BLOCKCHAIN TECHNOLOGY ARCHITECTURE AND KEY CHARACTERISTICS

Prof. Gayathri Naidu, Prof. Reeta Mishra

Assistant Professor and head of Computer Engineering Department,
S.B. Polytechnic, Savli, Dist.-Vadodara, Gujarat, India

Assistant Professor in Information Technology Department,

K.J. Institute of Engineering & Technology, Savli, Dist.-Vadodara, Gujarat, India

ABSTRACT

Blockchain is a decentralized transaction and data management technology developed first for Bitcoin cryptocurrency. Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation system and Internet of Things (IoT), and so on. This paper presents a comprehensive overview on blockchain technology, blockchain architecture and comparison of different blockchains types like public blockchain, private blockchain and consortium blockchain. The reason for the interest in Blockchain is, its central attributes that provide security, anonymity and data integrity without any third party organization in control of the transactions, and therefore it creates interesting research areas, especially from the perspective of technical challenges and limitations. The majority of research is focusing on revealing and improving limitations of Blockchain from privacy and security perspectives, but many of the proposed solutions lack concrete evaluation on their effectiveness and scalability.

Key words: —*Blockchain, Bitcoin, Decentralized, Hash Value*

I. INTRODUCTION

Blockchain:

A blockchain is a growing list of records, called blocks, which are linked using cryptography. Blockchains are a remarkably transparent and decentralized way of recording lists of transactions. Blockchains which are readable by the public are widely used by cryptocurrencies. Private blockchains have been proposed for business use. Some marketing of blockchain has been called "snake oil". [3]

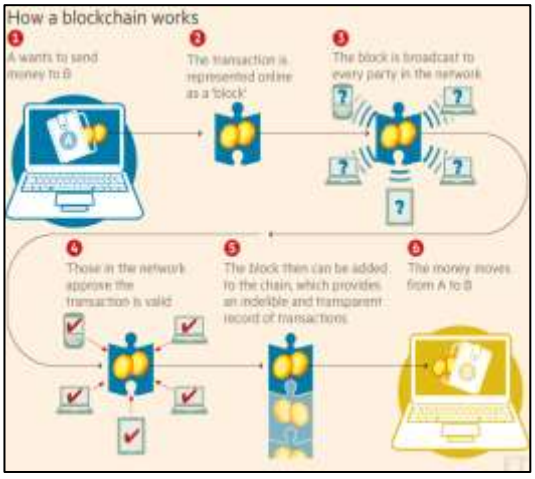

Fig. 1: How a Blockchain Works

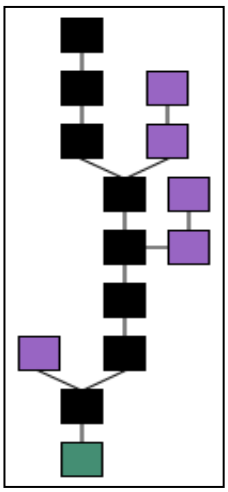

Fig. 2: Blockchain Formation

Blockchain formation:

The main chain (black) consists of the longest series of blocks from the genesis block (green) to the current block. Orphan blocks (purple) exist outside of the main chain.

II. BLOCKCHAIN ARCHITECTURE

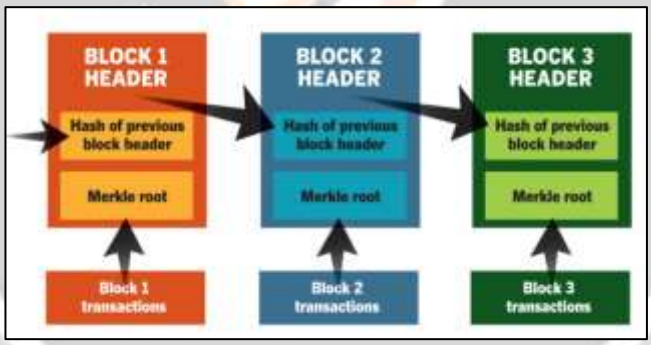

Fig. 2: Blockchain Formation

Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a merkle tree root hash). By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority.

