International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 6, October 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Investigation of Blockchain Based Identity System for Privacy Preserving University Identity Management System

Kyaw Soe Moe, Mya Mya Thwe

University of Computer Studies, Hpa-An, Myanmar

ABSTRACT

Existing blockchain based identity systems are analyzed under the context of the university identity management requirements. The private or consortium blockchain is more suitable for identity system which will be used for university. The transparency of public blockchains raises some concerns for privacy and confidentiality. The most important issue is that the volume of the data generated can be very large exceeding the practical storage capabilities of the current blockchain usages. The existing identity systems are not well fixed with the university identity management system really needs, especially; they remain needing the relevant issue of effective consent revocation. The append-only storage of blockchain can be a barrier for implementing the revocability of consent. Some private blockchain based system has the potential vendor lock-in effects. Thus, hybrid identity system is suggested for university identity management.

KEYWORDS: *blockchain; identity; identity management system; privacy*

How to cite this paper: Kyaw Soe Moe | Mya Mya Thwe "Investigation of Blockchain Based Identity System for Privacy Preserving University Identity Management System" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-6, October 2019, pp.336-341, URL: https://www.ijtsrd.com/papers/ijtsrd28095.pdf

IJTSRD28095

I. INTRODUCTION

One of the essential mechanisms to preserve the privacy and security of university database is an identity system. Any failure or error throughout the identification process might lead to an irreversible consequence. The identity forms the basis for most types of access control mechanisms and it also help in establishing the system accountability. Thus, the identity contributes to the protection of privacy by reducing the risks of an unauthorized access to the university information, a data breach issue, and an identity theft issue [1]. Therefore, the identity system is a critical building block for privacy and security of university database.

To share the university data via any online environment, without the benefit of a face-to-face personal contact, the process of authenticating the identity of a user is very important. The lack of a demonstrable link between a physical person and a digital identity can create an additional uncertainty that does not exist under an offline mode [2]. Without an adequate identity system, identifying an individual can be a complicated process. Moreover, the identifying and authenticating process must be done on a growing number of people and entities with whom the system is electronically dealing with. A digital identity system relates individuals to their respective online identities. There are three types of digital identity solutions including federated, self-sovereign, and hybrid [3], each of which has different schemes and architectural options.

In the world of blockchain, the identity storage is not really a repository. The blockchain is simply a distributed record of transactions [4]. It tracks a flow of information. Thus, blockchain can be used for storing the identity, not as a container of information, but as a service that provides an on-demand access to a specific piece of information that may reside anywhere. The information may be represented as a transaction inside the block or as a record resided in a traditional database. The services could aggregate and verify the data from a wide variety of sources to respond to a specific question on whether or not the user is currently qualified to access the requested data.

Despite there being many possible applications of a digital identity system using blockchain, each application offers different solutions for different conditions, as well as taking along their own advantages and disadvantages. In this work, several applications of digital identity system using blockchain are investigated in order to find the most suitable identify system using blockchain methodology for university identity management system. The remaining of this paper organized as follow. Next the university identity management system requirements are discussed in order to layout the objectives for the following investigation. Then, the blockchain and the digital identity technologies are discussed in order to investigate the twenty existing digital identity systems using blockchain application. Finally, the conclusion is given.

II. UNIVERSITY IDENTITY MANAGEMENT SYSTEM

We consider a university where the administration delivers identity credentials to students, teachers, and staff. These credentials provide certificates of various fields related to the user including their name, their status at the university (student, teacher, etc.), and their academic records. Individuals may use such identities, revealing some (or none) of these fields, to authenticate themselves to various university services such as the university pool or medical clinic.

Now imagine that a user wants to claim a discount on car insurance re-served for students with high GPAs. This student may need to coordinate her university identity with a driver's license issued by her local government. Then she can selectively reveal information to the service provider, the insurer. If her status at the university changes, her university identity can be revoked preventing her from performing such authentications, even as her driver's license identity remains valid.

A. The Privacy of Identity System and Blockchain

The term "privacy" is used frequently, but there is no universally accepted definition of the term. Privacy comprises several principles such as anonymity, pseudonymity, unobservability, unlinkability, and revocability of consent [5].

- **Anonymity –** can be defined as the state of being not identifiable within a set of subjects or entities.
- **Pseudonymity –** is the use of pseudonyms as identifiers. An advantage of pseudonymity technologies is the accountability or the enforcement of any misbehavior.
- **Unlinkability –** ensures that a user may consume multiple resources or services without letting other entities to link these multiple resource or service accesses together.
- **Unobservability –** permits a user to access resources or services and avoiding other entities, especially third parties, to observe that the resource or service is being used.
- **Revocability of consent –** allows users to withdraw their consent of any specific action over the data to certain individuals. This rule is critical for the enforcing of privacy.

