CHALLENGES AND OPPORTUNITIES IN BLOCKCHAIN: A REVIEW

Ranjitha.S

Student, Department of BCA, Indus Valley Degree College, Bangalore

Abstract: Block chain has numerous benefits such as decentralisation, persistency, anonymity and audit ability. There is a wide spectrum of block chain applications ranging from crypto currency, financial services, risk management, internet of things (IoT) to public and social services. Although a number of studies focus on using the block chain technology in various application aspects, there is no comprehensive survey on the block chain technology in both technological and application perspectives. To fill this gap, we conduct a comprehensive survey on the block chain technology. In particular, this paper gives the block chain taxonomy, introduces typical block chain consensus algorithms, reviews block chain applications and discusses technical challenges as well as recent advances in tackling the challenges. Moreover, this paper also points out the future directions in the block chain technology.

Keywords: Block chain; IoT; internet of things; consensus algorithms; crypto currency; smart contract.

1. Introduction

Recently, crypto currency has attracted extensive attentions from both industry and academia. Bitcoin that is often called the first crypto currency has enjoyed a huge success with the capital market reaching 10 billion dollars in 2016 (coin desk, 2016). The block chain is the core mechanism for the Bitcoin. Block chain could be regarded as a public ledger, in which all committed transactions are stored in a chain of blocks. This chain continuously grows when new blocks are appended to it. The block chain technology has the key characteristics, such as decentralisation, persistency, anonymity and audit ability. Block chain can work in a decentralised environment, which is enabled by integrating several core technologies such as cryptographic hash, digital signature (based on asymmetric cryptography) and distributed consensus mechanism. With block chain technology, a transaction can take place in a decentralised fashion. As a result, block chain can greatly save the cost and improve the efficiency.

2. Block chain Architecture

The block chain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger. Each block points to the immediately previous block via a reference that is essentially a hash value of the previous block called parent block.

➢ Block

A block consists of the block header and the block. In particular, the block header includes:

- Block version: indicates which set of block validation rules to follow.
- Parent block hash: a 256-bit hash value that points to the previous block.
- Merkle tree root hash: the hash value of all the transactions in the block.

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.

➢ Digital Signature

Each user owns a pair of private key and public key. The private key is used to sign the transactions. The digital signed transactions are spread throughout the whole network and then are accessed by public keys, which are visible to everyone in the network. The typical digital signature is involved with two phases: the signing phase and the verification phase.

➢ Key characteristics of block chain

• Decentralization: In conventional centralized transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank) inevitably resulting the cost and the performance bottlenecks at the central servers.

• Persistency: Since each of the transactions spreading across the network needs to be confirmed and recorded in blocks distributed in the whole network, it is nearly impossible to tamper. Additionally, each broadcasted block would be validated by other nodes and transactions would be checked.

• Anonymity: Each user can interact with the block chain network with a generated address. Further, a user could generate many addresses to avoid identity exposure. There is no longer any central party keeping users' private information. This mechanism preserves a certain amount of privacy on the transactions included in the block chain.

➢ **Taxonomy of blockchain systems**

Current blockchain systems can be roughly categorized into three types: public block chain, private blockchain and consortium blocks.

• Consensus determination: In public block chain, 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 who could determine the final consensus.

• Read permission: Transactions in a public blockchain are visible to the public while the read permission depends on a private blockchain or a consortium blockchain. The consortium or the organization could decide whether the stored information is public or restricted.

• Immutability: Since transactions are stored in different nodes in the distributed network, so it is nearly impossible to tamper the public blockchain. However, if the majority of the consortium or the dominant organization wants to tamper the blockchain, the consortium blockchain or private blockchain could be reversed or tampered.

• 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.

3. Consensus algorithms

In blockchain, how to reach consensus among the untrustworthy nodes is a transformation of the Byzantine Generals (BG) Problem (Lamport et al., 1982). In BG problem, a group of generals who command a portion of Byzantine army circle the city. The attack would fail if only part of the generals attack the city. Generals need to communicate to reach an agreement on whether attack or not. However, there might be traitors in generals. The traitor could send different decisions to different generals. This is a trust less environment.

➢ **Approaches to consensus**

Proof of work (PoW) is a consensus strategy used in Bitcoin network (Nakamoto, 2008). POW requires a complicated computational process in the authentication. In POW, each node of the network is calculating a hash value of the constantly changing block header. The consensus requires that the calculated value must be equal to or smaller than a certain given value. Transactions in the new block would be validated in case of frauds.

Proof of stake (Pops) is an energy-saving alternative to POW. Instead of demanding users to find a nonce in an unlimited space, POS requires people to prove the ownership of the amount of currency because it is believed that people with more currencies would be less likely to attack the network. Since the selection based on account balance is quite unfair because the single richest person is bound to be dominant in the network.

4. Applications of blockchain

❖ Finance

❖ Enterprise transformation.

❖ P2P financial market

❖ Risk management

• **Finance**

Financial services: The emergency of blockchain systems such as Bitcoin (Nakamoto, 2008) and (hyperledger, 2015) has brought a huge impact on traditional financial and business services. Peters et al. (Peters and Panayi, 2015) discussed that blockchain has the potential to disrupt the world of banking. Blockchain technology could be applied to many areas including clearing and settlement of financial assets etc.

- **Enterprise transformation**: In addition to the evolution of financial and business services, blockchain can help traditional organizations to complete the enterprise transformation smoothly. Consider an example of postal operators (POs). Since traditional postal operators (POs) act as a simple intermediary between merchants and customers, blockchain and crypto currency technology can help POs to extend their simple roles with the provision of new financial and un-financial services. In Jag et al. (2016), Jag and Bach explored opportunities of arising blockchain technology for POs and claimed that each PO could issue their own post coin which is a kind of collared coin of Bit coin.

- **P2P financial market**: Blockchain could also help build a P2P financial market in a secure and reliable way. Noyes explored ways of combining peer-to-peer 364 Z. Blockchain-based MPC market allows offloading computational tasks onto a network of anonymous peer-processors.

- **Risk management**: Risk management framework plays a significant role in financial technology (FinTech) and now it can be combined with blockchain to perform better. Pilkington (Pilkington, 2016) provided a novel risk-management framework, in which blockchain technology is used to analyze investment risk in the Luxembourgish scenario. Investors who nowadays hold securities through chains of custodians tend to face the risk of any of these failings.

➢ **Public and social services**

Blockchain can also be widely used in public and social services.

• Land registration. One of the typical blockchain applications in public services is the land registration (NRI, 2015), in which the land information such as the physical status and related rights can be registered and publicized on blockchains.

• Education. Blockchain is originally devised to enable currency transactions to be carried out in trust less environment.

However, if we regard the learning and teaching process as the currency, blockchain technology can potentially be applied to the online educational market. in Devine (2015), blockchain learning was proposed. In blockchain learning, blocks could be packed and placed into blockchain by teachers and the learning achievements could be thought as coins.

• Free-speech right. Moreover, blockchain can be used to secure internet infrastructure such as DNS and identities. For example, Name coin (name coin, 2014) is an experimental open-source technology that improves decentralization, security, censorship resistance, privacy, and speed. It protects free-speech rights online by making the web more resistant to censorship.

➢ **Reputation system**

Reputation is an important measure on how much the community trusts you. The greater your reputation, the more trustworthy you are regarded by others. The reputation of a person can be evaluated on his or her previous transactions and interactions with the community. There is a rising number of cases of personal reputation records falsification. For example, in e-commerce, many service-providers enrol a huge number of fake customers to achieve a high reputation. Blockchain can potentially solve this problem.

➢ **Security and privacy**

• Security enhancement. We have seen the proliferation of various mobile devices and various mobile services, which are also exhibiting their vulnerability to malicious nodes. There are a number of anti-malware filters proposed to detect the suspected files through pattern matching schemes, which a central server to store and update the virus patterns. However, these centralised countermeasures are also vulnerable to malicious attackers. Blockchain can potentially help to improve the security of distributed networks. In particular, Charles (Noyes, 2016a) proposed a novel anti-malware environment named BitAV, in which users can distribute the virus patterns on blockchain. Blockchain technologies can also be used to improve the reliability of security infrastructure. For example, conventional public key infrastructures (PKIs) are often susceptible to single point of failure due to the hardware and software flaws or malicious attacks.

As shown in Axon (2015), blockchain can be used to construct a privacy-aware PKI while simultaneously improving the reliability of conventional PKIs.

• Privacy protection. In addition to the increasing risk of the exposure of our private data to malwares, various mobile services and social network providers are collecting our sensitive data.

propose a decentralised personal data management system that ensures the user ownership of their data. This system is implemented on the blockchain. The system can protect the data against these privacy issues:

• data ownership

• data transparency and audit ability

• fine-grained access control.

5. Challenges and recent advances

As an emerging technology, blockchain is facing multiple challenges and problems. We summarise three typical challenges: scalability, privacy leakage and selfish mining.

➢ **Scalability**

With the amount of transactions increasing day by day, the blockchain becomes heavy. Currently, Bitcoin blockchain has exceeded 100 GB storage. All transactions have to be stored for validating the transaction. However, large block size would slow down the propagation speed and lead to blockchain branches. So scalability problem is quite tough. There are a number of efforts proposed to address the scalability problem of the blockchain, which could be categorized into two types:

➢ **Privacy leakage**

The blockchain is believed to be very safe as users only make transactions with generated addresses rather than real identity. Users also could generate many addresses in case of information leakage. Multiple methods have been proposed to improve anonymity of blockchain, which could be roughly categorized into two types:

• In blockchain, users addresses are pseudonymous. But it is still possible to link addresses to user real identity as many users make transactions with the same address frequently.

Mixing service is a kind of service which provides anonymity by transferring funds from multiple input addresses to multiple output addresses. Anonymous, a zero-knowledge proof is used. 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 is unlinked from transactions to prevent transaction graph analyses.

➢ **Selfish mining**

The blockchain is susceptible to attacks of colluding selfish miners. Generally, it is convinced that nodes with over 51% computing power could reverse the blockchain and reverse the happened transaction. 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 publication, honest miners are wasting their resources on a useless branch while selfish miners are mining their private chain without competitors.

➢ **Possible future directions**

The blockchain has shown its potential in industry and academia. We discuss possible future directions with respect to five areas: blockchain testing, stop the tendency to centralization, big data analytics, smart contract and artificial intelligence.

➢ **Blockchain testing**

Recently different kinds of blockchains appear and over 700 crypto currencies are listed in coin desk (2017) up to now. However, some developers might falsify their block chain performance to attract investors driven by the huge profit.

Besides, when users want to combine block chain into business, they have to know which block chain fits their requirements. So block chain testing mechanism needs to be in place to test different block chains. Block chain testing could be separated into two phases: standardization phase and testing phase.

➢ **Stop the tendency to centralization**

Blockchain is designed as a decentralized system. However, there is a trend that miners are centralized in the mining pool. Up to now, the top 5 mining pools together owns larger than 51% of the total hash power in the Bitcoin network (bitcoin worldwide, n.d.). Apart from that, selfish mining strategy (Eyal and Sirer, 2014) showed that pools with over 25% of total computing power could get more revenue than a fair share.

Rational miners would be attracted into the selfish pool and finally, the pool could easily exceed 51% of the total power. As the blockchain is not intended to serve a few organizations, some methods should be proposed to solve this problem.

- **Big data analytics**

Blockchain could be well combined with big data. Here we roughly categorized the combination into two types: data management and data analytics. As for data management, block chain could be used to store important data as it is distributed and secure. Block chain could also ensure the data is original. For example, if block chain is used to store patients' health information, the information could not be tampered and it is hard to steal that private information. When it comes to data analytics, transactions on block chain could be used for big data analytics.

- **Artificial intelligence**

Recent developments in blockchain technology are creating new opportunities for artificial intelligence (AI) applications (Omohundro, 2014). AI technologies could help solve many block chain challenges. For instance, there is always an oracle who is responsible for determining whether the contract condition is satisfied. Generally, this oracle is a trusted third party. AI technique may help build an intelligent oracle. It is not controlled by any party, it just learns from the outside and train itself. In that way, there would be no argues in he smart contract and the smart contract can become smarter. On the other hand, AI is penetrating into our lives now. Block chain and smart contract could help to restrict misbehaviors done by AI products. For instance, laws written in smart contract could help to restrict misbehaviors done by driverless cars.

6. Conclusion

The blockchain is highly appraised and endorsed for its decentralized infrastructure and peer-to-peer nature. However, many researches about the block chain are shielded by Bit coin. But block chain could be applied to a variety of fields far beyond Bit coin. Block chain has shown its potential for transforming the traditional industry with its key characteristics: decentralization, persistency, anonymity and audit ability. In this paper, we present a comprehensive survey on the blockchain. We first give an overview of the block chain technologies including block chain architecture and key characteristics of the block chain. We then discuss the typical consensus algorithms used in the block chain. We analyze and compare these protocols in different respects. We also investigate typical block chain applications.

References

1.Akins, B.W., Chapman, J.L. and Gordon, J.M. (2013) A Whole New World: Income Tax Considerations of the Bitcoin Economy.

2.antshares (2016) Antshares Digital Assets for Everyone, https://www.antshares.org. Atzori, L., Iera, A. and Morabito, G. (2010) 'The internet of things: a survey', Computer Networks, Vol. 54, No. 15, pp.2787–2805.

3.Billah, S. (2015) One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner.