Blockchain-enhanced Identities for Secure Interaction

Dipto Chakravarty
Chief Technology Officer
Exostar, LLC
E-mail: dchakravarty@gmp4.hbs.edu

Tushar Deshpande
Department of Computer Science
Stony Brook University
E-mail: tushar.deshpande@gmail.com

***Abstract*—Securing identities in online communities like Facebook and Google requires thinking beyond mobility and cloud as federation methods can be gamed. While use of adaptive authentication and biometrics on mobile devices has become the norm, its security can be bolstered lot more with a distributed ledger like blockchain. This paper presents an augmented security model based on the blockchain distributed ledger, depicting how blockchain can help us build decentralized identity ecosystem.**

I. Introduction

Securing identities in online communities like Facebook and Google requires thinking beyond mobility and cloud as federation methods can be gamed. While use of adaptive authentication and biometrics on mobile devices has become the norm, its security can be bolstered lot more with a distributed ledger like blockchain. Within a community of users who do not necessarily trust each other, one can still reach consensus over certain facts without having to employ a central authority. This introduces the case of blockchain to enhance the security model. The networked nature of the blockchain not only enables decentralized administration; it also makes the blockchain robust against attacks and natural disasters. This is one of the reasons why blockchain-based identity management has been proposed as a solution for refugees [1]. In war, floods or fires, passports and other important documents can easily be destroyed, but a blockchain network lives on, just like the internet. This paper presents an augmented security model based on blockchain distributed ledger, illustrating how blockchain can form the foundation of the *decentralized identity ecosystem.*

II. What is digital identity?

A *digital identity* can be defined as a set of claims made by one digital subject about itself or another digital subject [2]. *Digital subject* is the digital representation of the person or the thing that is being described, whereas a *claim* is an assertion of a property about a subject. A claim needs to be attested. E.g., the claim that a driver's license id is S123456 needs to be attested by the Registry of Motor Vehicles to be valid.

III. Evolution of Identities

The models for identity have evolved from centralized identity to decentralized identity via the following stages [3]:

1) **Centralized identity**: They are controlled and administered by a single authority. E.g., an organization assigns and controls employee IDs of all its employees.
2) **Federated identity**: They make it possible for a single identity to be used at multiple sites, thereby enabling *Single Sign-On* (SSO). The multiple sites that support federated identities need to use a standard, such as SAML (Security Assertion Markup Language) to share the authentication data.
3) **User-Centric identity**: They allow a user to share an identity across multiple services without using federation. Examples of such identities include OAuth and OpenID.
4) **Self-sovereign identity**: It is an identity that is fully controlled by a subject. A self-sovereign identity can be shared across multiple sites with user's consent. It consists of claims that a subject makes about itself as well as the claims made about the subject by others. Since no single central authority owns self-sovereign identities, they can be supported using *decentralized identity* system.

IV. Blockchain Basics

Blockchain is a *tamper-evident distributed ledger* [4]. As shown in Fig. 1, the use of hash pointers in blockchain to chain together the data blocks ensures that it is impossible for an attacker to modify an intermediate block without modifying all subsequent blocks as well as the hash pointer at the head of the list. The hash pointer at the head of the list is, however, protected. So, any attempts by the attacker to modify the blockchain can be easily detected.

The blockchain concept can also be understood from the real-life example of Mumbai's *Dabbawallas* [5]. These *dabbawallas*, or the lunch box carriers, deliver lunch boxes from people's homes to their workplaces. The first carrier receives a lunch box from a home and writes the encoded locations of the source and the destination addresses on the box. This public information is validated by the carrier by including his own signature on the box, thereby asserting that the source and destination addresses are correct. Then, the carrier takes the box to a nearby railroad station, where all boxes are being collected. Now, another carrier picks up the box, verifies that the box contains a valid signature from the previous carrier, writes the name of the next collection point that is closer to the destination, puts his own signature on the box,