Blockchain utilizes a public key crypto system and its properties already support most of the above principles [6]. Thus, blockchain technology can be a suitable technology for attaining the privacy preserving model, despite there being some counter arguments on the use of blockchain in this context. By using typical blockchain applications, such as Hyperledger, many criteria can be implemented as a self-execution model similar to the chain-code or the smart contract. However, the append-only storage of blockchain can be a barrier for implementing the revocability of consent. Revoking consent allows the users to grant or withdraw their consent of any specific action over data to certain individuals.

III. The Blockchain Technology

Blockchain technology has become popular with Bitcoin, a crypto currency. Generally, a blockchain is a distributed, transactional database. The blockchain resides on the network, and not within a single institution which charged with maintaining and keeping the record [7]. Blockchain is composed of nodes which are linked by a peer-to-peer (P2P) communication network with its own layer of protocol messages for node communication and peer discovery [4]. A node is a physical/virtual machine that communicates via TCP/IP and UDP with other nodes. The nodes in blockchain system identify each other by their IP address and users reference each other via their public keys. The private key of a user is used for cryptographically signing a message and transaction (Tx). A user is only represented by a public key (address) and could theoretically login from any other node.

A. The Challenges of Blockchain

Contrary to the expectation, blockchain also has some drawbacks. Several challenges that commonly arise in relation to blockchains are as follow.

- **Performance –** When a transaction is being processed, a blockchain has to perform the same tasks that a regular database does, but it carries three additional burdens [13] including a signature verification, a consensus mechanism and a redundancy. Thus, the processing time of blockchain can be slower than that of a conventional centralized database.
- **Scalability –** Scalability is a major issue for a public blockchain [8]. The larger the blockchain grows, the requirements on storage, bandwidth and computational power are also larger.
- **Privacy –** Blockchain can preserve a certain amount of privacy through the public key (an address for each entity) [9]. However, the values of all transactions and the balances for each public key are publicly visible [10]. Thus, the public nature of the blockchain means the private data would flow through every full node fully exposed.
- **Energy Consumption –** A block creating process of a public blockchain consumes a large amount of computational power and a large amount of electricity. The computational power is used for this process only.

All of the above challenges affect the development of the university identity management application. The most important issue is that the volume of the data generated can be very large exceeding the practical storage capabilities of the current blockchain usages.

B. Types of Blockchain

There are three types of blockchain including private blockchain, consortium blockchain and public blockchain. Private or consortium blockchain is linked to a limited environment such as company, group of companies or one specific value chain, while public blockchain supports a permission-less type of blockchain.

- **Private blockchain –** For a fully private blockchain, the write permissions are kept centralized to one organization while read permissions may be public or restricted to an arbitrary extent. An example for this type of blockchain is Hyperledger.
- **Consortium blockchain –** Consortium blockchain is partly private. The consensus process is controlled by a preselected set of nodes. The right to read the blockchain may be public or restricted to a set of participants [11]. Examples of this type are Ethereum and R3.
- **Public blockchain –** this type of blockchain maintains the principle that anyone in the world can access the data. This includes the consensus process to write the data into the public blockchain or to block it. An example of a public blockchain is bitcoin.

The public blockchain and the private or consortium blockchain are compared based on six categories and summarized in Table1.

TABEL 1: COMPARISON OF PUBLIC VS PRIVATE/CONSORTIUM BLOCKCHAIN

Characteristics	Public	Private/Consortium
Access	➢ Open read/write access	➢ Permissioned read and/or write access
Control	➢ Fully distributed	➢ Partially distributed
Security	➢ Proof of work ➢ Proof of Stake ➢ Other consensus mechanism	➢ Pre-approved participants
Identity	➢ Anonymous ➢ Pseudonymous	➢ Known Identities
Speed	➢ Slow	➢ Fast
Asset	➢ Native Asset	➢ Any Asset

Thus, it can be grouped into public and private. Both types offer different advantages and disadvantages. According to the comparison which is shown in Table 1, the private or consortium blockchain is more suitable for identity system which will be used for university database.

