H. Roßnagel, C.H. Schunck, S. Mödersheim, D. Hühnlein (Hrsg.): Open Identity Summit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 171

IdToken: the new decentralized approach to digital identity

Edoardo Talamo[1] Alma Pennacchi[1]

Abstract: The ability to store and share digital data offers benefits that the digitization of information has become a growing trend but has raised questions about the security of personal data. There have been countless high-profile hacks and personal information leaks. Furthermore users don't (and shouldn't) always trust an external server of a third party to store their personal data. Blockchain tries to offer a compelling solution to the problem of combining accessibility with privacy and security. Records can be held securely, using end-to-end encryption, and yet openly authenticated so that data can still be trusted as reliable. This project goes deeper in this solution thanks to an innovative idea and development of a new kind of blockchain non fungible token specifically created to store and manage digital identities and sensible data. It has the potential to resolve issues blockchain alone was starting to approach and improves security, privacy and accessibility.

Keywords: Blockchain non fungible token; blockchain; digital identity; idtoken; security; privacy; idchain; hyperledger indy

1 Introduction

A blockchain is a growing list of blocks across several computers that are linked in a peer-to-peer network using cryptography. Each block contains a cryptographic hash of the previous one, a timestamp and transaction data. A token in the blockchain ecosystem is any asset that is digitally transferable between two people. They are accessible only by the person who has the private key for that address and can only be signed using this private key. So tokens represent programmable assets or access rights, managed by a smart contract[Cr] and an underlying distributed ledger. Blockchain is a particular type or a subset of distributed ledger technology. DLT is a way of recording and sharing data across multiple data stores (also known as ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers (nodes) that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently. In the digital identity management, blockchain solutions have the potential to make operations more efficient and improve the delivery of services in the public and private sectors[Wo]. Identity management built on blockchain technology would enable an identity model, which reduces issues for certain use cases. Blockchain identity management provides a software ecosystem for

[1] Fondazione universitaria INUIT Tor Vergata, Via dell'Archiginnasio snc – Casale 4 00133 Rome (Italy), edoardo.talamo@gmail.com,alma.pennacchi@gmail.com

private, secure, powerful identity. Nowadays even though thanks to blockchain technology digital identity management could have a significative improvement, there are still open issues: usability, handling of (lost) private keys, achieving a critical mass of users and furthermore the majority of blockchains for digital identities store some data in a third party system (like a wallet that saves informations in the memory of a computer or a server) because still there isn't a technology totally blockchain native[Ku][Mu]. In this article we will introduce a new tool for digital identities management to take full advantage of blockchain to minimize the amount of data saved outside it. We will introduce a new concept of non fungible token[Ho], IdToken, and we show how to use it in defining the process of authentication of a digital identity by a reliable party. The use of the IdToken makes the solution safer, faster and reusable.

2 State of art

Without blockchain technology, Identity federation allows users to maintain login credentials with multiple credential service providers[Da] (CSP) and then choose among them when logging into different online services. Users register once with their selected CSP and establish online credentials to be managed by that CSP for authentication. When a user wants to access a relying party (RP) service, that user is redirected to their preferred CSP for authentication using the credentials the user established with that CSP. The CSP then presents the status of the authentication to the RP so that the user may be granted access to the service or application they wish to use. In this way, users do not need to register or establish login credentials with each service they want to access, and instead they only need to provide their credentials to their selected CSP. Identity federations consist of CSPs and RPs that have agreed to participate in a specific federated identity management arrangement. This identity model comes with certain issues such as there is always trust to a central authority required. Transparency cannot be fully provided, since there is a trusted authority involved. These issues can play an important role in certain use cases, which leads to the conclusion that a new identity model for these use cases has to be developed. In the blockchain ecosystem there aren't organizations that traditionally centralize identity. The immutable blockchain ledger verifies and ensures that the users, transactions, messages are legitimate. Blockchain authentication[Is] is done by smart contracts which are written and deployed to blockchain. The need for a third party to authenticate transactions is eliminated. Costs can be reduced while security and privacy are greatly enhanced. Effort of hijacking the authentication process would be much greater in the distributed environment. The result is a reliable, public source of truth under no single entity's control, robust to system failure, resilient to hacking, and highly immune to subversion by hostile entities. Nowadays probably the best example of identity management blockchain software is: Hyperledger Indy[Hy]. There are numerous solutions to manage data using Hyperledger Indy blockchain such as Sovrin[Li], a decentralized global public utility for self- sovereign identity and MyData[Li] an initiative which joint forces with Sovrin to build self- sovereign identity and authentication mechanism. Indy is a distributed ledger, purpose-built for decentralized

identity. It has complete open source specifications, terminology, and design patterns that allow for the development of decentralized identity solutions. Hyperledger Indy would seem to be a good solution for solving problems on digital identity but some issues still remain unsolved. In the next section we present a more efficient and innovative solution; it is based on the Indy software and manages the exchange of information between two users, in a more faster and secure way, thanks to a new kind of non fungible token based on the model designed in HYperledger Fabric: IdToken. A non-fungible token (NFT) is a special type of cryptographic token which represents something unique; non-fungible tokens are thus not mutually interchangeable by their individual specification. A NFT is generated by a smart contract which is a computer program that directly controls digital assets. This contracts are stored on blockchain technology.

