**BLOCKCHAIN TECHNOLOGY**

**by**

**ADAMU MOHAMMED SANUSI**

**st/cs/nd/19/450**

**A SEMINAR PRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY, FEDERAL POLYTECHNIC MUBI, ADAMAWA STATE, NIGERIA**

**DECEMBER, 2021**

**Abstract**

*Blockchain, the foundation of Bitcoin, has received extensive attentions recently. 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. However, there are still many challenges of blockchain technology such as scalability and security problems waiting to be overcome. This paper presents a comprehensive overview on blockchain technology. We provide an overview of blockchain architechture firstly and compare some typical consensus algorithms used in different blockchains. Furthermore, technical challenges and recent advances are briefly listed. We also lay out possible future trends for blockchain.*

# **INTRODUCTION**

Nowadays cryptocurrency has become a buzzword in both industry and academia. As one of the most successful cryptocurrency, Bitcoin has enjoyed a huge success with its capital market reaching 10 billion dollars in 2016 (Kosba, 2017). With a specially designed data storage structure, transactions in Bitcoin network could happen without any third party and the core technology to build Bitcoin is blockchain, which was first proposed in 2008 and implemented in 2009 (Akins & Gordon, 2013). Blockchain could be regarded as a public ledger and all committed transactions are stored in a list of blocks. This chain grows as new blocks are appended to it continuously. Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency. The blockchain technology generally has key characteristics of decentralization, persistency, anonymity and auditability. With these traits, blockchain can greatly save the cost and improve the efficiency.

Since it allows payment to be finished without any bank or any intermediary, blockchain can be used in various financial services such as digital assets, remittance and online payment. Additionally, it can also be applied into other fields including smart contracts, public services, Internet of Things (IoT), reputation systems and security services. Those fields favor blockchain in multiple ways. First of all, blockchain is immutable. Transaction cannot be tampered once it is packed into the blockchain. Businesses that require high reliability and honesty can use blockchain to attract customers. Besides, blockchain is distributed and can avoid the single point of failure situation. As for smart contracts, the contract could be executed by miners automatically once the contract has been deployed on the blockchain (Biryukov, 2014).

Although the blockchain technology has great potential for the construction of the future Internet systems, it is facing a number of technical challenges. Firstly, scalability is a huge concern. Bitcoin block size is limited to 1 MB now while a block is mined about every ten minutes. Subsequently, the Bitcoin network is restricted to a rate of 7 transactions per second, which is incapable of dealing with high frequency trading. However, larger blocks means larger storage space and slower propagation in the network. This will lead to centralization gradually as less users would like to maintain such a large blockchain. Therefore the tradeoff between block size and security has been a tough challenge. Secondly, it has been proved that miners could achieve larger revenue than their fair share through selfish mining strategy (Eyal & Sirer, 2014). Miners hide their mined blocks for more revenue in the future. In that way, branches could take place frequently, which hinders blockchain development. Hence some solutions need to be put forward to fix this problem. Moreover, it has been shown that privacy leakage could also happen in blockchain even users only make transactions with their public key and private key (Tschorsch et al., 2016). Furthermore, current consensus algorithms like proof of work or proof of stake are facing some serious problems. For example, proof of work wastes too much electricity energy while the phenomenon that the rich get richer could appear in the proof of stake consensus process.

There is a lot of literature on blockchain from various sources, such as blogs, wikis, forum posts, codes, conference proceedings and journal articles. Tschorsch et al. (2016), made a technical survey about decentralized digital currencies including Bitcoin. Compared to Zhang and Wen (2015), the paper focuses on blockchain technology instead of digital currencies. Nomura Research Institute made a technical report about blockchain. This paper focuses on state-of-art blockchain researches including recent advances and future trends.

**BLOCKCHAIN ARCHITECTURE**

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger. With a previous block hash contained in the block header, a block has only one parent block. It is worth noting that uncle blocks (children of the block’s ancestors) hashes would also be stored in Ethereum blockchain. The first block of a blockchain is called genesis block which has no parent block. We then explain the internals of blockchain in details (Noyes, 2016).

## Block

A block consists of the block header and the block body. The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions. Digital signature based on asymmetric cryptography is used in an untrustworthy environment. We next briefly illustrate digital signature (Noyes, 2016).

## 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 Alice wants to send another user Bob a message. (1) In the signing phase, Alice encrypts her data with her private key and sends Bob the encrypted result and original data. (2) In the verification phase, Bob validates the value with Alice’s public key. In that way, Bob 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) (Zhang & Wen, 2016).

## Key Characteristics of Blockchain

In summary, 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.

**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.

**Anonymity**. Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user. 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.

**Taxonomy of blockchain systems**

Current blockchain systems are categorized roughly into three types: public blockchain, private blockchain and consortium blockchain (Tschorsch et al., 2016). In public blockchain, all records are visible to the public and everyone could take part in the consensus process. Differently, only a group of pre-selected nodes would participate in the consensus process of a consortium blockchain. As for private blockchain, only those nodes that come from one specific organization would be allowed to join the consensus process.

A private blockchain is regarded as a centralized network since it is fully controlled by one organization. The consortium blockchain constructed by several organizations is partially decentralized since only a small portion of nodes would be selected to determine the consensus. The comparison among the three types of blockchains.

**Consensus determination**. In public blockchain, each node could take part in the consensus process. And only a selected set of nodes are responsible for validating the block in consortium blockchain. As for private chain, it is fully controlled by one organization and the organization could determine the final consensus.

**Read permission**. Transactions in a public blockchain are visible to the public while it depends when it comes to a private blockchain or a consortium blockchain.

**Immutability**. Since records are stored on a large number of participants, it is nearly impossible to tamper transactions in a public blockchain. Differently, transactions in a private blockchain or a consortium blockchain could be tampered easily as there are only limited number of participants.

**Efficiency**. It takes plenty of time to propagate transactions and blocks as there are a large number of nodes on public blockchain network. As a result, transaction throughput is limited and the latency is high. With fewer validators, consortium blockchain and private blockchain could be more efficient.

**Centralized**. The main difference among the three types of blockchains is that public blockchain is decentralized, consortium blockchain is partially centralized and private blockchain is fully centralized as it is controlled by a single group.

**Consensus process**. Everyone in the world could join the consensus process of the public blockchain. Different from public blockchain, both consortium blockchain and private blockchain are permissioned.

Since public blockchain is open to the world, it can attract many users and communities are active. Many public blockchains emerge day by day. As for consortium blockchain, it could be applied into many business applications (Noyes, 2016).

# **CHALLENGES & RECENT ADVANCES**

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.

**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:** Since it is harder for node to operate full copy of ledger, Bruce proposed a novel cryptocurrency scheme, in which the old transaction records are removed (or forgotten) by the network. A database named account tree is used to hold the balance of all non-empty addresses. Besides lightweight client could also help fix this problem.

**Redesigning blockchain:** Bitcoin-NG (Next Generation) was proposed. The main idea of Bitcoin-NG is to decouple conventional block into two parts: key block for leader election and microblock to store transactions. The protocol divides time into epoches. In each epoch, miners have to hash to generate a key block. Once the key block is generated, the node becomes the leader who is responsible for generating microblocks. Bitcoin-NG also extended the heaviest (longest) chain strategy in which microblocks carry no weight. In this way, blockchain is redesigned and the tradeoff between block size and network security has been addressed (Sharples & Domingue, 2015).

**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, 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 has shown that a user’s Bitcoin transactions can be linked to reveal user’s information. Moreover, Biryukov et al. (2014) 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.

**Anonymous**. Miners do not have to validate a transaction with digital signature but to validate coins belong to a list of valid coins. Payment’s origin are unlinked from transactions to prevent transaction graph analyses. But it still reveals payments’ destination and amounts. Transaction amounts and the values of coins held by users are hidden.

**Selfish Mining**

Blockchain is susceptible to attacks of colluding selfish miners. In particular, Eyal and Sirer (2014), 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, 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. Yet in some cases, it can result in 13% gains in comparison with a non-trail-stubborn counterpart. A study by Zhang and Wen (2015) shows that there are selfish mining strategies that earn more money and are profitable for smaller miners compared to simple selfish mining. But the gains are relatively small. Furthermore, it shows that attackers with less than 25% of the computational resources can still gain from selfish mining.

# **CONCLUSION**

Blockchain has shown its potential for transforming traditional industry with its key characteristics: decentralization, persistency, anonymity and auditability. In this paper, we present a comprehensive overview on blockchain. The seminar paper first gave an overview of blockchain technologies including blockchain architecture and key characteristics of blockchain. It also discusses the typical consensus algorithms used in blockchain.

**RECOMMENDATIONS**

1. Blockchain based applications are springing up, it is therefore recommended that there be an in-depth investigation on blockchain-based applications in the future.
2. It is also recommended that the use of blockchain technology be more emphasized and explain even to the common man for easy understanding and usage.

**REFERENCES**

Akins, J. & Gordon, M. (2013). The elliptic curve digital signature algorithm (ecdsa). *International Journal of Information Security*, 1(1), 36–63.

Biryukov, D., Khovratovich, I. & Pustogarov, I. (2014). Deanonymisation of clients in bitcoin p2p network. *International Journal on Computer and Communications Security*, 3(4), 15–29.

Eyal, I. & Sirer, G. (2014). Majority is not enough: Bitcoin mining is vulnerable,” in *Proceedings of International Conference on Financial Cryptography and Data Security*, 4(2), 436– 454.

Kosba, A. (2017). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *Journal of information Technology on Security and Privacy (SP)*, 3(9), 839–858.

Noyes, J. (2016). Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning. *International Journal on Financial Cryptography and Data Security*, 8(6), 486–504.

Sharples, J. & Domingue, O. (2015). The blockchain and kudos: A distributed system for educational record, reputation and reward. *International Journal* *on Technology Enhanced Learning, 5(2)*, 490–496.

Tschorsch, F. & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies,” *Journal of Electrical Electronics Communications Surveys Tutorials*, 8(3), 2084–2123.

Zhang, J. & Wen, J. (2015). An iot electric business model based on the protocol of bitcoin. *International Journal on Intelligence in Next Generation Networks,* 2(5), 184–191.