IV. Digital Identity System

The identity can be seen from different perspectives and the identity is applicable in different domains, depending on the objective. Generally, the identity refers to a set of qualities and characteristics that make an entity definable, distinguishable, and recognizable compared to other entities [12]. In digital world, an identity is electronic information associated with an individual. The identity systems are used as a part of an authentication process and an authorization process [13]. The identity information is saved and managed in a standard format by entities. There are three categories of digital identity system which are widely available [3] including federated, self-sovereign, and hybrid.

A. Federated Identity System

Federated identity systems provide authentication and authorization capabilities across organizational and system boundaries. It requires agreements that an identity at one provider is recognized by other providers and contractual agreements on data ownership [14]. Conceptually, it involves a group of organizations setting up a trust relationship that allows them to share assertions about the user identities, in order to grant the users, access to their resources [15]. Federated identity management allows users to access multiple services based on a single authentication [16]. This makes the users very dependent on the availability of an identity provider (issuer). When the identity provider goes down or discontinues their service (and the only offered authentication method is using), the user cannot log in anymore.

The federated identity system allows for the joining of partners among providers to deliver service automation to both customers and other providers. In this model the client is responsible for managing its users and passwords (the client does not face any additional costs, because they already have to manage these). However, the federated identity still faces common challenges, especially in terms of security and privacy [20]. In relation to security, it is vulnerable to various attacks on web applications, such as replay attacks, man-in-the-middle attacks, session hijacking, etc. Regarding privacy, the service provider may get hold of more user information than is required because it lets users dynamically distribute identity information across security domains, increasing the portability of their digital identities.

B. Self-sovereign Identity System

Self-sovereign identity system allows the users to choose which of their identities to be used for each application, allowing the users to store their identifiers and credentials for different service providers in a single tamper-resistant hardware device, which could be a smart card or some other portable personal device [17]. A further practical advancement of this system is attribute-based identity. This approach aims to solve security-related and privacy-related problems by using an attribute-based credential technique. It enables attributes to be issued and stored with the data subject [18].

The clear benefit is allowing the user to select the attributes they share with the requesting party. It ameliorates privacy concerns because users have full control over their data and knows who using it and when [21]. Even though users know and can control their data, in a decentralized model, only the relying parties such as services or applications know the identity provider; otherwise they would have no basis for making the decision to trust an assertion.

C. Hybrid Identity System

Hybrid identity system provides an alternative when both federated and user-centric approaches do not readily cope with certain circumstances. On the other hand, the federated models raise some privacy concerns since the data may be available to every entity within the circle of trust. Hence, the hybrid model allows the users to configure and track access to their data, while the identity providers store and manage user credentials [19].

Hybrid identity system is suitable for dealing with unstable environments which require system flexibility since it manages everything, including users and devices. Thus, the system can be extended if there is an increasing amount of work. It also provides better scalability as one of its benefits because it offers connectivity to cloud-based applications. Most of the implementations still experience the vendor lock-in effect, in which a person or company is obliged to deal only with a specific company [22].

D. Suitable Identity Approach

According to the discussion above, the hybrid approach is the most suitable choice for university identity management due to the following reasons:

- Hybrid identity is a mixture of federated identity and user-centric identity. So, using hybrid identity can enlarge the implementation cluster and many service providers could join to create a system with no centralized power.
- Hybrid identity offers scalability because its flexibility and its extensible feature to an open environment like cloud-based services.
- The hybrid system allows the use of blockchain and IoT which would allow an integration from multiple applications.
- By using blockchain as the database technology for hybrid identity, the users would be able to take control of their own attributes, specifically called self-sovereign identity (SSI).

