Blockchain for Maintaining Assets: A Survey

Abhishek Yadav[1], Sai Pisey[2], Vedant Tilvankar[3], Prof. Sarita Khedikar[4]

[1-3]Students, Dept. of Computer Engineering, Smt. Indira Gandhi College of Engineering, Navi Mumbai, Maharashtra, India.
[4]Professor, Dept. of Computer Engineering, Smt. Indira Gandhi College of Engineering, Navi Mumbai, Maharashtra, India.

---***---

Abstract - Since the introduction of Bitcoin in January 2009 by Satoshi Nakamoto, the thought of creating products & solving existing real-life problems in all facets of life with non-centralized technology i.e Blockchain has gained considerable momentum owing to its immutable nature. This has created a plethora of possible use case scenarios. A huge amount of potential applications - right from education to healthcare to defence have been theorized and many have been implemented. With the emergence of novel feature-packed Blockchains like Ethereum & frameworks like Hyperledger Fabric, the process of developing Blockchain-based software and products has been expedited & simplified. This paper talks about one specific application of Blockchain - 'Asset Registration & Management' and discusses various concepts & ideas attributed to the same.

Key Words: **Blockchain, Ethereum, Smart Contract, Digital Assets, Security.**

1.INTRODUCTION

Blockchain in simple terms is a distributed ledger that keeps a track record of all the transactions performed in a network and is tamper & revision proof. The virtues of Blockchain were most functionally apparent in Bitcoin's blockchain implementation which allows decentralizing currency - something which was always believed to require a centralized third party to ensure a smooth exchange. This led to a revision of the aforementioned thought with scientists and researchers trying to explore the complete potential of this technology in other walks of life**[8]**.

From being the backbone of the famous cryptocurrency Bitcoin, Blockchain has evolved and different types of blockchains have been developed which serve different use cases in multiple domains. One such transformation is Ethereum which was conceived in 2013 by programmer Vitalik Buterin. The wide usage & versatility of Ethereum can be credited to the availability of a programmable utility known as a 'Smart Contract'. To highlight the revolutionary implications of such functionality, we can take a glimpse at the inherently vulnerable nature of Centralized Systems **[1]**. Smart Contracts have empowered us to create parallel systems in which no central authority is required - the programmed code executes automatically on completion of, or occurrence of certain tasks or triggers respectively & performs desired functions according to the terms of the contract or agreement according to which the smart contract has been created. Right from the dawn of the Internet age, maintaining digital assets has been a difficult task for obvious reasons. Blockchain Asset storage provides an answer to this problem. This paper explores and discusses some recent research in this domain.

2. BLOCKCHAIN

2.1 INCEPTION

Contrary to popular belief, blockchain did not originate in 2008, rather a protocol similar to the blockchain was described in 1982 by cryptographer David Chaum in his dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups". In the subsequent year, scientists Stuart Haber and W. Scott Scornetta proposed a computationally practical solution for time-stamping digital documents. The necessity behind the development of this solution can be traced back to the transition from physical document storage to digital document storage technology, which provided efficiency but increased the possibility of fraud via back-dating or tampering due to the ramifications of digital storage- 'ease of editing'. The aforementioned scientists developed a system that stored a cryptographically secured or hashed chain of blocks to store the time-stamped documents as a solution to this problem. In 1992, Merkle trees were introduced in this design, which allowed the collection of several documents into one block. Later in 2004, due to the emergence of the idea of digital cash, computer scientist and cryptographic activist Hal Finney introduced a system called Reusable Proof Of Work(RPoW) as a prototype. Blockchain gathered fame when it was proposed by Satoshi Nakamoto in 2008 to support the idea of trustless cryptocurrency Bitcoin as it allowed time-stamping blocks without the need of a trusted third party and to serve as a public ledger for all users of the currency**[7]**. As of today, many mutations of the vanilla blockchain platform have been created and found, each differing in its structure and functionality, most of which are the backbone of various cryptocurrencies that exist today. Some notable examples are - Ethereum, Stellar, Tron, Corda, Hyperledger Fabric, Open-chain etc.