Currency transactions between persons or companies are often centralized and controlled by a third party organization. Making a digital payment or currency transfer requires a bank or credit card provider as a middleman to complete the transaction. In addition, a transaction causes a fee from a bank or a credit card company. The same process applies also in several other domains, such as games, music, software etc. The transaction system is typically centralized, and all data and information are controlled and managed by a third party organization, rather than the two principal entities involved in the transaction. Blockchain technology has been developed to solve this issue. The goal of Blockchain technology is to create a decentralized environment where no third party is in control of the transactions and data. Blockchain is a distributed database solution that maintains a continuously growing list of data records that are confirmed by the nodes participating in it. The data is recorded in a public ledger, including information of every transaction ever completed.

Blockchain is a decentralized solution which does not require any third party organization in the middle. The information about every transaction ever completed in Blockchain is shared and available to all nodes. This attribute makes the system more transparent than centralized transactions involving a third party. In addition, the nodes in Blockchain are all anonymous, which makes it more secure for other nodes to confirm the transactions. Bitcoin was the first application that introduced Blockchain technology. Bitcoin created a decentralized environment for cryptocurrency, where the participants can buy and exchange goods with digital money. However, even though Blockchain seems to be a suitable solution for conducting transactions by using cryptocurrencies, it has still some technical challenges and limitations that need to be studied and addressed. High integrity of transactions and security, as well as privacy of nodes are needed to prevent attacks and attempts to disturb transactions in Blockchain. In addition, confirming transactions in the Blockchain requires a computational power. [1]

Background Blockchain, mostly known as the technology running the Bitcoin cryptocurrency, is a public ledger system maintaining the integrity of transaction data . Blockchain technology was first used when the Bitcoin cryptocurrency was introduced. To this day, Bitcoin is still the most commonly used application using Blockchain technology. Bitcoin is a decentralized digital currency payment system that consists of a public transaction ledger called Blockchain. The essential feature of Bitcoin is the maintainability of the value of the currency without any organization or governmental administration in control. The number of transfers and users in the Bitcoin network is constantly increasing. In addition, the conversions with traditional currencies, e.g. KRW, EUR and USD, occur constantly in currency exchange markets. Bitcoin has therefore gained the attention of various communities and is currently the most successful digital currency using Blockchain technology.

Digital Signature:

Each user owns a pair of private key and public key. The private key that shall be kept in confidentiality is used to sign the transactions. The digital signed transactions are broadcasted throughout the whole network. The typical digital signature is involved with two phases: *signing phase* and *verification phase*. For instance, an user A wants to send monet to another user B. (1) In the signing phase, User A encrypts data with its private key and sends B the encrypted result and original data. (2) In the verification phase, B validates the value with A's public key. In that way, B could easily check if the data has been tampered or not.
The typical digital signature algorithm used in blockchains is the elliptic curve digital signature algorithm (ECDSA) [2].

III. KEY CHARACTERISTICS OF BLOOCKCHAIN

Blockchain has following key characteristics.

• *Decentralization.* In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank), inevitably resulting to the cost and the performance bottlenecks at the central servers. Contrast to the centralized mode, third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to maintain data consistency in distributed network. [4]

• *Persistency.* Transactions can be validated quickly and invalid transactions would not be admitted by honest miners. It is nearly impossible to delete or rollback transactions once they are included in the blockchain. Blocks that contain invalid transactions could be discovered immediately. [4]

• *Anonymity.* Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user. Note that blockchain cannot guarantee the perfect privacy preservation due to the intrinsic constraint. [4]

Auditability. Bitcoin blockchain stores data about user balances based on the Unspent Transaction Output (UTXO) model : Any transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the blockchain, the state of those referred unspent transactions switch from unspent to spent. So transactions could be easily verified and tracked. [4]

Types of Blockchain:

- Public Blockchain
- Private Blockchain
- Consortium Blockchain

Property	**Public Blockchain**	**Consortium Blockchain**	**Private Blockchain**
Consensus determination	All miners	Selected set of nodes	One organization
Efficiency	Low	High	High
Cost	High	Low	Low
Centralized	No	Partial	Yes

TABLE 1: Comparisons among public blockchain, consortium blockchain and private blockchain

IV. CHALLENGES

Despite the great potential of blockchain, it faces numerous challenges, which limit the wide usage of blockchain. We enumerate some major challenges and recent advances as follows.

A. Scalability

With the amount of transactions increasing day by day, the blockchain becomes bulky. Each node has to store all transactions to validate them on the blockchain because they have to check if the source of the current transaction is unspent
or not. Besides, due to the original restriction of block size and the time interval used to generate a new block, the Bitcoin blockchain can only process nearly 7 transactions per second, which cannot fulfill the requirement of processing millions of transactions in real-time fashion. Meanwhile, as the capacity of blocks is very small, many small transactions might be delayed since miners prefer those transactions with high transaction fee.
There are a number of efforts proposed to address the scalability problem of blockchain, which could be categorized into two types:

- *Storage optimization of blockchain*
- *Redesigning blockchain*.

B. Privacy Leakage

Blockchain can preserve a certain amount of privacy through the public key and private key. Users transact with their private key and public key without any real identity exposure. However, it is shown in [40], [5] that blockchain cannot guarantee the *transactional privacy* since the values of all transactions and balances for each public key are publicly visible. Besides, the recent study [41] has shown that a user's Bitcoin transactions can be linked to reveal user's information. Moreover, Biryukov et al. presented an method to link user pseudonyms to IP addresses even when users are behind Network Address Translation (NAT) or firewalls. each client can be uniquely identified by a set of nodes it connects to. However, this set can be learned and used to find the origin of a transaction. Multiple methods have been proposed to improve anonymity of blockchain, which could be roughly categorized into two types: [4]

- *Mixing*
- *Anonymous*.

C. Selfish Mining

Blockchain is susceptible to attacks of colluding selfish miners. In particular, Eyal and Sirer [10] showed that the network is vulnerable even if only a small portion of the hashing power is used to cheat. In selfish mining strategy, selfish miners keep their mined blocks without broadcasting and the private branch would be revealed to the public only if some requirements are satisfied. As the private branch is longer than the current public chain, it would be admitted by all miners. Before the private blockchain publishment, honest miners are wasting their resources on an useless branch while selfish miners are mining their private chain without competitors. So selfish miners tend to get more revenue. Based on selfish mining, many other attacks have been proposed to show that blockchain is not so secure. In stubborn mining [48], miners could amplify its gain by non-trivially composing mining attacks with network-level eclipse attacks. The trail-stubbornness is one of the stubborn strategy that miners still mine the blocks even if the private chain is left behind. Each

block must be generated and accepted by the network within a maximum time interval. Within ZeroBlock, selfish miners cannot achieve more than its expected reward. [4]

V. CONCLUSION

Blockchain has shown its potential for transforming traditional industry with its key characteristics: decentralization, persistency, anonymity and auditability. This paper presents a comprehensive overview on blockchain. blockchain architecture and key characteristics of blockchain and comparison done among the types of blockchain along with the parameters like consensus determination, efficiency and cost Nowadays blockchain based applications are springing up and planned to conduct in-depth investigations on blockchain-based applications in the future..

References:

[1] Jesse Yli-Huumo1 , Deokyoon Ko2 , Sujin Choi4 *, Sooyong Park2 , Kari Smolander3 "Where Is Current Research on Blockchain Technology? - A Systematic Review.", PLOS ONE, 10(11), [e0163477]. DOI: 10.1371,October 2016.

[2] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ecdsa)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[3] https://en.wikipedia.org/wiki/Blockchain

[4] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3 2013," An Overview of Blockchain Technology:
Architecture, Consensus, and Future Trends" IEEE 6th International Congress on Big Data 2017.

[5]https://www.blockchaindailynews.com/The-difference-between-a-Private-Public-Consortium-Blockchain_a24681.html