TABEL 2: CURRENT BLOCKCHAIN BASED IDENTITY SYSTEMS

Project	Underlying Blockchain	Type	Purpose	Remark
uPort [23]	Ethereum	Private/ consortium	To support self-sovereign identity	Still in the closed-beta stage
Cambridge Blockchain [24]	Cambridge Blockchain	Private/ consortium	To support financial institutions	At alpha stage since 2015
Netki [25]	Hyperledger	Private/ consortium	To support financial service companies	Charge based on number of certificates and complexity of validation
KYC-Chain [26]	Ethereum	Private/ consortium	To support Banking companies	Under development
HYPR [27]	HYPR biometric security platform	Private/ consortium	To support device ID (Mobile and IOT systems)	Use biometric authentication
Guardtime's BLT [28]	KSI Blockchain	Private/ consortium	To replace RSA with their authentication and signature protocol	Based on Guardtime's quantum-secure Keyless Signature Infrastructure (Hashing function)
Evernym [29]	Hyperledger	Private/ consortium	To support merchandising and field marketing services	Absolutely relied on Self-sovereign identity
e-Residency [30]	KSI Blockchain	Private/ consortium	To support blockchain notary service	Creating P2P version of e-governance
Regis[31]	Ethereum	Private/ consortium	To support online registry system	Build a DNS like registry and attach an auction behavior
I/O Digital [32]	I/O Coin	Private/ consortium	To support identity management and messaging	Intended for crypto-currency
Bloom [33]	Ethereum	Private/ consortium	To support credit scoring	Still in development
Jolocom [34]	Ethereum	Private/ consortium	To support self- sovereign identity	Still in development
ShoCard [35]	Bitcoin	Public	To support financial services companies	Still in development
UniquID [36]	Bitcoin	Public	To support authentication of devices	utilize biometric information
Bitnation [37]	Bitcoin	Public	To establish the concept of world-citizenship	Collaborating with the Estonian e-Residency program
Civic [38]	Bitcoin	Public	General purpose	identity verification and protection tools
OIX [39]	collaborative cross-sector membership organization	Public	To support federated identity	In pilot in 2016 registering new and diverse trust frameworks and communities of interest.
Cryptid [40]	Factom blockchain	Public	To change data into a compact format	User encryption and QR codes
CredyCo [41]	Bitcoin	Public	To support document verification	Software as a service (Saas)
DIF [42]	Blockstack [Bitcoin]	Public	General purpose	No address registration, identifier modification, authentication, and authorization

V. Current Blockchain based Digital Identity Systems

Several companies have been pioneering the development of blockchain-based digital identity management and authentication. Table 2 shows several implementation solutions grouped by the types of blockchain used as the underlying technology for developing digital identity systems.

Most of the existing blockchain based identity systems are intended to support for financial purposes. Generally, federated identity systems are mostly developed on public blockchains while self-sovereign systems are developed on private blockchains. Most of them are under development. The existing identity systems are not well fixed with the university identity management system really needs, especially; they remain needing the relevant issue of effective consent revocation. Some private blockchain based system has the potential vendor lock-in effects. On the other hand, the transparency of public blockchains raises some concerns for privacy and confidentiality.

VI. Conclusion

Blockchain technique has its own properties such as pseudonymity and protection against fraud and it is attracting to use blockchain in identity system for university identity management. Contrary to the expectation, blockchain also has some drawbacks such as performance, scalability and energy consumption. The drawbacks of the blockchain are still open research area and it must be considered for using in identity management field. According to the identity nature, the private or consortium blockchain is recommended to be used for underlying system, but we have to consider the vendor lock-in effect. According to the comparison which is shown in section 4 (D), the hybrid approach is the most suitable choice for university identity management system. The current blockchain based identity systems are compared in Table 2 and each blockchain based identity systems is built on private blockchain or public blockchain. However, the existing blockchain based identity systems might not be suitable for university identity management requirements due to several factors such as a high probability of vendor lock-in issue, a slow execution and a high computational power requirement.

References

[1] "Introduction to Online Identity Management - Google Search," 02-Mar-2018.

[2] Oecd, "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers," OECD Publishing, OECD Digital Economy Paper 186, Nov. 2011.

[3] R. Halim and S. A. Shaharyar, "Digital Identity Management," Linköpings University, Sweden, 2011.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[5] A. Pfitzmann and M. Köhntopp, "Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology," in Designing Privacy Enhancing Technologies, Springer, Berlin, Heidelberg, 2001, pp. 1–9.

[6] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[7] D. Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin, 2016.

[8] K. Croman et al., "On Scaling Decentralized Blockchains," in Financial Cryptography and Data Security, 2016, pp. 106–125.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain Challenges and Opportunities: A Survey," presented at the International Journal of Web and Grid Services, 2017.

[10] A. Kosba, A. Miller, E. Shi, Z. Wen, and 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.

[11] BlockchainHub, "Blockchains & Distributed Ledger Technologies," Types of Blockchains. [Online]. Available: https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/.

[12] G. B. Ayed, Architecting User-Centric Privacy-as-a-Set-of-Services: Digital Identity-Related Privacy Framework. Springer, 2014.

[13] A. Bhargav-Spantzel, A. C. Squicciarini, and E. Bertino, "Establishing and protecting digital identity in federation systems," J. Comput. Secur., vol. 14, no. 3, pp. 269–300, Jan. 2006.

[14] S. Balasubramaniam, G. A. Lewis, E. Morris, S. Simanta, and D. B. Smith, "Identity management and its impact on federation in a system-of-systems context," in 2009 3rd Annual IEEE Systems Conference, 2009, pp. 179–182.

