computer Networks and Communications Security 5 (2017) 137.
[110] M. Al-Bassam, SCPKI: A Smart Contract-based PKI and Identity System, in: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, ACM, 2017, pp. 35–40.
[111] R. Xu, Y. Chen, E. Blasch, G. Chen, Blendcac: A Smart Contract enabled Decentralized Capability-based Access Control Mechanism for the IoT, Computers 7 (2018) 39.
[112] C. Lin, D. He, X. Huang, K.-K. R. Choo, A. V. Vasilakos, BSeIn: A Blockchain-based Secure Mutual Authentication with Fine-grained Access Control System for Industry 4.0, Journal of Network and Computer Applications 116 (2018) 42–52.
[113] M. S. Ali, K. Dolui, F. Antonelli, IoT Data Privacy via Blockchains and IPFS, in: Proceedings of the Seventh International Conference on the Internet of Things, ACM, 2017, p. 14.
[114] C. H. Lee, K. Kim, Implementation of IoT System using Block Chain with Authentication and Data Protection, in: 2018 International Conference on Information Networking (ICOIN), 2018, pp. 936–940. doi:10.1109/ICOIN.2018.8343261.
[115] J. P. Cruz, Y. Kaji, N. Yanai, RBAC-SC: Role-Based Access Control Using Smart Contract, IEEE Access 6 (2018) 12240–12251. doi:10.1109/ACCESS.2018.2812844.
[116] A. Outchakoucht, E. Hamza, J. P. Leroy, Dynamic Access Control Policy based on Blockchain and Machine Learning for the Internet of Things, Int. J. Adv. Comput. Sci. Appl 8 (2017) 417–424.
[117] Q. Lyu, Y. Qi, X. Zhang, H. Liu, Q. Wang, N. Zheng, SBAC: A Secure Blockchain-based Access Control Framework for Information-centric Networking, Journal of Network and Computer Applications 149 (2020) 102444.
[118] G. Ali, N. Ahmad, Y. Cao, Q. E. Ali, F. Azim, H. Cruickshank, BCON: Blockchain based Access CONtrol Across Multiple Conflict of Interest Domains, Journal of Network and Computer Applications 147 (2019) 102440.
[119] I. Karamitsos, M. Papadaki, N. B. Al Barghuthi, Design of the blockchain smart contract: A Use Case for Real Estate, Journal of Information Security 9 (2018) 177.

