An Overview of Bitcoin and Blockchain Technology

Dingchang Yang

Abstract

With the revolution brought by Bitcoin to the field of digital currency, blockchain, the core mechanism of Bitcoin, has distinct advantages for its decentralization, anonymity, and immutability. Nowadays, a wide range of blockchain applications has grown up and covered various fields including cryptocurrency, financial services, and Internet of Things. However, the blockchain technology is still facing potential challenges such as scalability and security problems. Here we present a comprehensive overview of blockchain technology. This paper starts by introducing the Bitcoin mechanism and the blockchain architecture. From there we compare several typical consensus algorithms used in different blockchains. Furthermore, we discuss some technical challenges and recent advances to solve these challenges.

Keywords: blockchain, bitcoin, cryptocurrency

An Overview of Bitcoin and Blockchain Technology

I. Introduction

In recent years, the Internet has witnessed the advent of many applications, such as BitTorrent and Gnutella, that solves problems in a distributed way. Bitcoin, the first decentralized cryptocurrency, has achieved a huge success by establishing a billion dollar economy. Its core mechanism, blockchain, was first proposed in 2008 by Satoshi Nakamoto and implemented in 2009. Blockchain could be interpreted as a public ledger, in which each block records previous committed transactions. Compared to centralized digital currencies, the blockchain technology has numerous advantages such as decentralisation, immutability, and anonymity (Maroufi et al, 2019). With the blockchain technology, each transaction can be processed in a decentralized way and stored distributedly. As a result, blockchain can tremendously save the cost and improve overall efficiency.

The rest of this paper is organized as follows. Section II introduces Bitcoin mechanism and the blockchain architecture. Section III shows how the blockchain reaches consensus and different consensus algorithms used in the blockchain. Section IV discusses some potential challenges and possible solutions and Section V concludes the paper.

II. Bitcoin and Blockchain

Assume Alice want to transfer a digital coin to Bob. In order to do so, she could sign a contract saying “Alice has transferred one coin to Bob” and announce it to the public. This contract is considered a signed contract and can be verified by using Alice’s Public key. However, digital signature cannot prevent forged transactions: Alice could *double spend* her coin by sending the same signature to another person before she broadcast this transaction, and Bob

could steal coins from Alice's account by *replaying* the same contract. Obviously, we could solve these ambiguities by assigning serial numbers to these transactions, but we also need a trusted system to issue the serials. In a centralized way, a bank is the system we all trust that issues coins with unique serial numbers and maintains a record of ownership and transactions of every coin.

To get rid of the central bank, Bitcoin assumes that everyone is the bank. Every Bitcoin user keeps a copy of the ledger of all ownership and transactions. In Bitcoin, the blockchain takes the role of this distributed ledger (Nakamoto, 2008). Blockchain is a sequence of blocks which consist of a block header and a block body. Each block only has one parent block with its hash recorded in the block header. The first block of a blockchain is called genesis block and has no parent 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. In this way, all the data are connected in a linked list structure. It is nearly impossible to retract a transaction once it is accepted and therefore ensures the immutability of the blockchain.

The blockchain is safeguarded by hashing and digital signatures from corruption and compromise. Hashing provides a way for everyone on the blockchain to agree on the current world state, while digital signatures provide a way to ensure that all transactions are only made by the rightful owners (Ozercan et al, 2018). Each user owns a pair of private key and public key. The private key is used to sign the transactions, while the public key is available for every user in the blockchain. These digital signed transactions are spread throughout the whole network and then are accessed by senders' public keys. The typical digital signature is involved

with two phases: the signing phase and the verification phase (Johnson, Menezes & Vanstone S, 2001). To sign a transaction, a hash value is first generated from the transaction then encryption of this hash value by using senders' private key and sends the encrypted hash with the original data to the receiver. The receiver verifies the received transaction through the comparison between the decrypted hash by using senders' public key and the hash value derived from the received data by the same hash function as the sender. Additionally, users interact with the blockchain network through hashed addresses, which prevents identity disclosure and also ensures their anonymity on the transactions.

III. Consensus

In blockchain, how every node reaches consensus can be interpreted as a Byzantine Generals Problem. In this problem, a group of generals who command a portion of Byzantine army circle the city. Some generals prefer to attack while other generals prefer to retreat. However, the attack would fail if only part of the generals attack the city. Thus, they have to reach a consensus to attack or retreat. How to reach a consensus in distributed system is a challenge. In blockchain, there is no central node that tells ledgers on distributed nodes to coordinate with it. Distributed storage of multiple copies of the block chain opens up new possibilities for cheating. A typical Sybil attack could subvert the whole network by gaining 51% computations of the system. We next discuss several common approaches to reach consensus in blockchain.