2.2 CONCEPT

The main motivation behind the development of blockchain is to replace centralized trust-based systems with peer to peer, decentralized, trustless, encrypted, tamper-proof systems which rely on cryptographic and other infallible methods for their operation and are transparent. The fundamental unit of a blockchain is a block. It contains a batch of valid transactions encoded in a Merkle tree along with a timestamp and cryptographic hash of the previous block. Starting from the genesis block, each block is linked to its previous block. Each block is digitally signed & an attempt to tamper with the contents of a block entails the modification of all subsequent blocks. This ensures integrity in a blockchain. It also facilitates inexpensive verification of transactions. Once created, blocks are broadcasted and verified by all other nodes. Once a consensus is achieved, the block is added to the blockchain. In the traditional blockchain, verification is incentivized by rewards. This is known as Proof of Work - proof that a node has worked transaction-related algorithms to verify a certain block. This is the consensus algorithm used in Bitcoin's underlying blockchain**[7]**. Although this is the most prominently known algorithm, it doesn't scale well. The computational problem to be worked on becomes harder as the network grows and requires devices or nodes with higher-end device configurations and a huge pool of resources which eventually inhibits the ability of all but a few powerful nodes(big organizations) to verify transactions. Thus, the network tends towards centralization and also becomes vulnerable to attacks like 51% attack. To overcome this, other consensus algorithms like Proof of Stake(PoS), Proof of Capacity(POC) etc. exist albeit their share of concerns**[3]**.

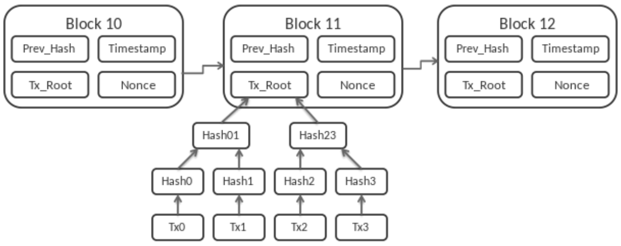

Fig -1: A brief overview of a blockchain segment

(By Matthäus Wander - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=26816920)

In a nutshell, the Block addition process is-

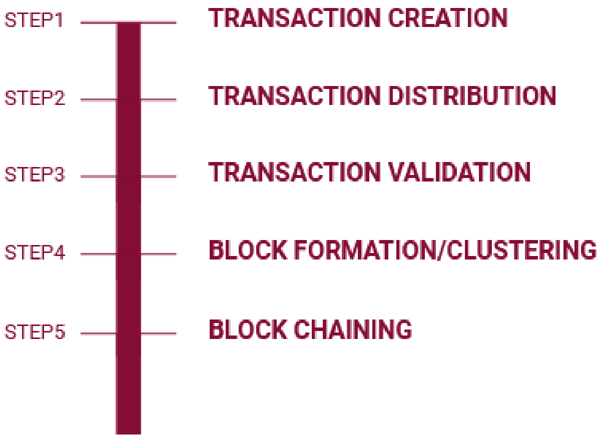

Fig -2: Block Addition process in Blockchain

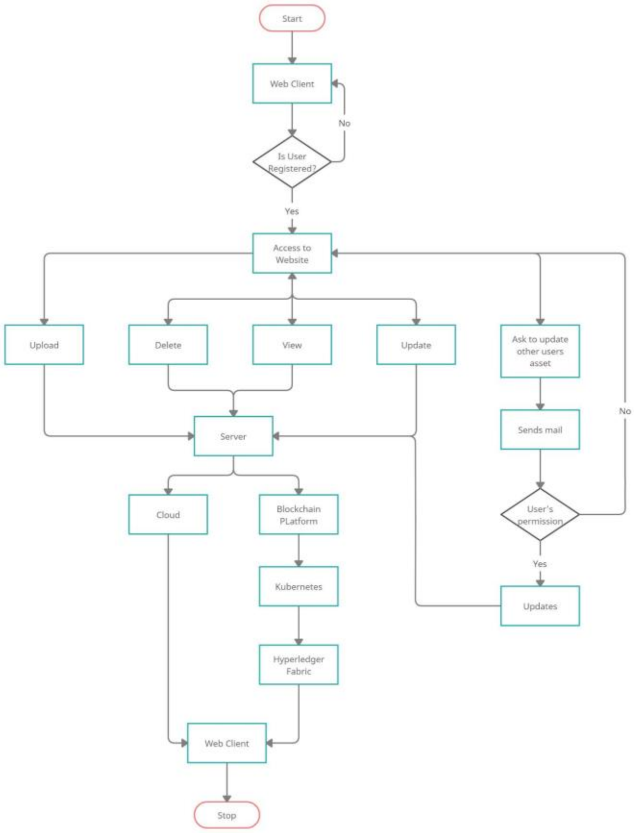

Fig -3: Flowchart of Blockchain Asset Management System

3. ETHEREUM

Ethereum was built to enable developers, publish smart contracts and distributed applications(dApps) that can be used without the risks of downtime, fraud, or interference from a third party. It describes itself as "the world's programmable blockchain.".

Ethereum was not only built as a currency exchange or cryptocurrency as we know it today but it was among the first to consider the potential of blockchain technology for uses beyond the trading virtual currency.

ETH was created as a platform that can be used to "codify, decentralize, secure, and trade just about anything."

For data to persist forever we need some kind of persistence mechanism - Ethereum persistence mechanism is that the whole chain is accounted for when running the node. New data is added to the end of the chain and it keeps growing. This is called blockchain-based persistence. Contract-based persistence has the intuition that data cannot be stored forever and instead must be kept with contract agreements. These are agreements made with multiple nodes that have promised to hold a piece of data for some time. They must be refunded or renewed whenever they run out to keep the data persisted.

In most cases, instead of storing all data on-chain, the hash of where the data is located on a chain gets stored. This way, the entire chain doesn't need to scale to keep all of the data**[6]**.

4. SURVEY

4.1 ASSET MANAGEMENT

All entities like automobiles, houses, organizations etc. can be classified as assets. These assets are owned by certain individuals or groups of individuals and have corresponding documentation about some time existence, ownership, transferability etc. These documents or records can be digitally signed and stored in the blockchains to secure them from tampering. It will also improve the efficiency and reduce the cost as there would be no intermediary to verify the transactions**[4]**. In addition to traditional blockchain-like features, the USP of Ethereum is the availability of 'Smart Contracts': Contracts that execute and perform desired operations automatically when certain conditions are met, without the mediation of a third party to enforce the contract. Ethereum by nature is a public blockchain but can be modified and built as a private or permissioned blockchain as per requirements. Thus, dApps can be created which can automate and decentralize the process of buying, selling & transferring of assets based on smart contracts which would execute only after a certain set of conditions are met, e.g. proof of being the next of kin to inherit property, transfer of funds after obtaining an asset (supply chain application) etc**[5]**.

4.2 IDENTITY MANAGEMENT

Due to the rise of traffic on the internet, there have been multiple challenges faced in identity management which include - security, privacy & usability.

Blockchain technology provides a solution to the above problems without the need for a central trusted authority. It is used for creating an identity on the blockchain making it easier to manage individuals and giving them more power over who has access to it.

Through the infrastructure of a blockchain, the verifying parties do not need to check the validity of the actual data in the provided proof but can rather use the blockchain to check the validity of the attestation and attesting party (such as the government) from which they can determine whether to validate the proof**[2]**.

Birth/Marriage/Death certificates

For example, when an identity owner presents proof of their date-of-birth or any other certificate of such kind, rather than checking the truth of the date of birth itself, the verifying party will validate the government's signature who issued and attested to this credential to then decide whether they trust the government's assessment about the accuracy of the data.

Revocation means deleting or updating a credential. The possibility for an issuer to revoke a credential is crucial to an identity infrastructure for the main reason that identities are dynamic**[13]**.

Licenses/Allowances

Attributes can change over time e.g. house address or several children, and some credentials should have an expiry date for example a passport or drivers licence. The fact is, however, that to ensure the trustworthiness of the system and eliminate the possibility to defraud, credentials are immutable.

After issuing, no one (not even the issuer) can change the information inside the credential. Hence, when attributes change, a new credential needs to be issued and the old one needs to be announced invalid. Thus, at each proof, the users need to prove that the credentials used in the proof are still valid. The revocation registry allows them to prove this without contacting the issuing party**[14]**.

4.3 INTELLECTUAL PROPERTY MANAGEMENT

Nowadays lots of legal, economic and technology-focused debates on how to control the value bound in easily reproducible assets against copyright are going on.

Today, copyright is characterised by an expansive focus that encompasses text-based, painterly, sculptural, photographic, choreographic, architectural, audio-visual, musical, and code-based works, It was considered as a tool that would legally limit and restrict how assets should be reproduced**[9]**.

As blockchain technology is secured and distributed it will help curb the copyright issues and will maintain the authenticity of the asset. It will help control the reproducible assets too.

