2017 IEEE International Conference on AI & Mobile Services (AIMS)

Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging

Zhixong Chen
Mercy College
zxchen@ieee.org

Yixuan Zhu
Mercy College
yzhu@mercymavericks.edu

***Abstract*— This paper is to explore applications of the blockchain technology to the concept of "proof of X" such as proof of identity, proof of property ownership, proof of specific transaction, proof of college degree, proof of medical records, proof of academic achievements, etc. It describes a novel approach of building a decentralized transparent immutable secure personal archive management and service system. Personal archive is defined as a collection of various artifacts that reflect personal portfolio as well as personal unique identifications. Personal portfolio is beyond of a statement of personal achievement. It is an evidentiary document designed to provide qualitative and quantitative chronically documents and examples. Subjects can tag their information with proof, that is, certified by trusted entities or organizations like universities. Such proofs are associated with confidentiality levels exposed in the public domains. Personal identifications include biometrics as well as other multi-factors such as something the subject "has", the subject "knows" or the subject "acts". Stack holders in a consortium oriented blockchain network serve as verifiers and /or miners that provide their trusted services the delegated proof of stake. Such personal archive based system can be exploited to various applications including professional network like Linkedin, instant credit approval like alipay or live human from social bots like internet social media. A prototype simulation shows that such personal portfolio management and service system is feasible and immune to many ID attacks.**

Keywords—Personal Archive Service System, Digital Portfolio, Identification, Blockchain, Consortium Block Chain, Public and Private Key, Anonymous, Transparent, De-centralization

I. INTRODUCTION

Personal archive service system (PASS) is defined as a collection of digital artifacts as well as a collection of service tools. A personal digital artifact (PDA) is a digital form of personal achievements with evidentiary documents (PAE) or of personal identifications (PID) that can be used to uniquely identify a person. Examples of PAE are such as personal education, experiences, training, degree, diploma, academic transcripts and various certificates. Personal wealth like property value, bank balance, investments can also be examples of PAE. Typical examples of PID are biometric measures from the person like finger prints, iris and vein. Other information known only to the person, physical objects owned by the person can be examples of PID. Behavior patterns, personal reflection and characteristics are also considered as examples of PID.

The collection of PAEs are similar to personal portfolio (PP). It is associated with timeline that assembles a specific characteristics of a person. PP is distinct from resume in that it is more of inclusive and expanding than a line of statements in resume.

To be useful and trustful, these PDAs need to be verified by a third party who should have direct knowledge of these claimed artifacts. For example, a university can provide official transcripts to their graduates. A landlord is able to provide a letter of reference to their tenants. No other entities can do that.

We define various roles in this process. We use the term "subject" to be a person or a user who is building his or her collection of PDAs, "certifier" to be an institute or an entity that provides certification, "inquisitor" to be an agent or organization who provides service of investigation and obtaining relevant proof of any particular subject, and "client" to a person or organization using professional services provided by "inquisitor". For example, for a potential candidate to be hired by a company, the candidate is a subject, the company is a client who needs to hire a third party to verify all the information provided by the subject. The third party is the inquisitor and the company is a client of the inquisitor. The inquisitor needs to contact various certifiers such as universities who gain education, companies who used to work, or organizations who issue other certifications.

This process of verifying PDAs by inquisitors is often time consuming. It is also repeated every time a client makes a request. In some cases, it obtains information beyond the consent given by the subject. Therefore, it poses a threat of privacy. Moreover, it is essentially a model of centralized system that can potentially cause a point of failure, a point of bottleneck, a point of confusion and a point of abuse. For example, clearance for teaching when hiring an adjunct by a third party takes time. In some extreme cases we have experienced that the semester starts while the clearance is still pending. Another example is about name change by a subject. Without revealing its previous name used, the subject is hard to get verified. We see a case that a subject wants an institution to issue a new diploma due to name change. It is usually a mission impossible task although in this case the subject has all other IDs that remain the same just name difference.