[120] A. Spielman, Blockchain: Digitally Rebuilding the Real Estate Industry, Ph.D. thesis, Massachusetts Institute of Technology, 2016.
[121] M. Dijkstra, Blockchain: Towards Disruption in the Real Estate Sector, An Exploration on the Impact of Blockchain Technology in the Real Estate Management Process, University of Delft, Delft.[Google Scholar] (2017).
[122] D. Oparah, D. Oparah, 3 Ways That The Blockchain Will Change The Real Estate Market, 2016. URL: https://techcrunch.com/2016/02/06/3-ways-that-blockchain-will-change-the-real-estate-market/.
[123] C. Fernandez, S. Hickmott, A. Norta, Tokenizing Commercial Property With Smart Contracts (2020).
[124] M. Raskin, The Law and Legality of Smart Contracts (2016).
[125] A. Savelyev, Contract Law 2.0:'Smart' Contracts as the Beginning of the End of Classic Contract Law, Information & Communications Technology Law 26 (2017) 116–134.
[126] R. O'Shields, Smart contracts: Legal Agreements for the Blockchain, NC Banking Inst. 21 (2017) 177.
[127] R. Koulu, Blockchains and online dispute resolution: smart contracts as an alternative to enforcement, SCRIPTed 13 (2016) 40.
[128] K. E. Levy, Book-smart, Not Street-smart: Blockchain-based Smart Contracts and the Social Workings of Law, Engaging Science, Technology, and Society 3 (2017) 1–15.
[129] J. L. de la Rosa, D. Gibovic, V. Torres, L. Maicher, F. Miralles, A. El-Fakdi, A. Bikfalvi, On Intellectual Property in Online Open Innovation for SME by means of Blockchain and Smart Contracts, in: 3rd Annual World Open Innovation Conf. WOIC, 2016.
[130] F. Tietze, O. Granstrand, Enabling the digital economy-distributed ledger technologies for automating ip licensing payments, in: Managing Innovation in a Global and Digital World, Springer, 2020, pp. 347–365.
[131] K. Lauslahti, J. Mattila, T. Seppala, Smart Contracts–How will Blockchain Technology Affect Contractual Practices? (2017).
[132] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, J. J. Kishigami, Blockchain Contract: A Complete Consensus using Blockchain, in: 2015 IEEE 4th global conference on consumer electronics (GCCE), IEEE, 2015, pp. 577–578.
[133] C. K. Frantz, M. Nowostawski, From Institutions to Code: Towards Automated Generation of Smart Contracts, in: 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W), IEEE, 2016, pp. 210–215.
[134] E. J. Scheid, B. Stiller, Automatic SLA Compensation based on Smart Contracts, Technical Report, Technical Report IFI-2018.02 https://files.ifi. uzh. ch/CSG/staff/scheid . . . , 2018.
[135] M. Walport, Distributed Ledger Technology: Beyond Block Chain (A Report by the UK Government Chief Scientific Adviser), UK Government (2016).
[136] C.-W. Chiang, E. Betanzos, S. Savage, Blockchain for Trustful Collaborations between Immigrants and Governments, arXiv preprint arXiv:1805.01512 (2018).
[137] P. N.-M. Gheorghe, B. Ţigănoaia, A. Niculescu, Blockchain and Smart Contracts in the Music Industry–Streaming vs. Downloading, in: International Conference on Management and Industrial Engineering, 8, Niculescu Publishing House, 2017, pp. 215–228.
[138] B. Bodó, D. Gervais, J. P. Quintais, Blockchain and Smart Contracts: The Missing Link in Copyright Licensing?, International Journal of Law and Information Technology 26 (2018) 311–336.
[139] K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri, S. Gupta, A comparitive analysis on e-voting system using blockchain, in: 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), IEEE, 2019, pp. 1–4.
[140] A. B. Ayed, A conceptual secure blockchain-based electronic voting system, International Journal of Network Security & Its Applications 9 (2017) 01–09.
[141] P. McCorry, S. F. Shahandashti, F. Hao, A smart contract for boardroom voting with maximum voter privacy, in: International Conference on Financial Cryptography and Data Security, Springer, 2017, pp. 357–375.
[142] K. Patidar, S. Jain, Decentralized e-voting portal using blockchain, in: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, 2019, pp. 1–4.
[143] N. Fotiou, G. C. Polyzos, Smart Contracts for the Internet of Things: Opportunities and Challenges, in: 2018 European Conference on Networks and Communications (EuCNC), IEEE, 2018, pp. 256–260.
[144] K.-L. Wright, M. Espinoza, U. Chadha, B. Krishnamachari, SmartEdge: A Smart Contract for Edge Computing, 2018.
[145] K. R. Özyılmaz, A. Yurdakul, Designing a Blockchain-based IoT Infrastructure with Ethereum, Swarm and LoRa, arXiv preprint arXiv:1809.07655 (2018).
[146] M. Liu, F. R. Yu, Y. Teng, V. C. Leung, M. Song, Distributed Resource Allocation in Blockchain-Based Video Streaming Systems With Mobile Edge Computing, IEEE Transactions on Wireless Communications 18 (2019) 695–708.
[147] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, L. Xie, A Decentralized Solution for IoT Data Trusted Exchange based-on Blockchain, in: 2017 3rd IEEE International Conference on Computer and Communications (ICCC), IEEE, 2017, pp. 1180–1184.
[148] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, Z. Han, When Mobile Blockchain Meets Edge Computing, IEEE Communications Magazine 56 (2018) 33–39.
[149] A. Stanciu, Blockchain Based Distributed Control System for Edge Computing, in: 2017 21st International Conference on Control Systems and Computer Science (CSCS), 2017, pp. 667–671. doi:10.1109/CSCS.2017.102.
[150] J. Yang, Z. Lu, J. Wu, Smart-toy-edge-computing-oriented data exchange based on blockchain, Journal of Systems Architecture 87 (2018) 36–48.
[151] M. Samaniego, R. Deters, Pushing Software-Defined Blockchain Components onto Edge Hosts, in: Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019.
[152] Y. Xu, G. Wang, J. Yang, J. Ren, Y. Zhang, C. Zhang, Towards Secure Network Computing Services for Lightweight Clients Using Blockchain, Wireless Communications and Mobile Computing 2018 (2018).
[153] N. El Ioini, C. Pahl, Trustworthy Orchestration of Container-based Edge Computing using Permissioned Blockchain, in: 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, IEEE, 2018, pp. 147–154.
[154] G. Fortino, F. Messina, D. Rosaci, G. M. Sarne, C. Savaglio, A Trust-based Team Formation Framework for Mobile Intelligence in Smart Factories, IEEE Transactions on Industrial Informatics (2020).
[155] G. Fortino, F. Messina, D. Rosaci, G. M. Sarné, Using Blockchain for Reputation-Based Cooperation in Federated IoT Domains, in: International Symposium on Intelligent and Distributed Computing, Springer, 2019, pp. 3–12.
[156] G. Fortino, F. Messina, D. Rosaci, G. M. Sarne, Using Blockchain in a Reputation-based Model for Grouping Agents in the Internet of Things, IEEE Transactions on Engineering Management (2019).
[157] A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, Lsb: A Lightweight Scalable Blockchain for IoT Security and Privacy, arXiv preprint arXiv:1712.02969 (2017).
[158] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, R. Ranjan, IoTChain: Establishing Trust in the Internet of Things Ecosystem using Blockchain, IEEE Cloud Computing 5 (2018) 12–23.
[159] M. A. Khan, K. Salah, IoT security: Review, Blockchain Solutions, and Open Challenges, Future Generation Computer Systems 82 (2018) 395–411.
[160] J. Lin, Z. Shen, C. Miao, S. Liu, Using Blockchain to Build Trusted Lorawan Sharing Server, International Journal of Crowd Science 1 (2017) 270–280.
[161] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, Y. Zhao, EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts, IEEE Internet of Things Journal (2019) 1–1. doi:10.1109/JIOT.2018.2878154.
[162] S. Cha, T. Tsai, W. Peng, T. Huang, T. Hsu, Privacy-aware and blockchain connected gateways for users to access legacy IoT devices, in: 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), 2017, pp. 1–3. doi:10.1109/GCCE.2017.8229327.
[163] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, F. Sallabi, Softwarization of Internet of Things Infrastructure for Secure and Smart Healthcare, arXiv preprint arXiv:1805.11011 (2018).
[164] K. Rantos, G. Drosatos, K. Demertzis, C. Ilioudis, A. Papanikolaou, Blockchain-based Consents Management for Personal Data Processing in the IoT Ecosystem, in: proceedings of the 15th International Confer-

ence on Security and Cryptography (SECRYPT 2018), part of ICETE, 2018, pp. 572–577.

