Identity Management using Ethereum Blockchain Platform

Enabling ERC 725 and ERC 735 Token for Identity Management
Identity management is a set of policies, processes and technologies used for managing access to information systems, safeguarding digital data and tracking system activities. The existing identity management system is not that secure and reliable. Blockchain on the other hand is an emerging technology that has gained a lot of attention in the past 5-6 years. Blockchain can address all the issues with existing identity management system. In this technical paper, the author has used Ethereum platform (ERC 725 and ERC 735 token) for managing identities of particular users from their social media accounts.
Traditionally, Identity Management is defined as the set of policies, processes and technologies used for managing access to information systems, safeguarding digital data and tracking system activities.

Figure 1, shows representation of Identity Management.

However, rising data breach incidents, identity theft cases and expanding global regulations increase connectivity between multitude of devices and the vast amount of available data about consumer demographic preferences, transactions and social media activities have forced the industry to further embrace and redefine the growing field of Identity Management. Companies constantly face the threats of consequences of unauthorized access to their information, assets and fraudulent transactions. The consequences of poor identity management are enormous and can result in financial losses and business data theft, reduced productivity, damaged reputation and non-compliance with regulations. Each organization uses various Identity and Access Management processes and resources to identify and track digital identities, assign and streamline access, monitor activities, control the exchange of data, provide end to end audit capability. Figure 2 Shows the Identity and Access Management process.
Identity management is the most important component in terms of an organization's fraud management, connectivity and compliance infrastructure to ensure that information assets are accessible only to authorized entities. However, the existing identity management system is neither too secure nor too reliable. Let's assume the scenario of a system that asks users to upload their government issued identity document (assume Indian Govt.), like Aadhaar Card (UID), PAN (permanent account number), or Social Security number and so on for verification purpose. Sharing IDs might lead the users to compromise with their privacy and also might result in data breaches. Each of us uses digital identity documents on regular basis, for getting loan from banks, for buying land, in case of ticket booking and others. All these identity documents are issued by government agencies and its identity management is vulnerable to data theft and data breaches.

Blockchain\(^{(2)}\) is an effective way to addresses all these issues through decentralized networks. Identity Management using blockchain ensures that trust, privacy and all the legal documents are endorsed and verified by permissioned participants. In depth explanation of need for blockchain based identity management is mentioned in Section 1.6.
Basic components of blocks are:

A. **Hash**: Unique identifier of current block. (always unique)

B. **Previous Hash**: Hash of previous block.

C. **Data**: Based on the type of blockchain

Figure 3, shows how three blocks are linked together. Block 2 contains a hash of Block 1 and Block 3 has hash of a Block 2. Any alteration or tampering in the block will lead to a change in the block hash. For instance, let’s assume there is some alteration of data that has been done in Block 2 causing the hash of Block 2 to change. Block 3 as it points towards the previous state hash of block 2, following block will become invalid. It is important to note that the first block is a bit special, as it has no hash of the previous block and is referred to as the Genesis Block. So it is clear that blockchain uses hashing to detect fraud or tampering, but it not only relies on hashing, but it also uses some consensus algorithm to make the system more secure. For example, **Proof of Work (PoW)**\(^{(3)}\) is a mechanism which slows down the creation of new blocks in a blockchain network. In bitcoin it takes about ten minutes to calculate the required PoW and add a new block to the blockchain network. This mechanism makes the entire process very complex and secure. For example if anyone from figure 3, tries to tamper with Block 2 which is then that individual (node/peer) needs to recalculate the PoW of all the other following blocks, practically impossible if we consider current computing system. So blockchain enables security by creative use of hashing and consensus algorithm. Additionally, blockchain is a peer to peer decentralized network.

The authors have used **ethereum\(^{(4)}\)** platform (ERC 725 Token and ERC 735 Token)\(^{(5)}\) and have explained the working of ethereum blockchain platform block in section 1.2. ethereum falls under the category of public blockchain.
Ethereum is one of the most popular decentralized blockchain platform. It has contributed a lot to the evolution of cryptocurrency. It is a state machine that is based on transactions. In the world of computing, the state machine reads a series of inputs and based on the inputs the state of the machine will transit to a new state. Figure 4, shows the representation of state machine and its transition to new state based on the inputs.