But, the process of verification is becoming increasing necessary and a must. We have observed resume padding is becoming more epidemic [1]. Resume padding is to add false or exaggerated information to a resume to enhance credentials for a job. More than 40% of resumes inflates their salary, 33% inaccurate job description, 29% altered employment dates, 27%

978-1-5386-1999-5/17 $31.00 © 2017 IEEE
DOI 10.1109/AIMS.2017.31

falsified references, and 21% fraudulent degrees. Hence, we can image that the burden of requiring verification is very heavy.

Recently, blockchain technology, first introduced in bitcoin [20] as an innovative payment network and a new kind of money, is being applied to financial related industrials. Many other fields such as supply chain, manufacture, Internet of Things are exploiting it as well. [21-22 for example]. The key features from using the blockchain technology are its decentralized, consensus based shared ledger, smart contract, high transparency yet high privacy. The idea to have secure storage and transmission of digitally signed documents with a super audit trail in immutable document exchange networks is emerging in trade finance, shipping, and insurance, where everyone has the same demand to validate the identity of people and assets. It does not need a third party as an intermediary or authority for verification, cleaning house or any other purposes. It is being used in building a secure anonymous yet transparent immutable ID Service [33].

Personal Archive Service System (PASS) proposed in this paper is to use blockchain technology to exploit its desirable features such as immutable, transparency, anonymous and public consensus. The subject controls its own PDAs and makes decision to whom to release. Figure 1 illustrates the general infrastructure and architecture view of a PASS under blockchain. The subject, represented by icon has its own repository or wallet that aggregates all its relevant PDAs. The certifiers issue certificates to its owners as well as to a trusted network. It does such certificates once for everyone involved and should not be bothered anymore. There is no need to have a third party or an inquisitor. They also pass the certificates to a consortium oriented block chain network that the trust is developed in a delegated proof of stake. A client makes a request to the subject and gain access to those granted PDAs.

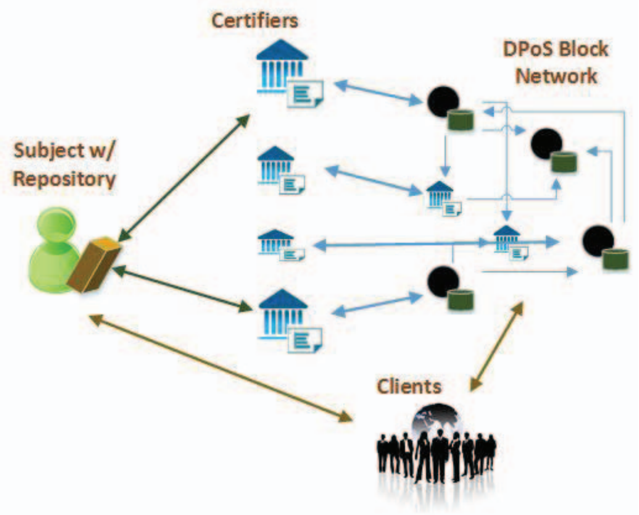

Figure 1: Architecture of PASS

Our main contributions is to propose a framework of using blockchain technology to build a personal archive that associated certifications. It preserves the authenticity, accuracy and transparency while keeps privacy. Inquisitors are no longer needed. A subject can decide what to reveal to whom and when based on the nature of the request. When a request is more of academic achievement, any PDAs associated with such tag can be unlocking and revealed. When a request is of identification, the subject can unlocking those PDAs such as biometrics. A client can gain access to the PDAs immediately and makes decision accordingly. Moreover, tools and services provided by the PASS can make any projects related to personal growth and timeline much easier.

The following section reviews the latest development of the concept "*proof of X*" using blockchain technology where X can be anything like identity, property ownership, specific transaction, college degree, medical records, and academic achievements. The next section will discuss the PASS, a personal archive service system upon which subjects can build their personal archives timely and accurately. They are certified so that they do not need to be verified every time to be used. The PASS is transpierce while maintains privacy. The last portion is devoted to the discussion on opportunity, challenging and future applications.