[165] O. J. A. Pinno, A. R. A. Gregio, L. C. E. De Bona, ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT, in: GLOBECOM 2017 - 2017 IEEE Global Communications Conference, 2017, pp. 1–6. doi:10.1109/GLOCOM.2017.8254521.

[166] B. Liu, X. L. Yu, S. Chen, X. Xu, L. Zhu, Blockchain-based Data Integrity Service Framework for IoT Data, in: 2017 IEEE International Conference on Web Services (ICWS), IEEE, 2017, pp. 468–475.

[167] S. Rathore, B. W. Kwon, J. H. Park, Blockseciotnet: Blockchain-based decentralized security architecture for iot network, Journal of Network and Computer Applications 143 (2019) 167–177.

[168] O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, F. Zanichelli, IoTChain: A Blockchain Security Architecture for the Internet of Things, in: 2018 IEEE Wireless Communications and Networking Conference (WCNC), IEEE, 2018, pp. 1–6.

[169] D. Nagothu, R. Xu, S. Y. Nikouei, Y. Chen, A Microservice-enabled Architecture for Smart Surveillance using Blockchain Technology, in: 2018 IEEE International Smart Cities Conference (ISC2), IEEE, 2018, pp. 1–4.

[170] G. C. Polyzos, N. Fotiou, Blockchain-Assisted Information Distribution for the Internet of Things, in: 2017 IEEE International Conference on Information Reuse and Integration (IRI), 2017, pp. 75–78. doi:10.1109/IRI.2017.83.

[171] D. G. Roy, P. Das, D. De, R. Buyya, QoS-aware Secure Transaction Framework for Internet of Things using Blockchain mechanism, Journal of Network and Computer Applications 144 (2019) 59–78.

[172] P. Mehta, R. Gupta, S. Tanwar, Blockchain envisioned uav networks: Challenges, solutions, and comparisons, Computer Communications (2020).

[173] A. Kapitonov, S. Lonshakov, A. Krupenkin, I. Berman, Blockchain-based Protocol of Autonomous Business Activity for Multi-agent Systems Consisting of UAVs, in: 2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS), IEEE, 2017, pp. 84–89.

[174] V. Sharma, I. You, G. Kul, Socializing Drones for Inter-service Operability in Ultra-dense Wireless Networks using Blockchain, in: Proceedings of the 2017 International Workshop on Managing Insider Security Threats, ACM, 2017, pp. 81–84.

[175] L. Yang, N. Elisa, N. Eliot, Privacy and Security Aspects of E-government in Smart Cities, Elsevier, 2019, pp. 89–102.

[176] D.-Y. Liao, X. Wang, 5G Wireless Micro Operators for Integrated Casinos and Entertainment in Smart Cities (2018) 115–149.

[177] C. Lazaroiu, M. Roscia, Smart District through IoT and Blockchain, in: 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA), IEEE, 2017, pp. 454–461.

[178] B. Leiding, P. Memarmoshrefi, D. Hogrefe, Self-managed and blockchain-based vehicular ad-hoc networks, in: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, ACM, 2016, pp. 137–140.

[179] J. Sun, J. Yan, K. Z. Zhang, Blockchain-based Sharing services: What Blockchain Technology can Contribute to Smart Cities, Financial Innovation 2 (2016) 26.

[180] P. K. Sharma, S. Y. Moon, J. H. Park, Block-VN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City., JIPS 13 (2017) 184–195.

[181] P. K. Sharma, N. Kumar, J. H. Park, Blockchain-based Distributed Framework for Automotive Industry in a Smart City, IEEE Transactions on Industrial Informatics (2018) 1–1. doi:10.1109/TII.2018.2887101.

[182] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, N. Zhang, A Secure Charging Scheme for Electric Vehicles with Smart Communities in Energy Blockchain, IEEE Internet of Things Journal (2018).

[183] S. R. Niya, S. S. Jha, T. Bocek, B. Stiller, Design and Implementation of an Automated and Decentralized Pollution Monitoring System with Blockchains, Smart Contracts, and LoRaWAN, in: NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2018, pp. 1–4.

[184] X. Feng, J. Ma, T. Feng, Y. Miao, X. Liu, Consortium Blockchain-Based SIFT: Outsourcing Encrypted Feature Extraction in the D2D Network, IEEE Access 6 (2018) 52248–52260.

[185] K. Biswas, V. Muthukkumarasamy, Securing Smart Cities using Blockchain Technology, in: 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS), IEEE, 2016, pp. 1392–1393.

