Identity Management Using Blockchain Technology

A. RASI MEGHANA[1], CH. V. RAMYA KRISHNA[2], D. P. R. SAI KUMARI[3]
[1, 2, 3] *Department of Electronics and Communication Engineering, Vasireddy Venkatadri Institute of Technology, Namburu, Guntur, Andhra Pradesh, India*

Abstract- ***Most online transactions require that individuals disclose specific personal information before they can proceed to access services. Thus, every time an individual discloses this information, it gets stored on numerous internet databases. As such, digital clones of one and the same individual spring into existence across these different platforms. This also exposes a lot of security issues. Blockchain can be used to create a platform that protects individuals' identities from theft and massively reduces fraudulent activities. The technology can also help businesses build strong blockchains that handle the issues of authentication and reconciliation encountered in several industries. Additionally, it can allow individuals the freedom to create encrypted digital identities that will replace multiple usernames and passwords. The entire system is implemented using Raspberry Pi 3 Model B.***

Indexed Terms- ***Blockchain, Digital Identity, Authentication, Security, Transactions, and Raspberry Pi.***

I. INTRODUCTION

"Blockchain Identity Management offers a decentralized and secure solution that puts users back in control via a distributed trust model"

The blockchain technology is benefiting several industries with transparency, security and many more features, adding value to their businesses. Thus, it is to be believed that it is all set to transform the current working of identity management as well, in a highly secure manner.

The existing identity management system is neither secure nor reliable. At every point, you are being asked to identify yourself through multiple government-authorized IDs like Voter ID, Passport, Pan Card and so on. Sharing multiple IDs leads to privacy concerns and data breaches. Therefore, the blockchain can pave the path to self-sovereign identity through decentralized networks.

A self-sovereign identity assures privacy and trust, where identity documents are secured, verified and endorsed by permissioned participants.

II. PROBLEMS WITH CURRENT IDENTITY MANAGEMENT

- Identity theft: People share their personal information online via different unknown sources or avail services which can put their identification documents into the wrong hands. Also, online applications maintain centralized servers for storing data; it becomes easier for hackers to hack the servers and steal the sensitive information.
- A combination of usernames and passwords: While signing up on multiple online platforms, users have to create a unique username and password every time. It becomes difficult for an individual to remember a combination of username and password for accessing different services. Maintaining different authentication profiles is quite a challenging task.
- KYC On-boarding: The current authentication process involves three stakeholders, including verifying companies/KYC companies, users, and third-parties that need to check the identity of the user. The overall system is expensive for all these stakeholders. Since KYC companies have to serve requests of different entities such as banks, healthcare providers, immigration officials, and so on, they require more resources to process their needs quickly
- Lack of Control: Currently, it is impossible for the users to have control over the personally identifiable information (PII). They do not have an idea of how many times PII has been shared or used without their consent. Moreover, individuals

do not even know where all their personal information has been stored. As a result, the existing identity management process requires an innovative change.

III. ROLE OF BLOCKCHAIN IN IDENTITY MANAGEMENT

Blockchain technology is well known for its tamper-proof nature. Since there is no central repository from which hackers can steal data, information stored on the blockchain is safe from data breaches that centralized databases frequently suffer from. Moreover, all transactions that happen between the identity holders and the companies are recorded on the blockchain, ensuring complete transparency.

Decentralized digital ledger technology also allows people the flexibility to create encrypted digital identities, which can be easily accessed through mobile applications, and be used to verify identity as and when required. This is a much more secure way as compared to carrying around traditional identity documents in wallets and bags.

We all heard about Bitcoin, Ether and other cryptocurrencies, which enables people to anonymously perform secure and trustworthy payments and transactions. In the heart of those cryptocurrencies there is a blockchain a decentralized database which records all transactions since their beginning. The entire network as opposed to a central entity such as a bank or government is continuously verifying the integrity of it. This way, users do not have to trust a central entity, but security is guaranteed by the strength and computing power of the entire network participating in the blockchain. Figure 1 shows the working of blockchain technology.