II. Literature review

Main issues of building personal digital artifacts (PDAs) are the verification process and the trustworthiness. Statistically as indicated in section I, more than 30% of job seekers modified their diploma information. 70% inflate their achievement [1].

Various efforts are made to build a level of verification and certification around academic achievement. Open Badge idea is one of them. The standard working group for open badges as it stated in its web site [2] communicates skills and achievements by providing visual symbols of accomplishments packed with verifiable data and evidence that can be shared across the web. Open Badges enable subjects manage their own learning achievements. The goal of the working group is to move the specifications more towards a standard that is clearer and easier to align with, maintain, and build from. Acclaim [3] is a digital badging platform based on the Open Badge Standard and backed by Pearson. Acclaim has issued millions of badges from reputable organizations like IBM for career-advancing achievements that help individuals move forward professionally. A badge issued through Acclaim is a digital representation of a learning outcome, experience or competency. These badges can be shared and verified online in a way that is easy and secure. They contain detailed information that provides context around what exactly was achieved, which organization recognizes the achievement, and the individual who earned the recognition. The services provided have their merits. The main shortcoming is its centralized model.

Sony Global Education announces that it will develop technology using blockchain for open sharing of academic proficiency and progress records on 2016 [4]. It is going to leverage blockchain's secure properties to realize encrypted transmission of data - such as an individual's academic proficiency records and measures of progress - between two specified parties. The actual working flow is yet to be seen and needs to be tested.

ID system is an aged long problem. W3 identifies seven general requirements for a global identity management service [9]: portability and Interoperability, extensibility, negotiated privacy and security, accountability, distributed registration authority, distributed certification authority and independent governing authority. Such service must use globally unique identifiers in a common interchange format, support extensible mapping to these identifiers from other commonly used identifiers and use a common protocol for asserting and authenticating a global identity. It must support global vocabulary definition as well as distributed local vocabulary definition. It needs support anonymity and pseudonymity for protection of personal privacy. So the aanonymity and pseudonymity for protection of personal privacy is under the purview of privacy and security.

ID system should support both hierarchical and peer-to-peer registration models. The governing authority should be chartered as an international non-profit organization so it is industry-, vendor-, and government-neutral in all respects. It should set both technical and operational standards for the service, as the two are tightly intertwined. It should manage global vocabulary development for universal identity attributes and global protocol control structures. It should set the accountability terms for all agents, including registration and certification authorities. It should serve as an impartial root authority for hierarchical registration or certification models.

OpenID with OpenID Connect [6-11] is to define and develop an open standard and decentralized authentication protocol. It enables relying parties (RP) to verify the identity of an end-user based on the authentication performed by OpenID provider (OP) or Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner. By allowing users to be authenticated through a third party service, it eliminates the need for webmasters to provide their own ad hoc login systems and a separate identity and password.

OAuth [19] is an open protocol to allow secure authorization from web. It enables a third party application to obtain specific access rights through http service. But it does not provide ID management and verification. OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol.

While OAuth enables third party authorization service, it is still centralized in terms of OpenID Provider. And users have to reveal many private information in order to be authenticated. It also poses a single point of failure. Moreover, it is against the very nature of internet that not a single central authority that controls who can do what.

Multiple biometric specific information can be used to identify human being in a very high accuracy [8, 32, 33]. This is particularly useful in the social media applications in which a user can be anonymous but needs to be stamped as a real human rather than a bunch of social bots. Therefore, results such as sentiment or poll from a social media application can represent the real situations and not skewed by social bots.

Some web applications like taskstream [6] provide user a platform to build personal portfolio. It can track the progress in particular projects and record reflection on particular topics. These applications can serve as a way to show a trace of personal growth that can provide a provenance of particular skills.

In [35], the author proposed ideas of using blockchain to prove identities in the digital world without centralized database in that it leads to a natural monopoly that everyone has to use. Whereas a decentralized system follows a common protocol that allows individuals to add new transactions and distribute them using peer-to-peer architecture with a super audit trail. A subject can give controlled key usage to clients such as banks, insurers, or governments who want to inspect the documents with smart contracts. A smart contract is a piece of code recorded in the common blocks. The contract can restrict the number or timing of inquisitions and record them all for the subject.