[186] A. Bahga, V. K. Madisetti, Blockchain Platform for Industrial Internet of Things, Journal of Software Engineering and Applications 9 (2016) 533.

[187] S. Ibba, A. Pinna, M. Seu, F. E. Pani, CitySense: Blockchain-oriented Smart Cities, in: Proceedings of the XP2017 Scientific Workshops, ACM, 2017, p. 12.

[188] A. Manzoor, M. Liyanage, A. Braeke, S. S. Kanhere, M. Ylianttila, Blockchain based Proxy re-encryption Scheme for Secure IoT Data Sharing, in: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, 2019, pp. 99–103.

[189] T. Hewa, A. Bracken, M. Ylianttila, M. Liyanage, Blockchain-based Automated Certificate Revocation for 5G IoT, in: ICC 2020-2020 IEEE International Conference on Communications (ICC), IEEE, 2020, pp. 1–7.

[190] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, M. Liyanage, The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions, in: 2020 2nd 6G Wireless Summit (6G SUMMIT), IEEE, 2020, pp. 1–5.

[191] C. de Alwis, H. K. Arachchi, A. Fernando, M. Pourazad, Content and Network-aware Multicast over Wireless Networks, in: 10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, IEEE, 2014, pp. 122–128.

[192] S. Raju, S. Boddepalli, N. Choudhury, Q. Yan, J. S. Deogun, Design and analysis of elastic handoff in cognitive cellular networks, in: 2017 IEEE International Conference on Communications (ICC), 2017, pp. 1–6. doi:10.1109/ICC.2017.7996835.

[193] E. Di Pascale, J. McMenamy, I. Macaluso, L. Doyle, Smart Contract SLAs for Dense Small-cell-as-a-service, arXiv preprint arXiv:1703.04502 (2017).

[194] J. Backman, S. Yrjölä, K. Valtanen, O. Mämmelä, Blockchain network slice broker in 5g: Slice leasing in factory of the future use case, in: 2017 Internet of Things Business Models, Users, and Networks, 2017, pp. 1–8. doi:10.1109/CTTE.2017.8260929.

[195] K. Valtanen, J. Backman, S. Yrjölä, Creating Value through Blockchain Powered Resource Configurations: Analysis of 5G Network Slice Brokering Case, in: 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), IEEE, 2018, pp. 185–190.

[196] P. Fernando, L. Gunawardhana, W. Rajapakshe, M. Dananjaya, T. Gamage, M. Liyanage, Blockchain-Based Wi-Fi Offloading Platform for 5G, in: 2020 IEEE International Conference on Communications Workshops (ICC Workshops), IEEE, 2020, pp. 1–6.

[197] S. Yrjölä, Decentralized 6G Business Models (2020).

[198] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, Y. Zhang, Blockchain and deep reinforcement learning empowered intelligent 5g beyond, IEEE Network 33 (2019) 10–17.

[199] A. Nag, A. Kalla, M. Liyanage, Blockchain-over-Optical Networks: A Trusted Virtual Network Function (VNF) Management Proposition for 5G Optical Networks, in: Asia Communications and Photonics Conference, Optical Society of America, 2019, pp. M4A–222.

[200] S. Raju, S. Boddepalli, S. Gampa, Q. Yan, J. S. Deogun, Identity Management using Blockchain for Cognitive Cellular Networks, in: 2017 IEEE International Conference on Communications (ICC), IEEE, 2017, pp. 1–6.

[201] P. Popovski, O. Simeone, Start Making Sense: Semantic Plane Filtering and Control for Post-5G Connectivity, arXiv preprint arXiv:1901.06337 (2019).

[202] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, Z. Ding, Blockchain Radio Access Network (B-RAN): Towards Decentralized Secure Radio Access Paradigm, IEEE Access 7 (2019) 9714–9723.

[203] S. Yrjölä, Analysis of Blockchain Use Cases in the Citizens Broadband Radio Service Spectrum Sharing Concept, in: International Conference on Cognitive Radio Oriented Wireless Networks, Springer, 2017, pp. 128–139.

[204] O. Duru, Z. Muhammad, Blockchain Roaming in the Maritime Industry, 2019. URL: https://splash247.com/blockchain-roaming-

in-the-maritime-industry/.

[205] Y. Wang, J. H. Han, P. Beynon-Davies, Understanding Blockchain Technology for Future Supply Chains: A Systematic Literature Review and Research Agenda, Supply Chain Management: An International Journal 24 (2019) 62–84.

[206] S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, J. Zhang, A Blockchain-Based Supply Chain Quality Management Framework, in: 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE), 2017, pp. 172–176. doi:10.1109/ICEBE.2017.34.

[207] A. Law, Smart Contracts and their Application in Supply Chain Management, Ph.D. thesis, Massachusetts Institute of Technology, 2017.

[208] Y. Yuan, F.-Y. Wang, Towards Blockchain-based Intelligent Transportation Systems, in: 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), IEEE, 2016, pp. 2663–2668.

[209] M. Nakasumi, Information Sharing for Supply Chain Management based on Block Chain Technology, in: 2017 IEEE 19th Conference on Business Informatics (CBI), volume 1, IEEE, 2017, pp. 140–149.