3 IdToken

From now on we will refer to Hyperledger Indy with the new improvement of the IdToken as IdChain. While we will discuss about IdChain we will consider the issues of Hyperledger Indy[2] highlighting the solutions that we obtained with IdChain.

3.1 Description

To better understand the development of IdToken and IdChain let's consider three actors: Alice (normal user), Acme (a corporation), Faber College (the guarantee of identity attributes for Alice: for example in this case the college certifies that a subject has obtained a degree with a certain grade). The registration in IdChain is the same for everyone, so we consider the Alice's example. Alice wants to register in the IdChain, she provides personal data (i.e. name, surname) and biometric data[Ga] (fingerprint or facial recognition). The biometric data is converted in a cryptographic hash and becomes the private key, which is stored in a crypto engine of a personal device, and after the generation of the private key will be generate the public key. When the registration in IdChain is complete, a new block in the ledger is created and the smart contract generator of token will execute and automatically generates, in the new block, her IdToken where Alice can insert all her personal data that are stored and encrypted with her public key. Alice can read and insert new informations in her IdToken using her private key (which is the biometric data hashed - ref. paragraph 3.1 row 7); if she wants to grant access to read-only data in the IdToken to someone she will have to share her public key. A strength of this token is that Alice can insert all the information that she wants inside the IdToken. Furthermore in Hyperledger Indy there were a wallet where a lot of sensible data were stored locally (smartphone, computer) and this could leave to losing fundamental information. Instead if a user loses his personal device, it is easy to access in the IdChain using biometric data[3]. IdChain allows users to exchange

[2] Here[De] there is the description of the procedure

[3] "The biometric data is converted in a cryptographic hash and becomes the private key"paragraph 3.1 row 7

personal data without the control of a central authority. Now let's examine an example using IdChain platform of Alice who wants to obtain a job at Acme using a reliable party (Faber College). If Alice wants to be an employee in Acme, she must exchange her personal data to Acme and she has to perform the following procedure:

1. Both Alice and Acme have an account on IdChain. Alice wants to identify herself to Acme with her attributes certified by Faber College with her IdToken.
2. Subsequently Alice request a connection to Acme giving access to her IdToken providing her public key. After receiving the request Acme accepts because it verified the Verifiable Credentials[Ve] in the IdToken.
3. The identity of Alice and Acme are verified (digital signature).
4. After the verification of identities, Acme sends the request of transcript to Alice asking for the information that the corporation needs to decide whether to hire Alice or not.
5. Alice accepts and sends the IdToken with only the transcript information required by Acme and validated by the reliable party.
6. Acme will be able to read Alice's data, decrypting the IdToken with her public key.
7. In the meantime that all these operations take place, each of these will be associated with a timestamp. In this way both users will be aware of the other's identity and will thus be able to carry out the operations between them in a safe and reliable manner.

The substantial difference between Hyperledger Indy and IdChain is the reusability of IdToken: in fact if Alice wanted to present her CV in other companies, in Hyperledger Indy all these companies should contact Faber College again. In IdChain, thanks to the reusability of the IdToken, there is no need for this step anymore. In the picture below we can find an explanatory workflow of IdChain.

3.2 IdChain properties and technical aspects

- There is no proprietary software or infrastructure, IdChain uses the public permissioned blockchain. This means that Identity Requesters do not have to invest a large amount of money to set up the technology infrastructure to support the IdChain Platform solution.
- Data is revocable, identity data is revocable by the authenticating owner of the data. For example, if a user changes his credit card number, then the former/invalid credit card number data is revoked on the blockchain by the authenticating owner of the data.
- Globally compatible, users store and share their own identity anywhere in the world. Their data is accessible anywhere in the US, Europe, Africa, or Asia.