Figure 4

Ethereum state machine starts with “Genesis State”, it is a state where prior to it no transaction has taken place in the blockchain network. When any transaction is successfully executed, the state of ethereum changes from its current state say from Genesis state to State 1. Figure 5, shows the transition of ethereum.

Figure 5. State transition of ethereum from Genesis state

Each state of etherum has a series of transactions and these transactions are grouped into “blocks”. Each block is linked with its previous block. Figure 6 shows the chaining or linking of each blocks in ethereum.
For a transaction to be added in block, it must be valid, and verified by all the peers or nodes known as miners. All the miners have to solve a cryptographic puzzle (known as proof of work) to validate the transaction for adding the transaction in the block.

**Smart Contracts** are actually a business logic that are being developed as per requirements. It is used for automating and executing specific tasks based on some events. In ethereum platform, Smart Contracts are written in “Solidity”, the Ethereum State Machine or (Ethereum Virtual Machine) converts the solidity code into low level machinery language called Opcodes. Opcodes, often known as operational codes, are a set of instructions to execute specific task. Initially there were 140 unique opcodes.
For the purpose of efficiency, opcodes are encoded in bytecodes. For execution of each opcodes, the network consumes some **Gas** and corresponding **gas price** is required to execute the **opcodes**. If gas price exceeds the available price (in ETH), the contract will not be executed at all. This is how Ethereum works along with **smart contracts**.

**ERC 725**: Standard for blockchain-based identity. ERC 725 describes proxy smart contracts that can be controlled by multiple keys and other smart contracts.

**ERC 735**: ERC 735 is an associated standard to add and remove claims to an ERC 725 identity smart contract. These identity smart contracts can describe human, groups, objects and machines.
Need for Blockchain based Identity Management

According to a recent survey report in 2018, more than 4.5 billion\(^6\) records have been exposed and data breaches have occurred on a regular basis. Companies like Google, Microsoft, Amazon, Facebook have failed to safeguard customers and user data. As internet has become an intrinsic part of our life, there is no way of sharing our data without it being misused. The current approach to identity management is not suitable in the era of vast internet usage. Blockchain based digital identity management solution could address all the above mentioned issues, viz. data breach and data theft, security, privacy and usability. At present, creating digital identity still requires government issued identity documents. As a result it becomes very hectic and causes unnecessary trouble for those who might have lost their documents due to some external factors. Till date there is no relevant system which could secure either online authentication of our personal identities or digital identities. Blockchain technology will simply resolve this problem without the need for a trusted, central authority. Business organizations or individuals could store and authenticate their identity on the blockchain system, which would provide greater control over who has their personal information and how they would access it. By embedding open-source, decentralized feature in identity management, we could create a digital identity, which could act as an incorruptible fingerprint. This fingerprint could be used to verify an identity on real time basis for any transaction. Once this ID is created, it could be used to verify service corresponding to an identity without requiring the need for unreliable and clumsy password/email combinations. An identity is typically verified by performing an identity transaction. This actually involves three parties, IO Identity Owner, The person or business being identified, next CI: The claim issuer, for attestation process and finally the Third Party. In the existing process, all the involved entities have to struggle a lot with paper driven and centralized system. Additionally, the IO gives up his personal data, and is vulnerable to losing ownership. As all the data (identity related documents) or millions of records being stored in the central server are vulnerable to being hackers by hacker and hence IO becomes vulnerable to identity theft. This discussion establishes that the existing identity management systems are neither too secure nor too reliable. The solution to this problem is blockchain. The idea is very simple, only digital identity owner or holder could manage and control his/her digital identity- a concept known as SSID (Self-Sovereign Identity), solving the earlier challenges outlined: Security, Privacy and Usability. This is done by combining blockchain technology and identity management solution like Selfkey. Selfkey identity wallet can be used to create a SelfKey ID which is an encrypted, digital fingerprint attached with the identity. The wallet and ID are stored in a local device which means that even if Selfkey database is breached, wallet users would still be completely unaffected. The digital identity is stored on the Ethereum Blockchain, instead of being stored on centralized server, and only the owner/holder controls the private key for accessing their information. Nobody else can access the data without the permission of the owner. The identity management over blockchain not only gives unprecedented level of control over data, but also removes the need for time intensive identity verification. Once
In this section the author has described how they have managed the identity of a particular user on the basis of their social account and policy or rules made by claim checkers. Here are some associated terms in the workflow:

**Identity:** Controlled by keys, has claims and can add claims to other identities.

**Claim Issuer:** It is also an identity which is trusted by Claim Checkers to issue valid claims.

**Claim Checker:** A contract that only allows interactions from identities holding claims from trusted issuer.

**Claim:** Some data on one identity that comes from another identity.

Firstly, the user will create an identity. Then the user will ask for claim identity from the issuer, based on the predefined claiming conditions, like having valid Google, Facebook, LinkedIn, Twitter and Github accounts. If the user holds a valid account, the claim issuer will generate valid claim keys.

The Selfkey ecosystem is completed, the identity holder would be able to access the services with a click of button without losing control of digital identity.
3.1 Creating valid claim checks

Figure 9 and 10, show how authors have created claims on the basis of Google accounts. Authors have created a claim naming Property Listing, and this claim can only be accessed by an identity if he/she holds a valid Google account.
3.2 Creating an Identity

Figure 11 and 12 show how authors have created a new identity.

Figure 11

Figure 12. Creating identity with a dummy name
Figure 13 and 14 show the detailed information like address, owner of the Identity as well as the event which triggered and Block No. on which the identity was created.

Figure 13. Address and owner of the identity

Figure 14. Transaction details
Claim checker for verification purpose

Figure 15, shows the summary of Claim Checks, initially tested using a dummy identity ‘Nick’ for claiming the previously created claim named ‘property listing’ without using a valid Google account. The claim checker simply rejected or invalidated the claim as as shown in figure 15.

Figure 15. Shows the claim status without having a valid Google account
Figure 16, shows the event details of the claim checking status, viz. on which block the transaction has taken place. In author’s case the claim checking transaction has occurred in Block 8.

![Figure 16. Event details of claim checking](image)

Figure 17, shows that the user has started adding Google accounts to get valid claim. Figure 18, shows how a user’s claim is validated by the claim issuer upon signing in with a Google account.

![Figure 17. Adding Google accounts for getting a valid claim](image)
Figure 19, shows the claiming stage by suing dummy name 'Nick' after the claim issuer verifies the claimed data. Figure 20, depicts the stage of getting claim from the claim issuer.
As the data is verified, it denotes that the identity ‘Nick’ holds a valid Google account. So the claim for claimed named Property Listing by Nick will be valid whenever the claim is made from Nick’s end.
Conclusion

From the above discussion and results, the authors have concluded that blockchain is tamper-proof and immutable. Therefore, it can play a vital role in identity management, and can address the issue of privacy concern and data breach that exists in the current Identity Management processes or systems.

References


4. Online Access:

Zensar Technologies

Zensar is a leading digital solutions and technology services company that specializes in partnering with global organizations across industries on their Digital Transformation journey. A technology partner of choice, backed by a strong track record of innovation, credible investment in Digital solutions; and unwavering commitment to client success. Zensar’s comprehensive range of digital and technology services and solutions enables its clients to achieve new thresholds of business performance. Zensar, with its experience in delivering excellence and superior client satisfaction through myriad of technology solutions, is uniquely positioned to help its clients surpass challenges they face running their existing business most efficiently, helping in their legacy transformation, and planning for business expansion and growth through innovative and digital way.

Corporate Headquarters: Pune – India
Global Offices: US | UK | Europe | South Africa

For more information please contact: marketing@zensar.com | www.zensar.com