978-1-5386-3443-1/18/$31.00 ©2018 IEEE

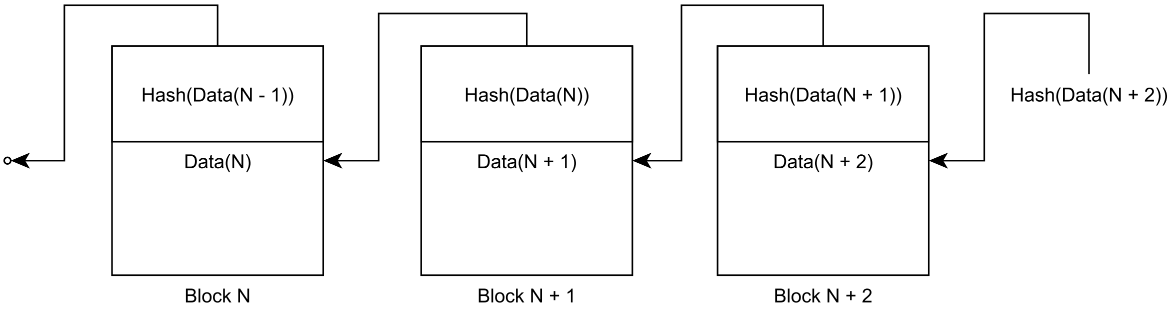

Fig. 1. Schematic diagram of a blockchain

and takes the box to the next collection point. In this way, eventually the lunch box is delivered to the destination. The process of a carrier verifying the information on the box by placing his own signature on the box is very similar to the verification performed during bitcoin mining, where a miner verifies transactions in the previous block by signing them. Once the data in the new block is verified, the new block is added at the end of the bitcoin blockchain.

V. Decentralized Identity using blockchain

In this section, we describe components of decentralized identities and how they can be implemented using blockchain.

```
{
  ”@context”:”https://w3id.org/did/v1”,
  ”id”:”did:ex:johndoe”,
  ”publicKey”:[{
    ”id”:”did:ex:johndoe#key1”,
    ”type”:”RsaSigningKey2018”,
    ”owner”:”did:ex:johndoe”,
    ”publicKeyPem”:”PUBLICKEY”
  }],
  ”authentication”:[{
    ”type”:”RsaSignatureAuth2018”,
    ”publicKey”:”did:ex:johndoe#key1”}],
  ”signature”:{
    ”type”:”RsaSignature2016”,
    ”creator”:”did:uport:hQMGzWxR8#key/1”,
    ”signatureValue”:”dw0yqie”
  }
}
```

Listing 1. Example of a decentralized identifier (DID) document

A. Decentralized Identity

As described in section III, decentralized identities are owned by individual entities. Decentralized identities are established using *Decentralized Identifiers* (DIDs) [6], [7]. These identifiers do not rely on a central authority. DIDs are characterized by the following important properties [8]:

- DIDs are not governed by any central authority
- DIDs are persistent
- DIDs support authentication via cryptographic proofs, such as digital signatures

DID documents are used to describe an entity that is being represented using DIDs. A DID document contains the DID, a set of public keys to verify the DID, a set of authentication methods to authenticate the entity's identity, and a signature to support integrity. Listing 1 presents a DID document that can be used to identify a person named John Doe [8].

B. Identity Trust Fabric (ITF)

Decentralized identity rely on *identity trust fabric* (ITF) [9]. ITF cryptographically stores *proof of identifiers* and profile attributes. Information stored in ITF is also immutable. So, ITF can be trusted by various entities involved in a distributed identity system. Since ITF reduces the role of a central authority in identity management (IdM), ITF acts as key enabler for the distributed identities. A platform that aims to serve as ITF needs to have the following properties:

- **Trust:** No single entity has enough authority to change the system rules
- **Assurance:** The platform should provide adequate level of identity assurance
- **Security:** The platform should provide integrity, confidentiality, and availability
- **Provenance:** The platform should provide a trusted time stamping service to record all data ever stored
- **Scalability:** The platform should support large volume of read/write operations

C. Blockchain as ITF

As described in section IV, blockchain is a tamper-evident distributed ledger. In a *permissionless* blockchain, no single participating node has special privileges. All nodes participate in a *distributed consensus protocol* to provide *trust*. A distributed consensus protocol, such as the one used for bitcoin mining [10], ensures that a block is added to the blockchain only after the block data has been cryptographically verified. The distributed consensus protocol, therefore, provides *assurance*. Blockchain's tamper-evidence guarantees the data *integrity*. Blockchain also provides data *confidentiality* by ensuring that only *one-way hash* of data is stored in a