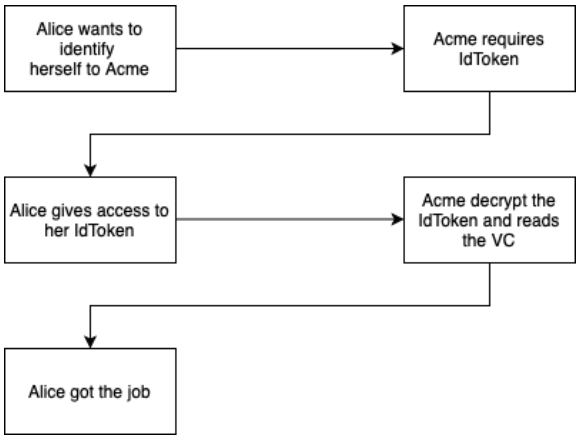

Fig.1:IdToken procedure

- Everything is blockchain native and nothing is stored locally.
- The Verifiable Credentials, and every personal information is stored and encrypted in the IdToken which is unique and not replicable.

Hyperledger Indy Issues	IdToken Solution
The Verifiable Credentials are not stored on the blockchain but they go in the wallet of the VC holder.	The Verifiable Credentials are stored in the IdToken which is blockchain native.
If the user wants to work in a new company, the new company has to request all the infos at the old one and after receiving them the user can finally interact with the new company.	If the user wants to work in a new company, he can directly give access to updated IdToken to the new company
The user has different DIDs for each service so for every interaction with applications that requires username/password a DID is created. Those occupy a lot of memory in the blockchain	The IdToken is unique and the user can access directly with it everywhere.
The lenght of a DID is too short and so there is a security problem because it is susceptible to security breaches	The IdToken is hashed so it's impossible to brute force it
The scalability reduce the security	The scalability is pair with the security

Tab.1:Hyperledger Indy issues and IdToken solution

In the table above we can observe what are the issues of Hyperledger Indy without IdToken and the solution that the token brings to the platform.

4 Conclusions and future developments

This new approach is useful, economical and secure for the digital identity management and certificate distribution thanks to the improvements of privacy, security and efficiency. Furthermore it can easily replace every kind of exchange of paper information and speed up the identification of users and companies, eliminating the open problems presented before in the management of digital identity. An important characteristic of the proposed solution is the impact in the usability of the blockchain. The IdChain open the doors to the use of crypto-engines embedded in portable devices (es. smart cards and others) and then is a first step to separate the peer from a specific device (computer). Biometrical key act as second authentication factor, giving an answer to weaknesses of the Indy authentication system for example the absence of a Certification Authority[Ce]. For future developments, we are working on extensions that allow us to solve problems still related to privacy and the use of biometric data in blockchain which, except for solutions related to fingerprints, is still a subject of study and experimentation. Another important tool that we are going to develop is to partition the amount of data within the IdToken to share only the information necessary in every use case witch is another aspect about usability and blockchain.

Literaturverzeichnis

[Ce] Certification Authority, https://csrc.nist.rip/groups/ST/crypto_apps_infra/documents/B2B-article.pdf, accessed 17/02/20.

[Cr] Creating a safe Smart Contract https://experts.illinois.edu/en/publications/step-by-step-towards-creating-a-safe-smart-contract-lessons-and-i, accessed 14/02/20.

[Da] Damiani, E. et al.: Managing Multiple and Dependable Identities (2003), IEEE Computer Society.

[De] Demonstration of Hyperledger Indy, https://github.com/hyperledger-archives/education/blob/master/LFS171x/indy-material/nodejs/README.md, accessed 17/02/20.

[Ga] Garcia, Paco: Biometrics on the blockchain (2018), Biometric Technology Today, volume 2018, issues 5, pages 5-7.

[Ho] Hong, S. et al.: Design of Extensible Non-Fungible Token Model in Hyperledger Fabric (2019), pages 1-2.

[Hy] Hyperledger Indy, https://www.hyperledger.org/projects/hyperledger-indy, accessed 15/02/20.

[Is] Ismail, Reza: Enhancement of Online Identity Authentication Though Blockchain Technology (2017), https://www.syscode.asia/assets/files/oia-blockchain.pdf.

[Ku] Kuperberg, M.: Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective (2019), IEEE Transactions on Engineering Management.

[Li] Lim, S.Y. et al.: Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey (2018), International Journal on Advanced Science, Engineering and Information Technology, volume 8, pages 1737.

[Mu] Muhle, A. et al.: A survey on essential components of a self-sovereign identity (2018), Computer Science Review, volume 30, pages 80-86.

[Ve] Verifiable Credentials, https://www.w3.org/TR/vc-data-model, accessed 18/02/20.

[Wo] Wolfond, Greg: A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors (2017), Technology Innovation Management Review, volume 7, pages 35-40.