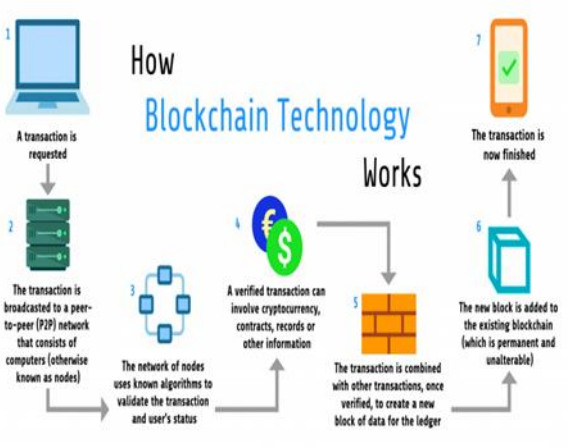


Figure 1: Working of Blockchain Technology

Authentication as a process of determining whether someone or something is, in fact, who or what it is declaring to be, is the key component of any trustworthy online system which handles sensitive data or transactions. Whether these systems are Internet of Things (IoT), industrial Internet, social networking or payment gateway system, the main aspect of those systems is the authentication process. The process of authentication is very visible to users. It directly influences their perception of trust. An ideal authentication process should be efficient, reliable and able to verify data credentials while protecting user's privacy.

IV. BLOCKCHAIN TECHNOLOGY

A blockchain is a chain of blocks of valid transactions. Each block includes the hash to the prior block in the blockchain. It uses a peer-to-peer network, which means every node in the network is connected to every other in the network. After the transaction is verified, it is broadcasted to the network and is added to everyone copy of the blockchain.

A block is referring to files where data pertaining to blockchain network is permanently stored. A block is like pages of a ledger or an account book. Each time a block is completed, it gives way to other block. Data stored in blocks cannot be altered. The genesis block, genesis. Son, is the first block of a blockchain.

Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without

a central authority (i.e., a bank, company or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published. In 2008, the blockchain idea was combined with several other technologies and computing concepts to create modern cryptocurrencies: electronic cash protected through cryptographic mechanisms instead of a central repository or authority. This technology became widely known in 2009 with the launch of the Bitcoin network, the first of many modern cryptocurrencies. In Bitcoin, and similar systems, the transfer of digital information that represents electronic cash takes place in a distributed system.

Bitcoin users can digitally sign and transfer their rights to that information to another user and the Bitcoin blockchain records this transfer publicly, allowing all participants of the network to independently verify the validity of the transactions. The Bitcoin blockchain is independently maintained and managed by a distributed group of participants. This, along with cryptographic mechanisms, makes the blockchain resilient to attempts to alter the ledger later (modifying blocks or forging transactions). Blockchain technology has enabled the development of many cryptocurrency systems such as Bitcoin and Ethereum1.

- Blockchain Structure

Blockchain technology is a data structure, which is represented by a list of blocks in a particular order, to establish, validate and share distributed ledger of different kinds of transactions through peer-to-peer (P2P) networks of computers (nodes). It is based on cryptographic hash functions, asymmetric-key cryptography and digital signature. The architecture of Blockchain network is a set of components and concepts as is shown in figure 2.

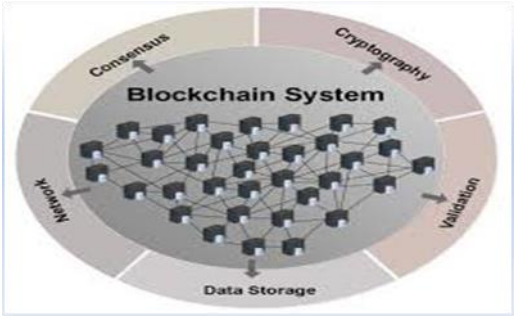


Figure 2: The Key Components of a Typical Blockchain System

Blockchain System is composed of a number of nodes and it mainly consists of the following mechanisms:

- Peer-to-peer network: Blockchain solutions are based on P2P network to exchange information between nodes using a secure broadcasting protocol. Each node is involved in the propagation of transaction without any central server. This topology is the basis of Blockchain decentralized feature.
- Storage: To store the entire blocks of transaction replicated on each node, Blockchain technology is based on state-machine replication. The decentralized storage eliminates the single point of failure so that the Blockchain system remains available despite the failure of some network participants. However, large blocks require large storage space and slower propagation in the network.
- Validation: this process ensures the integrity of Blockchain data avoiding issues such as double spending in crypto-currencies. Every node in the Blockchain network validates transactions against some rules by verifying that these transactions are legitimates and they have not already been spent. Then blocks consisting of valid transactions can be built.