978-1-5386-3443-1/18/$31.00 ©2018 IEEE

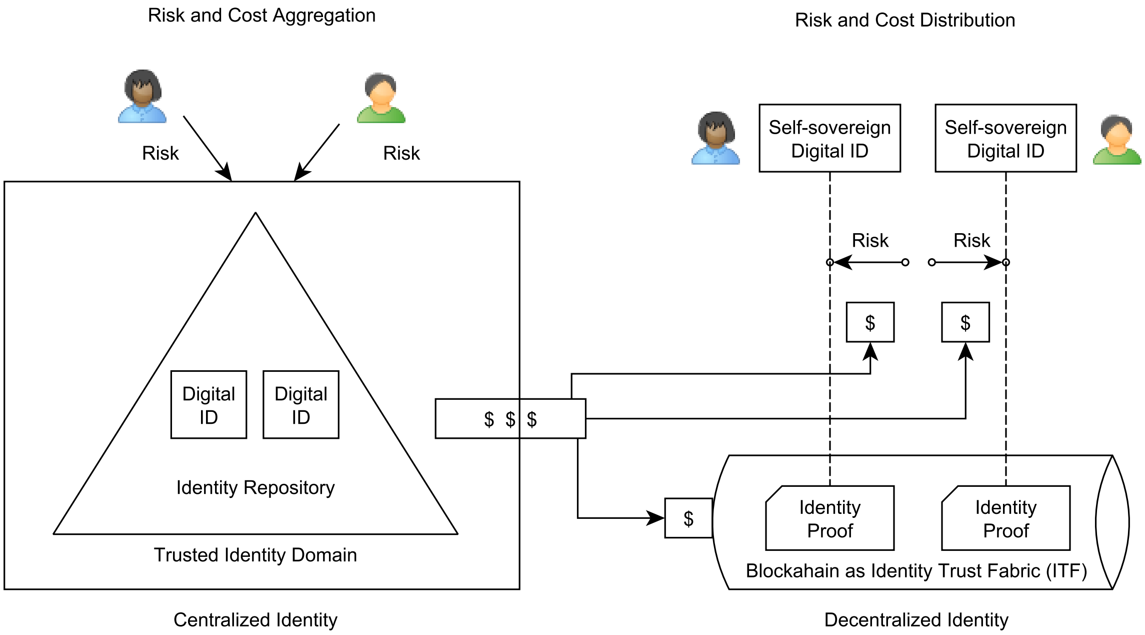

Fig. 2. Centralized identity v/s distributed identity on blockchain. Blockchain ITF lowers the implementation cost by storing fixed sized identity proofs instead of variable sized identity data. Also, since blockchain ITF does not store actual identity data, it improves the overall security by reducing risk.

block. Since blockchain is an *append-only* distributed ledger, it provides a trusted chronological history of all blocks that have been ever added to the blockchain. The blockchain, thus, provides *provenance*. The distributed nature of blockchain allows any node to easily join the blockchain, thereby making the system highly *scalable*. Since the blockchain provides trust, assurance, security, provenance, and scalability, it is very well suited to perform the role of an ITF [9].

D. Advantages of implementing distributed identity on blockchain ITF

As we can see from fig. 2, in a centralized identity, each user interacts directly with the central identity provider. The centralized identity provider is, therefore, required to implement an identity repository that fully controls and manages all digital identities. This results in a high implementation cost for the identity provider. The cost increases with the number of digital identities that need to managed. The cost also depends on the size of the digital identity data. Let us denote the number of identities being managed as N_{id} and the size of a single instance of identity data as W_{id}. The total implementation cost for the central identity provider, $Cost_{centralized}$, can now be represented using equation (1), where K_c is the proportionality constant.

$$Cost_{centralized} = K_c \cdot N_{id} \cdot W_{id} \tag{1}$$

Also, since all users directly interact with the identity provider, the identity provider becomes an attractive target for various security attacks. So, the risk associated with the identity provider is high as well. The risk is proportional to the number of identities being managed. So, the risk associated with a centralized identity solution, $Risk_{centralized}$, can be expressed using equation (2), where K_r is the proportionality constant.

$$Risk_{centralized} = K_r \cdot N_{id} \tag{2}$$

In a decentralized identity solution, users manage their own identities [11]. So, the identity data is stored off-chain, while the cryptographic identity proofs alone are stored within blockchain ITF [12]. The cost to implement blockchain ITF depends on the number of identity proofs to be stored. Since there is one identify proof per identity, the cost depends on the number of identities, N_{id}. The cost also depends on the size of identity proofs. However, unlike identity data, the identity proofs have a fixed size. So, the identity proof size can be represented as the constant value, K_{id}. The total implementation cost for the decentralized identity provider, $Cost_{decentralized}$, therefore, can be represented using equation (3), where K'_c is the proportionality constant.

$$Cost_{decentralized} = K'_c \cdot N_{id} \cdot K_{id} \tag{3}$$

Since in a decentralized identity solution, users manage their own identities, the risk associated with storage of identity data is distributed across all users. The blockchain provides a trusted and secure ITF for the decentralized identity. So, as shown by equation (4), a constant risk, K'_r is associated with a decentralized identity solution.