III. Structure of PASS

A. Artifacts, Portfolio and Archive

A personal digital artifact (PDA) is a piece of signed digital document that contains the following tags or fields:

- PDA-ID: an index generated by the system
- PDA-Type: Either personal achievements with evidentiary documents (PAE) or personal identifications (PID). It follows the sub-type such as diploma, degree, skills, and biometric measure. They should be standardized codes eventually.
- PDA-Description: a string to describe the nature of the PDA
- PDA-Subject: name of the person who owns the PDA
- PDA-Certifier: person or organization who issues certification toward this PDA
- PDA-Date-Start: the starting date of the PDA
- PDA-Date-End: the completion date of the PDA
- PDA-Date-Validation: optional date that the PDA is valid
- PDA-Comment: optional field
- PDA-Key-Cert: the public key associate with the certifier
- PDA-Key-Sub: the public key generated for the subject and this particular PDA. The private key is kept by the subject in its application
- PDA-Unique: used by the certifier to verify the ownership of this PDA. Date of Birth, Student ID or Universal ID, and/or something known only to the subject. It can be multiple fields required by the Certifier
- PDA-Data: data needed by the certifier. For PID type, it could be a specific biometric information. For PAE, it could be a scan of original certificate (hard copy)

Personal portfolio (PP) is a collection of PDAs whose PDA-type is under PAE (personal achievements with evidentiary documents). Personal identifications (PID) is a collection of PDAs whose PDA-type is under PID. Therefore PA is a union of PP and PIDs. Symbolically,

$$PA = \{P_p, P_{id}\},$$

where

$$P_p = \{PDA_{PAE1}, PDA_{PAE2}, \cdots, PDA_{PEAn}\}$$

and

$$P_{id} = \{PDA_{PID1}, PDA_{PID2}, \cdots, PDA_{PIDm}\}.$$

B. Servcie Tools

A service tool is a piece of code that performs a specific task required by the PP. It should include the following fields.

- ST-ID: an index generated by the system
- ST-Type: the nature of the service such as inquisitor, manager, or others.
- ST-Description: a string to describe the nature of the service
- ST-Input: Service conditions and parameters
- ST-Output: service results
- ST-Condition: under what condition and/or privilege the service should be performed
- ST-Creator: person or organization who issues the tool
- ST-Date: the date the service in place
- ST-Comment: optional field
- ST-Language: specific language that implements the tool.

A collection of service tools is denoted as T. It covers a variety of the services needed to make the PA workable. For example, requesting for a certificate, aggregating and synchronizing PP in local repository or wallet from public ledger, granting permission to a specific party to inspect PDA. Again, we can use the following notation to illustrate the set of tools.

$$T = \{ST_1, ST_2, \cdots, ST_n\}.$$

Hence, PASS can be symbolized as

$$PASS = \{PA, T\}$$

C. Subject, Inquisitor, Certifier, Client, Stake

The paper uses the following terms to describe a blockchain based distributed peer to peer network.

- The term "subject" is a person that is being discussed about his or her PDAs
- The term "certifier" is an institute or an entity that provides certification
- The term "inquisitor" is an agent or organization to investigate and get relevant proof
- The term "client" is a person or an organization that uses professional services (by "inquisitor").
- The term "stake node" is a special node in a consortium oriented block chain network. The trust is developed in a delegated proof of stake. It is like "Mining and Verification" in a bitcoin network.

For example, for a potential candidate to be hired by a company, the candidate is the subject, the company needs to hire a third party to verify all the information provided by the subject. The third party is the inquisitor and the company is a client of the inquisitor. The inquisitor needs to contact various certifiers such as universities who gain education, companies who used to work, or organizations who issue other certifications.

D. Initial Trust and Block of the Consortium Network

In general, the initial block or the first block in a blockchain, coined as initial state of a p2p network, is a difficult task. It needs an acceptable assumption by all peers. PASS adopts a consortium network in which states with certain reputation are included or voted for. Therefore, we can assume such initial block includes data structure in PASS and initial stakes exclusively. A Certifier can be one of the stakes but it does not need to be. To become a trusted certifier, the certifier needs to provide Stakes with its identity.

E. Delegated Proof of Stake (DPoS)

Proof of work (PoW) is a consensus algorithm used in bitcoin network. PoW is done through mining that is the main process of the decentralized clearing house, by which transactions are validated and cleared. Mining secures the bitcoin system and enables the emergence of network-wide consensus without a central authority. The competition to solve the proof-of-work algorithm to earn reward and the right to record transactions on the blockchain is the basis for bitcoin security model.

A more efficient consensus algorithm is Delegated Proof of Stake (DPoS). It is a variant of the Proof of Stake (PoS). Both were developed in order to reduce the cost and inefficient electricity usage associated with PoW. PoS allows every wallet which contains coins to 'stake', that is to participate in process of validating transactions and forming the distributed consensus and to earn coins in return. While in DPoS, every wallet which contains coins is able to vote for delegates, and it is these delegates who perform the function of validating transactions and maintaining the blockchain and take the transaction fees as profit. It is more efficient than PoS.

PASS uses DPoS. Delegated stake holders make global ledger.

F. Biometrics and Uniqueness

Biometrics in computer science is the discipline of using metrics related to human characteristics to do identification, authentication and access control. Fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina are among them. Other metrics can be related to behaviors such as voice, typing rhythm and walking patterns and reaction to certain stimulant [for example, 25, and 26]. As technology advances, biometrics accuracy improves greatly. The time needed to get such information is much faster. The way to get them is easier. The price is much affordable.

One main direction in biometric authentication is to detect fake biometrics quickly so that such system can be used for real time authentication [25, 26]. In a different application scenario in which biometrics is being used to differentiate human being from robots. The challenging is to detect efficiently non-human biometrics such as digital modification from vast amount of human biometrics. This is particularly useful in applications that require anonymity but identifiable human natures. We are investigating various methods such as principal component analysis, wavelets, and correlations to test such classification [27, for instance].

Like other PDAs, the actual biometrics are being used but not stored in the network. The one way function makes it hard to get original biometrics. In addition, it needs multiple biometric information to reduce the probability of false positive. Thus, it makes impossible to have two persons to have two the same biometrics within certain thresholds.

IV. COMMUNICATION OF PASS

We now to describe the genera sequence for a subject to get a PDA. Figure 1 in section I demonstrates the work flow. The main idea is to use consortium blockchain in which registered nodes with delegated proof of stake can record the result in a global ledger. These nodes can be a collection of reputable organizations and companies. Certifiers need not be a node in the network. Their main function is to provide a certificate to the subject. For example, a graduate can ask an official transcript to be one of its PDA. The graduate is the subject. The university is the certifier. The blockchain network can be composed by a collections organizations who are reputable and have incentive to maintain the blocks. Universities, textbook publishers and training societies are ideal candidates. Clients can be any employers who are going to offer a job to the subject.

Figure 2 illustrates the time sequence for PDA-PAE. It is for illustration and has no detailed data structure exchange. Here, the subject makes a request of getting a certificate of one particular achievement to a certifier. The certifier is registered and authorized to issue such certificate. These information is encrypted by the pubic key of the certifier so that no one else can view the PDA. When the certifier gets the request, it verifies the request information in the PDA first and responds either denied or a certificate. In reality, communication between the subject and the certifier is more complicated than it is illustrated. It may ask for more evidences and specific information related to the PDA. It may ask for a proof of payment for the service before issuing the certificate. The certifier also sends the certificate to other nodes in the consortium blockchain network. The certificate includes information like the certifier digital signature with a unique number, a public key for the PDA, etc. can be viewed by other participants. Any node received the certificate will do the verification. It broadcast its verification to other nodes. The certificate will be recorded in the global ledger by a delegated stake.

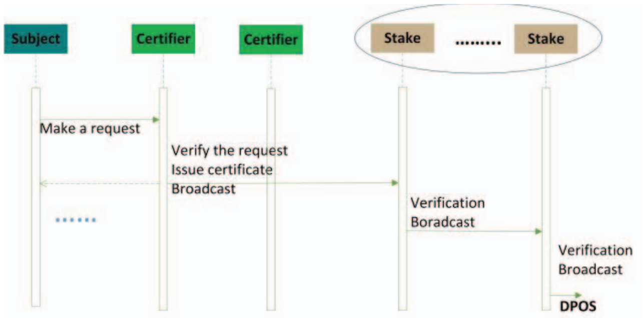

Figure 2: Time Sequence for PDA-PAE

Figure 3 demonstrates another example of the time sequence for PDA-PID. The PID is of biometric data or other id related information that the subject owns, knows and acts. Here we use the biometric measurement for illustration. Since it is shown statistically using two or more types of biometric information will reduce collision dramatically, the subject is asked to present at least two different types of biometric measures. In the end the ledger has all the verifiable subject information via consensus. So it requires a counter to count different types of biometric information.

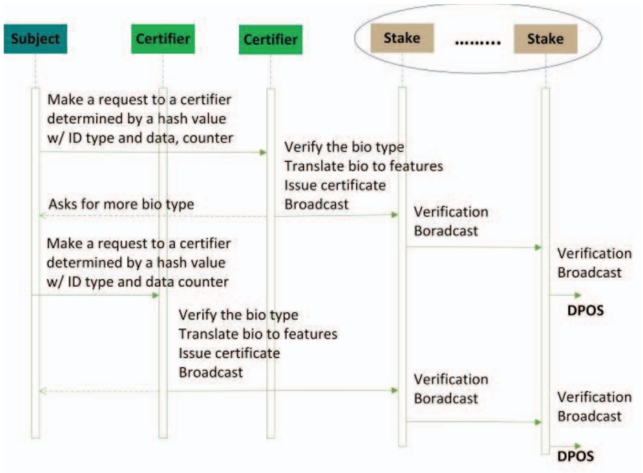

Figure 3: Time Sequence for PDA-PID

Detailed postfix operations can be referenced in [33]. Remember, there are various ways to realize the time sequence in figure 2 and figure 3.

V. SERVICE SYSTEM

An organization or entity (client) who needs some or all of the subject's PDAs in PA can negotiate with the subject directly rather than hires an inquisitor to do the verification. With a smart contract between the client and the subject, the client is able to inspect requested signed documents such as degree, transcript, working experiences, identifications, etc.

Figure 4 is an example of using PASS [32] in the case of internet social media. Internet social media lacks a layer of quality control to any postings, partially it has little background information on who is in the media circle or no control to whom allowed into the circle. Assessing trustworthiness of their postings is therefore based on postings themselves and their related information termed as signals. Most researches focus on exogenous signals such as hyperlink structures [11-18, 36]. Recent research is on endogenous signals such as correctness of factual information on postings [36]. Such signals result in placing high quality postings, mostly by experts in a relatively high ranking otherwise lost in a sea of postings. We have observed some novel practices on quality control of posting used in the internet social media are to associate with individual account. Examples are reacting to things (in Facebook [13]), scores (Karma in 14]) and reputation (some chat groups use reputation to decide who is allowed to make comments in 15]), personal online ratings based on the aggregated digital identity [7]. Some investigations and research are on who post what and when. During the process of sign in, some applications employ CAPTCHA [17], photo-based social authentication (Facebook), rate-limit violation (twitter, GitHub, Redit, etc.) and account connection property [16].

With the PASS, ID service can be provided in high confidence with the desired features a) real human being, b) no more alias account, c) anonymous and secure, d) transparent, e) immutable, f) consensus based de-centralized and g) revocable.