- Consensus: is a set of rules making all the nodes synchronized with an agreement on the transactions existence and on the state of the ledger. Several consensus processes have been proposed on Blockchain, the most common are:

i. Proof - of Work (PoW) which is based on the scarcity of computational resources where miners

race to find an acceptable solution of a hard mathematical problem .

ii. Proof - of -Stake (PoS) which is an alternative to PoW and it is based on the scarcity of the currency.

- Cryptography: this mechanism grants broad security and privacy to the data. Blockchain uses an asymmetric cryptography mechanism for transactions and wallets . Thus, the stored data is immutable and the created blocks are impossible to be deleted or edited.

  All the above mechanisms in blockchain make it more advantageous when compared to other technologies figure 3 shows advantages of Blockchain Technology

- Classification of Blockchain:
  Based on their permission model, Blockchain systems are categorized into three types :

  Permissionless or public Blockchains: In this category of infrastructure, anyone can join the network and begins submitting transactions without needing permission to interact with the network. This category of Blockchain has been the essence of the digital currencies market by introducing open source solutions like Bitcoin and Ethereum.

- Permissioned or Private Blockchains: these infrastructures are closed ecosystems which require pre-verification of the participating parties within the network. Therefore, only restricted users have the rights to validate the block transactions. Permissioned Blockchains are preferred by centralized organizations to increase the control of their internal business operation.

- Consortium Blockchain: this kind of Blockchain is partly private where the consensus process is controlled by a selected set of participants, while the right to read Blockchain data is allowed to the public or is restricted to the participants.

- Advantages of the blockchain technology include:

i. Immutability: nothing on the blockchain can change. Any confirmed transaction cannot be altered.
ii. Permanence: A public blockchain will act as a public ledger, data will be accessible if the blockchain remains active.
iii. Removal of intermediaries: The peer-to-peer nature of the blockchain does away with the need of intermediaries.
iv. Speed: Transactions are much faster than a centrally controlled ledger.
v. Security: Neither the node nor anyone else except the sender and the receiver can access the data sent across the blockchain.

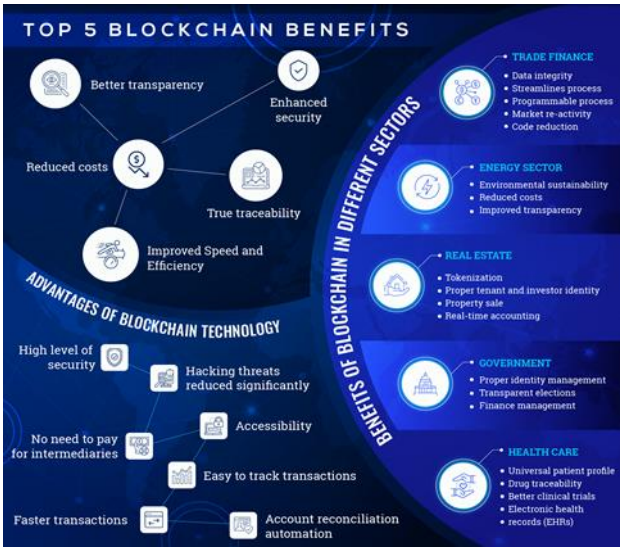


Figure 3: Advantages of Blockchain Technology.

V. IMPLEMENTATION OF IDENTITY MANAGEMENT ON BLOCKCHAIN

Software used: Among the available blockchain development platforms, the most popular are Ethereum, Hyperledger, and IBM Blockchain. For the evaluation of this model, Ethereum is being used as a platform. The software packages and libraries used in the design are listed in Table 1.

Table 1. Packages and Libraries used in the system design.