[210] K. Komathy, Verifiable and Authentic Distributed Blockchain Shipping Framework for Smart Connected Ships, Journal of Computational and Theoretical Nanoscience 15 (2018) 3275–3281.

[211] L. Ge, C. Brewster, J. Spek, A. Smeenk, J. Top, F. van Diepen, B. Klaase, C. Graumans, M. d. R. de Wildt, Blockchain for Agriculture and Food: Findings from the Pilot Study, 2017-112, Wageningen Economic Research, 2017.

[212] S. Green, Decentralized Agriculture: Applying Blockchain Technology in Agri-Food Markets, Master's thesis, Faculty of Graduate Studies, 2018.

[213] M. Kim, B. Hilton, Z. Burks, J. Reyes, Integrating Blockchain, Smart Contract-Tokens, and IoT to Design a Food Traceability Solution, in: 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2018, pp. 335–340. doi:10.1109/IEMCON.2018.8615007.

[214] L. E. Cartier, S. H. Ali, M. S. Krzemnicki, Blockchain, Chain of Custody and Trace Elements: An Overview of Tracking and Traceability Opportunities in the Gem Industry., Journal of Gemmology 36 (2018).

[215] C. Gutierrez, A. Khizhniak, A Close Look at Everledger–How Blockchain Secures Luxury Goods, 2017.

[216] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, B. Stiller, A blockchain-based Architecture for Collaborative DDoS Mitigation with Smart Contracts, in: IFIP International Conference on Autonomous Infrastructure, Management and Security, Springer, Cham, 2017, pp. 16–29.

[217] W. Shao, Z. Wang, X. Wang, K. Qiu, C. Jia, C. Jiang, Lsc: Online auto-update smart contracts for fortifying blockchain-based log systems, Information Sciences 512 (2020) 506–517.

[218] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, M. Bertoncini, Blockchain-based Decentralized Management of Demand Response Programs in Smart Energy Grids, Sensors 18 (2018) 162.

[219] I. Kounelis, G. Steri, R. Giuliani, D. Geneiatakis, R. Neisse, I. Nai-Fovino, Fostering Consumers' Energy Market through Smart Contracts, in: 2017 International Conference in Energy and Sustainability in Small Developing Economies (ES2DE), IEEE, 2017, pp. 1–6.

[220] O. Van Cutsem, D. H. Dac, P. Boudou, M. Kayal, Cooperative energy management of a community of smart-buildings: A blockchain approach, International Journal of Electrical Power & Energy Systems 117 (2020) 105643.

[221] K. Tanaka, K. Nagakubo, R. Abe, Blockchain-based Electricity Trading with Digital Grid Router, in: 2017 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2017, pp. 201–202. doi:10.1109/ICCE-China.2017.7991065.

[222] P. Danzi, M. Angjelichinoski, Č. Stefanović, P. Popovski, Distributed proportional-fairness control in microgrids via blockchain smart contracts, in: 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2017, pp. 45–51.

[223] S. Cheng, B. Zeng, Y. Huang, Research on Application Model of Blockchain Technology in Distributed Electricity Market, in: IOP Conference Series: Earth and Environmental Science, volume 93, IOP Publishing, 2017, p. 012065.

[224] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, C. Weinhardt, A Blockchain-based Smart Grid: Towards Sustainable Local Energy Markets, Computer Science-Research and Development 33 (2018) 207–214.

[225] M. Mylrea, S. N. G. Gourisetti, Blockchain for Smart Grid Resilience: Exchanging Distributed Energy at Speed, Scale and Security, in: 2017 Resilience Week (RWS), IEEE, 2017, pp. 18–23.

[226] H. Malik, A. Manzoor, M. Ylianttila, M. Liyanage, Performance Analysis of Blockchain based Smart Grids with Ethereum and Hyperledger Implementations, in: IEEE International Conference on Advanced Networks and Telecommunications Systems, 2019, pp. 1–5.

[227] A. Dorri, M. Steger, S. S. Kanhere, R. Jurdak, Blockchain: A Distributed Solution to Automotive Security and Privacy, IEEE Communications Magazine 55 (2017) 119–125.

[228] K. L. Brousmiche, T. Heno, C. Poulain, A. Dalmieres, E. B. Hamida, Digitizing, Securing and Sharing Vehicles Life-cycle over a Consortium Blockchain: Lessons learned, in: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 2018, pp. 1–5.

[229] G. Bohl, J. F. Dickson, Private Blockchains in Automotive Safety (2017).

[230] G. Ongena, K. Smit, J. Boksebeld, G. Adams, Y. Roelofs, P. Ravesteyn, Blockchain-based Smart Contracts in Waste Management: A Silver Bullet?, in: Bled eConference, 2018, p. 19.

[231] B. Fu, Z. Shu, X. Liu, Blockchain Enhanced Emission Trading Framework in Fashion Apparel Manufacturing Industry, Sustainability 10 (2018) 1105.

[232] Y.-P. Lin, J. Petway, W.-Y. Lien, J. Settele, Blockchain with Artificial Intelligence to Efficiently Manage Water Use under Climate Change, 2018.

[233] H. Cardeira, Smart contracts and their applications in the construction industry, 2015.

[234] Ž. Turk, R. Klinc, Potentials of Blockchain Technology for Construction Management, Procedia engineering 196 (2017) 638–645.