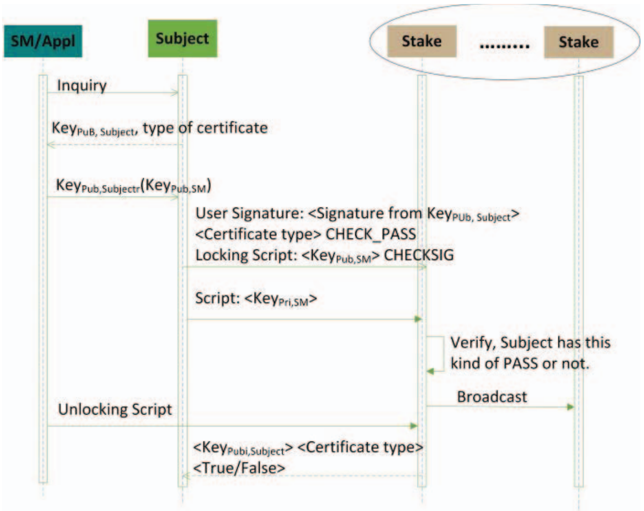
SM/Appl
Subject
Stake
....
Stake
Inquiry
$Key_{PuB, Subject}$, type of certificate
$Key_{Pub,Subjectr}(Key_{Pub,SM})$
User Signature: <Signature from $Key_{PUb, Subject}$>
<Certificate type> CHECK_PASS
Locking Script: <$Key_{Pub,SM}$> CHECKSIG
Script: <$Key_{Pri,SM}$>
Verify, Subject has this kind of PASS or not.
Broadcast
Unlocking Script
<$Key_{Pubi,Subject}$> <Certificate type>
<True/False>

Figure 4: PASS Service

The steps are as follows

1. An application such as an internet social media makes a request to the subject for feature verification;
2. The Subject sends its public key and relevant PDAs to the application;
3. The application returns its public key signed by subject's public key;
4. The subject passes its signed unlocking script, signature, list of PDAs with their types and methods to gain inspection of PDAs;
5. The subject also sends a locking script that includes the public key of the application for signature check. It is unlocked only when the signature matches the application;
6. A stake in the consortium P2P network makes check if the subject has such PDAs; It continues when they are existed;
7. The stake broadcasts to the rest of the stakes so they all can use this for verification;
8. The application sends the unlocking script with its signature;
9. The stake uses the unlocking script to pass back to the application if the verification is done successfully or failed.

As we see, such sequence of PASS can be generalized to any other applications who need to verify PDAs.

VI. Discussion

In this paper, we have illustrated a novel approach of personal document management using blockchain technology, PASS. PASS is exploiting the features from the blockchain well. Whenever a subject would like to make a trace of achievement or new characteristics, the subject can archive it right away rather than waiting for an inquisitor later on.

The opportunity for such application is pervasive. It can be used in online applications as well as other applications like employment and promotion. It eliminates a third party completely yet keeps its anonymity and accountability.

One main challenging in implementation is to find a collection of stakes who are reputable while have incentive in working on the network. It also needs a mechanism or protocol to vote in or vote out a stake. The weight of stake needs to be defined quantitatively.

Related challenging is to solicit well known organizations to be certifiers. That is these organizations need to move their manual process to electronic process and issue certificates digitally. The other side of the challenging is the threshold to reject an applicant for certifier.

In order to have wide adoption, standardization PDA structure and communication protocol are crucial. We know some PDAs are typical and easy to get certified. Some other PDAs are not. For example, it is a standard process to get a certified transcript. But, it is not easy to certify a reflection from a particular project conducted by particular personnel like professors. Reference letters usually serve the purpose. A detailed chronical project work can also serve the purpose. Therefore, transferring such reference into digital certification needs more work. We may leave a room for some PDAs without certification.

The last challenging seems pervasive, that is to keep the list of the unlocking keys in a safe place. Without them, there is no way to unlock PDAs and to be useful.