$$Risk_{decentralized} = K'_r \tag{4}$$

978-1-5386-3443-1/18/$31.00 ©2018 IEEE

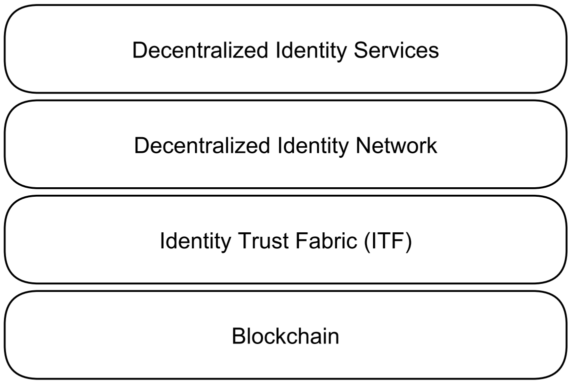
Decentralized Identity Services
Decentralized Identity Network
Identity Trust Fabric (ITF)
Blockchain

Fig. 3. Decentralized Identity Ecosystem

The constant identity proof size K_{id} is likely to be much smaller than the arbitrarily sized identity data W_{id}. So, from equations (1) and (3), we see that the implementation cost for a decentralized identity solution would be smaller than the implementation cost for a centralized identity solution. Similarly, from equations (2) and (4), we see that the risk associated with a decentralized identity solution is constant as compared to the risk associated with a centralized identity solution. The decentralized identity, therefore, significantly reduces the risk.

Blockchain as ITF allows us to implement a decentralized identity solution that minimizes the risk while also reducing the implementation cost. So, as shown in Fig. 3, the blockchain forms the foundation of the *decentralized identity ecosystem*.

VI. Future work

As a future work, we intend to continue exploring various use cases of blockchain as identity solution. More specifically, we would like to explore how blockchain can augment government issued identification, beyond the approaches used by existing solutions, such as ShoCard [13]. We would also like to study how blockchain can enhance security by providing passwordless authentication. Combining Fast Identity Online (FIDO) and blockchain seems to be a promising approach to provide universal passwordless authentication via blockchain [14].

VII. Conclusions

In this paper, we defined digital identities and showed how digital identities are transitioning from centralized identities towards decentralized identities. We discussed how decentralized identifiers (DIDs) are used to establish digital identities. We examined how blockchain provides a trusted distributed ledger. We showed how the trust, assurance, security, provenance, and scalability offered by blockchain enable it to be used as the identity trust fabric (ITF) for implementing decentralized identity. Finally, we discussed the cost and the risk associated with centralized and decentralized identity solutions and showed how the blockchain as ITF lets us implement decentralized identity solution that minimizes the risk, thereby enhancing the security, while also reducing the solution cost.

References

[1] "Blockchain against hunger: Harnessing technology in support of syrian refugees," May 2017. [Online]. Available: https://www.wfp.org/news/news-release/blockchain-against-hunger-harnessing-technology-support-syrian-refugees

[2] K. Cameron, "The laws of identity," May 2005. [Online]. Available: https://msdn.microsoft.com/en-us/library/ms996456.aspx

[3] C. Allen, "The path to self-sovereign identity," April 2016. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovererign-identity.html

[4] A. Narayanan, E. Felten, A. Miller, and G. S., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, 1st ed. Princeton University Press, 2016.

[5] G. Sachdeva, "What is blockchain and why banks are so interested in this technology?" October 2016. [Online]. Available: https://www.linkedin.com/pulse/what-blockchain-why-banks-so-interested-technology-gaurav-sachdeva/

[6] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, and M. Sabadello, "Decentralized identifiers (DIDs): Data model and syntaxes for decentralized identifiers (DIDs)," August 2018. [Online]. Available: https://w3c-ccg.github.io/did-spec/

[7] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security Privacy*, vol. 16, no. 4, pp. 20–29, July 2018.

[8] D. Reed, "Decentralized identifiers (DIDs): The fundamental building block of self-sovereign identity (SSI)," May 2018. [Online]. Available: https://www.slideshare.net/SSIMeetup/decentralized-identifiers-dids-the-fundamental-building-block-of-selfsovereign-identity-ssi

[9] H. Farahmand, "Blockchain: The dawn of decentralized identity," September 2016. [Online]. Available: https://www.gartner.com/doc/3464117/blockchain-dawn-decentralized-identity

[10] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008 (http://bitcoin.org/bitcoin.pdf).

[11] C. Jagers, "Digital identity and the blockchain," June 2017. [Online]. Available: https://medium.com/learning-machine-blog/digital-identity-and-the-blockchain-10de0e7d7734

[12] P. Vigna and M. Casey, *The Truth Machine: The Blockchain and the Future of Everything*, 1st ed. St. Martin's Press, 2018.

[13] "Travel identity of the future," May 2016. [Online]. Available: https://shocard.com/wp-content/uploads/2016/11/travel-identity-of-the-future.pdf

[14] "FIDO authentication and blockchain," May 2017. [Online]. Available: https://www.slideshare.net/FIDOAlliance/fido-authentication-blockchain

978-1-5386-3443-1/18/$31.00 ©2018 IEEE