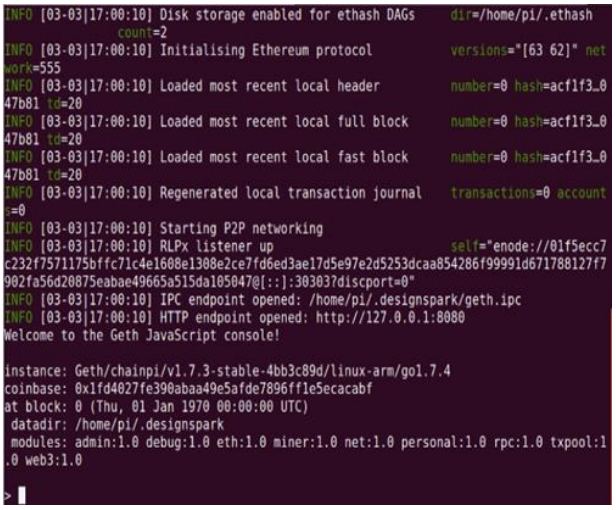
Package/Library	Version
geth	1.9.6
Ethereum	1.0.8
eth_abi	2.0.0
ethjsonrpc	0.3.0
Truffle	5.0.39
Solidity	0.5.12
Py_solc	3.2.0
Node	10.15.2
Web3.js	1.2.1
Python	3.7.3
go	1.10.4

An Ethereum node is created by using geth. geth is the implementation of Ethereum node in Go language. Truffle, an Ethereum based development and testing framework that is built over the Ethereum Virtual Machine (EVM), has been used for generating executable byte code. Truffle has in-built support for smart Contracts 'compilation and linking. The environment of the Truffle framework also supports binary management and smart contract deployment. It also supports automated contract testing for rapid prototyping of applications. In order to reduce the computational costs and complexity, this model uses lightweight smart contracts instead of conventional consensus mechanisms to record transactions and allow access to the resources.

Solidity, the official programming language to build smart contracts in Ethereum based blockchains, is used to code the smart contracts. Web3.py, a Python API based on web3.js, provides interaction between applications and the smart contracts

VI. RESULTS

Starting geth Console:



Balance Verification commands:

- Created another Node in Raspberry Pi
- Balance, by default, is ZERO.

- To perform a transaction, each node should be authorized. In order to authorize the node, the node should be added as a peer to the network. To add as a peer, we need enode information of the node.

CONCLUSION

Identity management is of paramount importance in secured digital transactions. In this work, we have proposed an identity management based on blockchain technology. Blockchain technology is the technology of future and can efficiently handle security threats. The built in features such as end-to-end traceability derived from immutability of data records, authentication and authorization adds value to the multidisciplinary technological solutions. In this blockchain based identity management system, the hashed addresses of the wallet are used as identities. We have created multiple accounts within the same system and added them as peers to a miner. The transactions are only allowed within the peers after proper identity verification. The proposed model uses open-source libraries and hence it is compatible with Ethereum main chain. The designed system can be deployed into any real-time application with miner modifications.

REFERENCES

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

[2] Wang, R.; He, J.; Liu, C.; Li, Q.; Tsai, W.; Deng, E. A Privacy-Aware PKI System Based on Permissioned Blockchains. In Proceedings of the 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 23–25 November 2018; pp. 928–931.

[3] Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Comm. Surveys & Tutorials 2015, 17, 2347–2376.

[4] Lindsay, J. Smart Contracts for Incentivizing Sensor Based Mobile Smart City Applications. In Proceedings of the 2018 IEEE International Smart Cities Conference(ISC2), Kansas City, MO, USA, 16–19September2018; pp. 1–4.

[5] Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. IEEE Access 2019, 7, 22328–22370.

[6] Hyperledger: Open Source blockchain Technologies. Available online: https://www.hyperledger.org/

[7] K. Cameron, ―The laws of identity,‖ Microsoft Corp, 2005.

[8] V. Buterin, ―On public and private blockchains,‖ Ethereum blog, vol. 7, 2015.

[9] Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.

[10] A. Tobin and D. Reed, ―The inevitable rise of self-sovereign identity,‖ The Sovrin Foundation, vol. 29, 2016