[235] R. J. Reisman, Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy, 2019.

[236] K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, A. Rastogi, T. Sibut-Pinote, N. Swamy, S. Zanella-Béguelin, Short Paper: Formal Verification of Smart Contracts, in: Proceedings of the 11th ACM Workshop on Programming Languages and Analysis for Security (PLAS), in conjunction with ACM CCS, 2016, pp. 91–96.

[237] G. Bigi, A. Bracciali, G. Meacci, E. Tuosto, Validation of decentralised smart contracts through game theory and formal methods, in: Programming Languages with Applications to Biology and Security, Springer, 2015, pp. 142–161.

[238] I. Sergey, A. Kumar, A. Hobor, Scilla: a Smart Contract Intermediate-level Language, arXiv preprint arXiv:1801.00687 (2018).

[239] T. Abdellatif, K.-L. Brousmiche, Formal Verification of Smart Contracts based on Users and Blockchain Behavior Models, in: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 2018, pp. 1–5.

[240] Z. Nehai, P.-Y. Piriou, F. Daumas, Model-checking of Smart Contracts, in: IEEE International Conference on Blockchain, 2018, pp. 980–987.

[241] S. K. Lahiri, S. Chen, Y. Wang, I. Dillig, Formal Specification and Verification of Smart Contracts for Azure Blockchain, arXiv preprint arXiv:1812.08829 (2018).

[242] I.-C. Lin, T.-C. Liao, A Survey of Blockchain Security Issues and Challenges., IJ Network Security 19 (2017) 653–659.

[243] P. Tsankov, A. Dan, D. Drachsler-Cohen, A. Gervais, F. Buenzli, M. Vechev, Securify: Practical Security Analysis of Smart Contracts, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2018, pp. 67–82.

[244] M. Suiche, Porosity: A Decompiler for Blockchain-based Smart Contracts Bytecode, DEF CON 25 (2017) 11.

[245] Exploratory Analysis of Block Chain Security Vulnerabilities, author=Manjunath, Pavan and Shah, Pritam Gajkumar, Australian Journal of Wireless Technologies, Mobility and Security e-ISSN 2200-1883 1 (2019) 5–10.

[246] L. Brent, A. Jurisevic, M. Kong, E. Liu, F. Gauthier, V. Gramoli, R. Holz, B. Scholz, Vandal: A Scalable Security Analysis Framework for Smart Contracts, arXiv preprint arXiv:1809.03981 (2018).

[247] M. Mossberg, F. Manzano, E. Hennenfent, A. Groce, G. Grieco, J. Feist, T. Brunson, A. Dinaburg, Manticore: A User-Friendly Symbolic Execution Framework for Binaries and Smart Contracts, arXiv preprint

arXiv:1907.03890 (2019).

[248] N. Atzei, M. Bartoletti, T. Cimoli, A Survey of Attacks on Ethereum Smart Contracts (sok), in: International Conference on Principles of Security and Trust, Springer, 2017, pp. 164–186.

[249] K. Wüst, A. Gervais, Ethereum Eclipse Attacks, Technical Report, ETH Zurich, 2016.

[250] R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, A. Singh, Empirical Vulnerability Analysis of Automated Smart Contracts Security Testing on Blockchains, in: Proceedings of the 28th Annual International Conference on Computer Science and Software Engineering, IBM Corp., 2018, pp. 103–113.

[251] S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko, Y. Alexandrov, Smartcheck: Static Analysis of Ethereum Smart Contracts, in: 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), IEEE, 2018, pp. 9–16.

[252] I. Grishchenko, M. Maffei, C. Schneidewind, EtherTrust: Sound Static Analysis of Ethereum Bytecode, Technische Universität Wien, Tech. Rep (2018).

[253] I. Nikolić, A. Kolluri, I. Sergey, P. Saxena, A. Hobor, Finding the greedy, prodigal, and suicidal contracts at scale, in: Proceedings of the 34th Annual Computer Security Applications Conference, ACM, 2018, pp. 653–663.

[254] C. Liu, H. Liu, Z. Cao, Z. Chen, B. Chen, B. Roscoe, ReGuard: Finding Reentrancy Bugs in Smart Contracts, in: Proceedings of the 40th International Conference on Software Engineering: Companion Proceeedings, ACM, 2018, pp. 65–68.

[255] B. Jiang, Y. Liu, W. Chan, Contractfuzzer: Fuzzing Smart Contracts for Vulnerability Detection, in: Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering, ACM, 2018, pp. 259–269.

[256] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, ACM, 2016, pp. 254–269.

[257] H. Liu, C. Liu, W. Zhao, Y. Jiang, J. Sun, S-gram: Towards Semantic-aware Security Auditing for Ethereum Smart Contracts, in: Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering, ACM, 2018, pp. 814–819.

[258] C.-F. Liao, C.-J. Cheng, K. Chen, C.-H. Lai, T. Chiu, C. Wu-Lee, Toward a service platform for developing smart contracts on blockchain in bdd and tdd styles, in: 2017 IEEE 10th Conference on Service-Oriented Computing and Applications (SOCA), IEEE, 2017, pp. 133–140.

[259] G. Destefanis, M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali, R. Hierons, Smart Contracts Vulnerabilities: A Call for Blockchain Software Engineering?, in: 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), IEEE, 2018, pp. 19–25.