REFERENCES

[1] http://infographicsmania.com/resume-padding-statistics/

[2] Open badge, https://openbadges.org/

[3] Acclaim https://www.youracclaim.com

[4] Sony Global Education https://www.sonyged.com/ and https://www.sony.net/SonyInfo/News/Press/201602/16-0222E/index.html

[5] https://www1.taskstream.com/

[6] OpenID Connect, http://openid.net/connect/

[7] A. Yasin and L. Liu, "An Online Identity and Smart Contract Management System", *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, Atlanta, GA, 2016, pp. 192-198.

[8] X Luna Dong, et al., Knowledge-Based Trust: Estimating the Trustworthiness of Web Sources, 02/2015, https://arxiv.org/abs/1502.03519,

[9] Requirements for a Global Identity Management Service, April 2001, https://www.w3.org/2001/03/WSWS-popa/paper57

[10] W Gitt, R Compton and J Fernandez, Biological Information — What is It?, http://www.worldscientific.com/doi/pdf/10.1142/9789814508728_0001

[11] L Page, The PageRank Citation Ranking: Bringing Order to the Web, 1998

[12] https://en.wikipedia.org/wiki/PageRank

[13] https://www.facebook.com/help/like

[14] http://lesswrong.com/

[15] http://www.wechat.com/en/

[16] X Yang, Q Cao, M Sirivianos, SybilRank: Aiding the Detection of Fake Accounts in Large Scale Social Online Services, https://users.cs.duke.edu/~qiangcao/sybilrank_project/index.html

[17] L v Ahn, et al, reCAPTCHA: Human-Based Character Recognition via Web Security Measures". Science, September 12, 2008. pp 1465-1468.

[18] S Yardi, N Feamster and A Bruckman, Photo-based authentication using social networks, Proceedings of the first workshop on Online social networks, WOSN'08 PP 55-60

[19] OAuth: https://kantarainitiative.org/about/principles/

[20] S Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, https://bitcoin.org/bitcoin.pdf

[21] Hyperledger https://www.hyperledger.org/

[22] R3 CEV Financial Consortium http://www.r3cev.com/

[23] The Enterprise Ethereum Alliance (EEA) http://entethalliance.org/

[24] DAO,decentralized autonomous organization https://forum.daohub.org/

[25] Chien Le, A Survey of Biometrics Security Systems, 2011, http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet.pdf

[26] L Lai, S Wai Ho and H. Vicent Poor "Privacy Security Trade-Offs in Biometric Security Systems - Part 2: Multi Use Case" IEEE Transactions on Information Forensic and Security, Vol 6, No.1, March 2011

[27] S B Nikam, S Agarwal, Ridgelet-based fake fingerprint detection, Neurocomputing, Volume 72, Issues 10–12, June 2009, Pages 2491–2506

[28] LF WU, et al, Non-Invertible Transformation Schems for Face Templete Protection, Signal Processing, Vol 28, No 7, 2012.

[29] M-d Yu and Srinvas Devadas, Pervasive, Dynamic Authentication of Physical Items, COMMUNICATIONS OF THE ACM, V60, N4, 2017, pp32-39

[30] K Gai, et al, Privacy-Preserving Adaptive Multi-channel Communications Under Timing Constraints, 2016 IEEE International Conference on Smart Cloud (SmartCloud), 2016, pp 190-195

[31] Schneier, B. Sensible authentication. ACM Queue 1, 10(2004): 74–78

[32] Wilson, C.et al, Fingerprint vendor technology evaluation 2003: summary of results and analysis report. NIST Internal Report 7123 (2004).

[33] Yixuan Zhu and Zhixiong Chen, RealID: Building A Secure Anonmous Yet Transparent Immutable ID Service, 2017 IEEE 3rd International Conference on Big Data Security on Cloud, Beijing, China

[34] Smart Contracts: The Blockchain Technology That Will Replace Lawyers, https://blockgeeks.com/guides/smart-contracts/

[35] Michael Mainelli, Blockchain Will Help Us Prove Our Identities in a Digital World, Harvard Business Review, March, 2016, https://hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world

[36] Xin Luna Dong, et al, Knowledge-Based Trust: Estimating the Trustworthiness of Web Sources, https://arxiv.org/abs/1502.03519 Submitted on 12 Feb 2015)