[15] D. W. Chadwick, "Federated Identity Management," in Foundations of Security Analysis and Design V, Springer, Berlin, Heidelberg, 2009, pp. 96–120.

[16] J. Kallela, "Federated Identity Management Solutions," in Seminar on Internetworking, 2008.

[17] A. Jøsang and S. Pope, "User Centric Identity Management," in Asia Pacific Information Technology Security Conference, 2005, p. 77.

[18] G. Alpár and B. Jacobs, "Credential Design in Attribute-Based Identity Management," in Bridging distances in technology and regulation, 2013, pp. 189–204.

[19] R. Sánchez-Guerrero, F. Almenárez, D. Díaz-Sánchez, A. Marín, P. Arias, and F. Sanvido, "An Event Driven Hybrid Identity Management Approach to Privacy Enhanced e-Health," Sensors, vol. 12, no. 5, pp. 6129–6154, May 2012.

[20] U. Fragoso-Rodriguez and M. Laurent, Federated identity architectures. 2006.

[21] S. Raj, Digital Identity and Access Management: Technologies and Frameworks: Technologies and Frameworks. IGI Global, 2011.

[22] "lock-in | Definition of lock-in in US English by Oxford Dictionaries," Oxford Dictionaries | English. [Online]. Available: https://en.oxforddictionaries.com/definition/us/lock-in.

[23] "uPort," uPort. [Online]. Available: https://www.uport.me/. [Accessed: 03-Mar-2018].

[24] "Cambridge Blockchain | Identity Compliance Solutions |," Identity Compliance Solutions | Cambridge Blockchain. [Online]. Available: https://www.cambridge-blockchain.com. [Accessed: 03-Mar-2018].

[25] "Netki Verify Your World." [Online]. Available: https://www.netki.com/. [Accessed: 03-Mar-2018].

[26] "KYC-Chain – Enhanced KYC on Blockchain Technology." [Online]. Available: https://kyc-chain.com/. [Accessed: 03-Mar-2018].

[27] "HYPR | Trust Everyone," HYPR Corp, 10-Jan-2018. [Online]. Available: https://www.hypr.com/. [Accessed: 03-Mar-2018].

[28] "BLT | New Blockchain Standard for Digital Identity." [Online]. Available: https://guardtime.com/blog/blt-new-blockchain-standard-for-digital-identity. [Accessed: 03-Mar-2018].

[29] "evernym | The identity revolution starts now," Evernym. [Online]. Available: https://www.evernym.com/. [Accessed: 03-Mar-2018].

[30] A. Alender, "What is Estonian e-Residency and how to take advantage of it? | LeapIN." [Online]. Available: https://www.leapin.eu/articles/e-residency. [Accessed: 03-Mar-2018].

[31] "Regis." [Online]. Available: https://regis.nu/. [Accessed: 03-Mar-2018].

[32] "I/O Digital – Enterprise Blockchain technology." [Online]. Available: https://iodigital.io/. [Accessed: 03-Mar-2018].

[33] J. Leimgruber, A. Meier, and J. Backus, "Bloom Protocol: Decentralized credit scoring," 2018.

[34] "Jolocom - Own your digital self : An easy to use decentralised digital identity for everyone." [Online]. Available: https://jolocom.com/. [Accessed: 03-Mar-2018].

[35] "Secure Enterprise Identity Authentication | ShoCard," ShoCard | Identity for a Mobile World. [Online]. Available: https://shocard.com/. [Accessed: 03-Mar-2018].

[36] "UniquID Inc. | Blockchain Identity Access Management." [Online]. Available: http://uniquid.com/. [Accessed: 03-Mar-2018].

[37] "BITNATION PANGEA - Your Blockchain Jurisdiction." [Online]. Available: https://tse.bitnation.co/. [Accessed: 03-Mar-2018].

[38] "Civic Identity Verification | Secure & Protect Identities," Civic. [Online]. Available: https://www.civic.com/. [Accessed: 03-Mar-2018].

[39] "Open Identity Exchange (OIX)," OIX. [Online]. Available: http://oixuk.org/. [Accessed: 03-Mar-2018].

[40] "Cryptid." [Online]. Available: http://cryptid.xyz/. [Accessed: 03-Mar-2018].

[41] "Credyco." [Online]. Available: https://mattermark.com/companies/credy.co.

[42] "DIF - Decentralized Identity Foundation." [Online]. Available: http://identity.foundation/. [Accessed: 03-Mar-2018].