One of the major challenges in the market of the art is that the artist is not alive to verify and authenticate the provenance. This could be changed by Blockchain, as there are decentralized lists of records that are linked and secured by using cryptography. Hosted by millions of computers simultaneously thus no centralized version of the information is available so a hacker cannot access or corrupt the data.**[10]**

When it comes to artwork, two things are really important, if the artwork is real and does a person have the authority to sell the artwork. Blockchain can track and verify the authenticity of the artwork through timestamps on transactions and cryptographic signature, this will solve the issue.

Blockchain has introduced a term as “Digital Scarcity” involves issuing a limited number of copies of artwork, that’s where NFTs take their place. NFTs are digital tokens tied to artwork to prove its authenticity and provenance. NFTs are non-fungible, which means that they are one of a kind. At a very high level, most NFTs are a part of the ethereum blockchain. Some others can implement their version of NFTs.**[12]**

Various artists can publish their artforms on blockchain platforms - anything from pictures, sculptures to videos. As they have NFT tagged, it will have a unique tag to it and for every transaction, it will have a unique timestamp to it for maintaining the provenance. And since it is based on the blockchain it is secured as blockchain is distributed, decentralized and hashed.

5. CONCLUSION

In Blockchain Asset Management, there would be a large number of users and different kinds of actions - users can upload their assets in the form of documents, audio, a video which indicates that the project is very flexible. Blockchain will also allow for the history of the transactions to be maintained in the ledger, and thereby ensuring that there is always a chain of record for any changes that have been made to any asset. This impenetrable digital ledger makes fraud, hacking, data theft or any other kind of scam activity impossible. If any modifications are required then the user can ask for permission from another user; if permission is granted then changes could be done. Thus it shows a good use case of the Blockchain. Digital asset management can be accomplished securely and conveniently in this version.

REFERENCES

[1] N. V. Kuchin and N. G. Butakova, "Vulnerability Analysis of Corporate Blockchain Systems to Network Attacks," 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2021, pp. 2366-2371, DOI: 10.1109/ElConRus51938.2021.9396701.

[2] Uri Jocobovitz, "Blockchain for Identity management", Technical Report #16-02, The Lynne and William Frankel Center for Computer Science Department of Computer Science, Ben-Gurion University, Beer Sheva, Israel, 2018.

[3] Guru, D.; Perumal, S.; Varadarajan, V. Approaches towards Blockchain Innovation: A Survey and Future Directions. *Electronics* **2021**, *10*, 1219. https://doi.org/10.3390/electronics10101219

[4] Danda B. Rawat, Vijay Chaudhary and Ronald Doku, “Blockchain: Emerging Applications and Use Cases”, Data Science and Cybersecurity Center (DSC^2), Department of Electrical Engineering and Computer Science, Howard University, Washington, DC 20059, USA. https://arxiv.org/abs/1904.12247

[5] Ethereum-powered tools and services. https://ethereum.org/en#what-are-dapps

[6] Ethereum,https://en.wikipedia.org/w/index.php?title =Ethereum&oldid=1049440802

[7] Blockchain,https://en.wikipedia.org/w/index.php?titl e=Blockchain&oldid=1049096395

[8] BlockchainExplained.https://www.investopedia.com/ terms/b/blockchain.asp

[9] Zeilinger, M. Digital Art as ‘Monetised Graphics’: Enforcing Intellectual Property on the Blockchain. *Philos. Technol.* 31, 15–41 (2018). https://doi.org/10.1007/s13347-016-0243-1

[10] Whitaker, Amy. (2019). Art and Blockchain: A Primer, History, and Taxonomy of Blockchain Use Cases in the Arts. Activate A Journal of Enterprise in the Arts. 21-47. 10.34053/artivate.8.2.2.

[11] Jung, Seung Wook. (2021). A Novel Authentication System for Artwork Based on Blockchain. 10.1007/978-3-030-79474-3_11.

[12] Nadini, Matthieu & Alessandretti, Laura & Di Giacinto, Flavio & Martino, Mauro & Luca, Maria & Baronchelli, Andrea. (2021). Mapping the NFT revolution: market trends, trade networks and visual features. https://arxiv.org/abs/2106.00647

[13] “Love on the Block” by Max Dovey; Ruth Catlow, Marc Garrett, Nathan Jones and Sam Skinner (eds), Artists Re: Thinking the Blockchain, Liverpool and London: Torque and Furtherfeld, 2017

[14] Blockchain Identity Management: The Definitive Guide(2021Update),https://tykn.tech/identity-management-blockchain/