Prove of Work

Prove of Work (PoW) is the consensus strategy used in the Bitcoin. In a decentralized network, someone has to be selected to record the transactions. The easiest way is random

selection, which is vulnerable to attack. In Bitcoin network, if a node wants to publish a block of transactions, a lot of work has to be done to prove that the node is not likely to attack the network (Nakamoto, 2008). In PoW, each node of the network is calculating a hash value of the block header. Nodes that calculate the hash values are called miners and the calculation of this specific hash value is called mining in Bitcoin. The block header contains a nonce and miners would try different nonce frequently to get different hash values. The consensus requires that the calculated value must be equal to or smaller than a certain given value. When one node reaches the target value, it would broadcast the block to other nodes and all other nodes must mutually confirm the correctness of the hash value. If the block is validated, other miners would append this new block to their own blockchains and the founder of this block would be awarded for a certain amount of Bitcoins plus the transaction fees recorded in the discovered block.

Prove of Stake

Prove of stake (PoS) is an energy-saving alternative to PoW and is based on the belief that people with more currencies would be less likely to attack the network. Miners in PoS have to prove the ownership of the amount of currency. This selection based on account balance is often considered unfair because the richest person is guaranteed to be dominant in the network. As a result, many solutions are proposed with the combination of the stake size to decide which node to publish the next block. Compared to PoW, PoS saves more computational energy for miners and is more effective. Unfortunately, as the mining cost is nearly zero, attacks might come as a consequence. Therefore, some blockchains tend to adopt PoW at the beginning and gradually transform to PoS. An example would be Ethereum, which switched from Ethash, a PoW based protocol, to Casper, a PoS based protocol (Caubet, 2018).

IV. Challenges

Nowadays, emerging blockchain-based applications are being implemented in a wide range of industries. Despite its great potential and advantages, blockchain still faces numerous challenges that limit its wide usage. Some of the major challenges and their recent advances are listed as follows.

Scalability

With daily increasing amount of transactions, the blockchain grows longer and longer. Even though its protocol limits new block being discovered at an interval of every ten minutes, Bitcoin has still experienced slowed transaction speeds and higher fees charged per transaction as a result of a substantial increase in users (Catalini & Gans, 2016). 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 blockchain of Bitcoin can only process around seven 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 transactions with higher transaction fee.

The current version of Bitcoin solves this problem by introducing *Storage optimization of blockchain* (Bruce, 2014). Since it is harder for nodes to operate on the full copy of ledger, Bruce proposed a new cryptocurrency scheme called account tree, in which the old transaction records are removed by the network. The idea of account tree is that everyone keeps a ledger of other people's remaining balance. Since these numbers are the result of previous transactions, old records are no longer needed to be stored in the client. Account tree allows lightweight

clients to outsource expensive computations over large inputs and ensures the computation result is correct by comparing results from multiple servers.

Selfish Mining

As we mentioned before, blockchain is susceptible to attacks of Sybil Attack. In small PoW based networks, attackers can easily gain 51% of their computing power and take over the system. Eyal and Sirer showed that the network is vulnerable even if only a small portion of the hashing power is used to cheat (2018). In selfish mining strategy, selfish miners keep their mined blocks without broadcasting. When the private branch is longer than the current public chain, it would be admitted by all other miners. Before the private blockchain publishment, honest miners are wasting their resources on a useless branch while selfish miners are mining their private chain without competitors. As a result, selfish miners tend to get more revenue than honest miners.

V. Conclusion

Blockchain has been highly appraised for its decentralized structure and peer-to-peer design. Although many researches and usage of the blockchain in real world are limited to cryptocurrency and financial services, blockchain has shown its potential far beyond Bitcoin with its advantages: decentralization, immutability, and anonymity. However, as a relatively new technology, blockchain is still facing several challenges that could potentially undermine the whole system.These challenges must be fully examined and mitigated before it could be widely applied to other fields.

References

Bruce, J. D. (2014). The mini-blockchain scheme. *White paper*.

Catalini, C., & Gans, J. S. (2016). Some simple economics of the blockchain(No. w22952). *National Bureau of Economic Research*.

Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM,* 61(7), 95-102.

Fernàndez-València, R., Caubet, J., & Vila, A. (2018). "Introduction to Blockchain Technology. *Cryptography Working Group.*

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

Maroufi, M., Abdolee, R., & Tazekand, B. M. (2019). On the Convergence of Blockchain and Internet of Things (IoT) Technologies. *arXiv preprint arXiv:1904.01936.*

Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. (2008).

Ozercan, H. I., Ileri, A. M., Ayday, E., & Alkan, C. (2018). Realizing the potential of blockchain technologies in genomics. *Genome research, 28(9), 1255-1263*.