[260] K. Delmolino, M. Arnett, A. Kosba, A. Miller, E. Shi, Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab, in: International Conference on Financial Cryptography and Data Security, Springer, 2016, pp. 79–94.

[261] Z. Gao, V. Jayasundara, L. Jiang, X. Xia, D. Lo, J. Grundy, Smartembed: A tool for clone and bug detection in smart contracts through structural code embedding, in: 2019 IEEE International Conference on Software Maintenance and Evolution (ICSME), IEEE, 2019, pp. 394–397.

[262] S. Wang, C. Zhang, Z. Su, Detecting nondeterministic payment bugs in ethereum smart contracts, Proceedings of the ACM on Programming Languages 3 (2019) 1–29.

[263] C. F. Torres, J. Schütte, R. State, Osiris: Hunting for integer bugs in ethereum smart contracts, in: Proceedings of the 34th Annual Computer Security Applications Conference, 2018, pp. 664–676.

[264] S. R. Niya, F. Shüpfer, T. Bocek, B. Stiller, Setting up Flexible and Light Weight Trading with Enhanced User Privacy using Smart Contracts, in: NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2018, pp. 1–2.

[265] D. Chatzopoulos, S. Gujar, B. Faltings, P. Hui, Privacy Preserving and Cost Optimal Mobile Crowdsensing using Smart Contracts on Blockchain, in: 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), IEEE, 2018, pp. 442–450.

[266] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, Provchain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability, in: Proceedings of the 17th IEEE/ACM international symposium on cluster, cloud and grid computing, IEEE Press, 2017, pp. 468–477.

[267] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, in: 2016 IEEE Symposium on Security and Privacy (SP), 2016, pp. 839–858. doi:10.1109/SP.2016.55.

[268] M. Al-Bassam, A. Sonnino, S. Bano, D. Hrycyszyn, G. Danezis, Chainspace: A sharded smart contracts platform, arXiv preprint arXiv:1708.03778 (2017).

[269] R. Yuan, Y.-B. Xia, H.-B. Chen, B.-Y. Zang, J. Xie, Shadoweth: Private Smart Contract on Public Blockchain, Journal of Computer Science and Technology 33 (2018) 542–556.

[270] F. Benhamouda, S. Halevi, T. T. Halevi, Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation, IBM Journal of Research and Development (2019).

[271] G. Zyskind, O. Nathan, A. Pentland, Enigma: Decentralized computation platform with guaranteed privacy, arXiv preprint arXiv:1506.03471 (2015).

[272] J. Poon, V. Buterin, Plasma: Scalable Autonomous Smart Contracts, White paper (2017) 1–47.

[273] S. Forestier, D. Vodenicarevic, Blockclique: Scaling Blockchains through Transaction Sharding in a Multithreaded Block Graph, arXiv preprint arXiv:1803.09029 (2018).

[274] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, P. Saxena, A Secure Sharding Protocol for Open Blockchains, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 17–30.

[275] M. Zamani, M. Movahedi, M. Raykova, Rapidchain: Scaling Blockchain via Full Sharding, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2018, pp. 931–948.

[276] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, B. Ford, Omniledger: A Secure, Scale-out, Decentralized Ledger via Sharding, in: 2018 IEEE Symposium on Security and Privacy (SP), IEEE, 2018, pp. 583–598.

[277] N. Grech, M. Kong, A. Jurisevic, L. Brent, B. Scholz, Y. Smaragdakis, Madmax: Surviving Out-of-Gas Conditions in Ethereum Smart Contracts, Proceedings of the ACM on Programming Languages 2 (2018) 116.

[278] I. Grishchenko, M. Maffei, C. Schneidewind, A Semantic Framework for the Security Analysis of Ethereum Smart Contracts, in: International Conference on Principles of Security and Trust, Springer, 2018, pp. 243–269.

[279] P. Otte, M. de Vos, J. Pouwelse, TrustChain: A Sybil-resistant Scalable Blockchain, Future Generation Computer Systems (2017).

[280] P. Mell, J. Kelsey, J. Shook, Cryptocurrency Smart Contracts for Distributed Consensus of Public Randomness, in: International Symposium on Stabilization, Safety, and Security of Distributed Systems, Springer, 2017, pp. 410–425.

[281] S. Popejoy, The Pact Smart Contract Language, June-2017.[Online]. Available: http://kadena. io/docs/Kadena-PactWhitepaper. pdf (2016).

[282] L.-D. Ibáñez, K. O'Hara, E. Simperl, On Blockchains and the General Data Protection Regulation (2018).

[283] A. Juels, A. Kosba, E. Shi, The Ring of Gyges: Investigating the Future of Criminal Smart Contracts, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 283–295.

[284] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, E. W. Felten, Arbitrum: Scalable, Private Smart Contracts, in: 27th {USENIX} Security Symposium ({USENIX} Security 18), 2018, pp. 1353–1370.

[285] F. Zhang, E. Cecchetti, K. Croman, A. Juels, E. Shi, Town crier: An authenticated data Feed for Smart Contracts, in: Proceedings of the 2016 aCM sIGSAC conference on computer and communications security, ACM, 2016, pp. 270–282.

[286] R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson, A. Juels, A. Miller, D. Song, Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts (2019).

# Survey on Blockchain based Smart Contracts:Applications, Opportunities and Challenges

Author Biographies

**Tharaka Hewa**

**Tharaka Hewa** is currently working as a Doctoral Student in Centre for Wireless Communication, University of Oulu, Finland. He received his Bachelor's degree in Computer Science from the University of Colombo School of Computing, Sri Lanka in 2013, and Master of Science in Information Security (Distinction) from the University of Colombo School of Computing in 2016. From 2012 to 2017, he worked in a leading digital payment solution provider in Sri Lanka as a Senior Software Engineer. Within his career in the industry, he contributed to many projects in mobile banking, internet banking, PKI, Automated Teller Machines and involved in the system integration and support. He is a certified engineer for SafeNet Luna SA 6.0 HSM. In 2017, he joined Nanyang Technological University as a Research Associate. He played a vital role in many research and implementation projects in different contexts. He contributed to cybersecurity and digital payment systems and co-authored 2 publications related to the blockchain applications in the industry with contributing to 1 patent. He contributed to ongoing research and implementation projects including blockchain for 3D printing, agriculture, luxury watches, music asset monetization, and aviation. In 2019 he joined Centre for Wireless Communication and his research focus in developing a blockchain-based platform as a service for private 5G networks. He contributes to ongoing research on blockchain, IoT, and PKI.

Tharaka Hewa's research interests are Blockchain, PKI, 5G, Banking Systems Security, Healthcare Security, and Smart Cities.

**Mika Ylianttila**

**Mika Ylianttila** (M. Sc, Dr.Sc, eMBA) is a full-time associate professor (tenure track) at the Centre for Wireless Communications (CWC), at the Faculty of Information Technology and Electrical Engineering (ITEE), University of Oulu, Finland. He leads NSOFT (Network security and softwarization) research group, at CWC Networks and Systems research unit, which studies and

develops secure, scalable and resource-efficient techniques for 5G and beyond 5G systems. He is the director of communications engineering doctoral degree program. Previously he was the director of Center for Internet Excellence (2012-2015), vice director of MediaTeam Oulu research group (2009-2011) and professor (pro tem) in computer science and engineering (2005-2010). He received his doctoral degree on Communications Engineering at the University of Oulu in 2005. He has coauthored more than 170 international peer-reviewed articles. His research interests include edge computing, network security, network virtualization and software-defined networking. He is a Senior Member of IEEE, and Editor in Wireless Networks journal.

**Madhusanka Liyanage**

**Madhusanka Liyanage** is currently an adjunct professor at the University of Oulu, Finland. He received his B.Sc. degree (First Class Honours) in electronics and telecommunication engineering from the University of Moratuwa, Moratuwa, Sri Lanka, in 2009, the M.Eng. degree from the Asian Institute of Technology, Bangkok, Thailand, in 2011, the M.Sc. degree from the University of Nice Sophia Antipolis, Nice, France, in 2011, and the Ph.D. degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. From 2011 to 2012, he worked a Research Scientist at the I3S Laboratory and Inria, Sophia Antipolis, France. He has been a Visiting Research Fellow at the Department of Computer Science, University of Oxford, Data61, CSIRO, Sydney, Australia, the Infolabs21, Lancaster University, U.K., and Computer Science and Engineering, The University of New South Wales during 2015-2018.

He has co-authored over 50 publications including two edited books with Wiley and one patent. He is the demo co-chair of WCNC2018 and publicity chair of ISWCS 2019. He served as a Technical program Committee Members at EAI M3Apps 2016, 5GU 2017, EUCNC 2017, EUCNC 2018, 5GWF 2018, MASS 2018, MCWN 2018, WCNC 2019, EUCNC 2019 conferences and Technical program co-chair in SecureEdge workshop at IEEE CIT2017 conference and Blockchain for IoT workshop at IEE Globecom 2018. He has also served as the session chair in a number of other conferences including IEEE WCNC 2013, CROWNCOM 2014, 5GU 2014, IEEE CIT 2017, IEEE PIMRC 2017, 5GWF 2018, Bobynet 2018, Globecom 2018. Moreover, He has received two best Paper Awards in the areas of SDMN security (at NGMAST 2015) and 5G Security (at IEEE CSCN 2017). Additionally, he has been awarded two research grants and 21 other prestigious awards/scholarships during his research career.

Dr. Liyanage has worked for more than twelve EU, international and national projects in ICT domain. He held responsibilities as a leader of work packages in several national and EU projects. Currently, he is the Finnish national coordinator for EU COST Action CA15127 on resilient communication services. In addition, he is/was serving as a management committee member for four other EU COST action projects namely EU COST Action IC1301, IC1303, CA15107 and CA16226. Liyanage has over three years' experience in research project management, research group leadership, research project proposal preparation, project progress documentation and graduate student co-supervision/mentoring, skills. In 2015, 2016 and 2017, he won the Best Researcher Award at the Centre for Wireless Communications, University of Oulu for his excellent contribution in project management and dissemination activities. Additionally, two of the research projects (MEVICO and SIGMONA projects) received the CELTIC Excellence Award in 2013 and 2017 respectively.

**Declaration of interests**

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: