IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends

Sarthak Yogesh Dokhe[1] and Sushma Laxman Wakchaure[2]
Student, Department of Computer Technology[1]
Lecturer, Department of Computer Technology[2]
Amrutvahini Polytechnic, Sangamner, Maharashtra, India

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 algorithmsused in different blockchains. Furthermore, technical challenges and recent advances are briefly listed. We also lay out possible future trends for blockchain.*

Keywords: Blockchain, decentralization, consensus, scalability

I. INTRODUCTION

Nowadays cryptocurrency has become a buzzword inboth industry and academia. As one of the most successful cryp-tocurrency, Bitcoin has enjoyed a huge success with its capital market reaching 10 billion dollars in 2016 [1]. With a spe- cially designeddata storage structure, transactions in Bitcoin networkcould happen without any third party and the core technology to build Bitcoin is blockchain, which was first proposed in 2008 and implemented in 2009 [2]. 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 appendedto it continuously. Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency. The blockchain technology generally has key characteristics ofdecentralization, 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 [3], [4]. Additionally, it can also be applied into other fields including smartcontracts [5], public services [6], Internet of

Things (IoT) [7], reputation systems [8] and security services [9]. Those fields favor blockchain in multipleways. First of all, blockchain is immutable. Transaction cannot be tampered onceit is packed into the blockchain. Businesses that require high reliabilityand 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 onthe blockchain.

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 whilea 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 [10]. 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 thisproblem. Moreover, it has been shown that privacy leakage could also happen in blockchain even users only make transactions with their public key

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

and private key [11]. 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, confer- ence proceedings and journal articles. Tschorsch et al. [12] made a technical survey about decentralized digital currencies including Bitcoin. Compared to [12], our paper focuses on blockchain technology instead of digital currencies. Nomura Research Institut made a technical report about blockchain [13]. Contrast to [13], our paper focuses on state-of-art blockchain researches including recent advances and future trends.

The rest of this paper is organized as follows. Section introduces blockchain architecture. Section III shows typical consensus algorithms used in blockchain. Section IV summa- rizes the technical challenges andthe recent advances in this area. Section V discusses some possible future directions and section VI concludes the paper.

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger [14]. Figure 1 illustrates an example of ablockchain. Witha 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 storedin ethereum blockchain [15]. The first block of a blockchain is called genesis block which has no parentblock. We then explain the internals of blockchain in details.

Block

A block consists of the block header and the block body asshown in Figure 2. In particular, the block header includes:

Block version: indicates which set of block validation rules to follow.Merkle tree root hash: the hash value of all the transac- tions in the block.

Timestamp: current time as seconds in universal timesince January 1, 1970.

II. BLOCKCHAIN ARCHITECTURE

Bits: target threshold of a valid block hash.

Nonce: an 4-byte field, which usually starts with 0 and increases for every hash calculation (will be explained in details in Section III).

Parent block hash: a 256-bit hash value that points to the previous 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. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions [13]. Digital signature based on asymmetric cryptography is used in an untrustworthy environment. We next brieflyillustrate digital signature.

Digital Signatur

Each user owns a pair of private key and public key. The private key that shall be kept in confidentiality is usedto sign the transactions. The digital signed transactions are broadcasted throughout the whole network. The typical digitalsignature is involved withtwo phases: signing phasend 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 sendsBob the encrypted result and original data. (2) In the verification phase,Bob validates the value with verification phase. For instance, an user Alice wants tosend another user Bob a message. (1) In the signing phase, Alice encrypts her data with her private key andsends 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) [16].

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), in- evitably resulting to the cost and the performance bottle- necks 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

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

Persistency. Transactions can be validated quickly andinvalid 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 discov- ered immediately.

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 (details willbe discussed in section IV).

Auditability. Bitcoin blockchain stores data about user balances based on the Unspent Transaction Output (UTX- O) model [2]: Any transaction has to refer to some previ- ous unspent transactions. Once the currenttransaction is recorded into the blockchain, the state ofthose referred unspent transactions switch fromunspent 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 con- sortium blockchain [17]. In public blockchain, all records are visible to the public and everyone could take part in the con- sensus 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 wouldbe allowed to jointhe consensus process.

Efficiency. It takes plenty of time to propagate transac- tions and blocks as there are a large number of nodeson 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.

Characteristics	Public Blockchain	Private Blockchain	Consortium Blockchain
Permission Read	Public Class	Could be public or restricted	May be public or restricted
Determination of Consensus	All miners	Only one organization	Designated set of nodes
Efficiency	Low	High	High
Immutability	Impossible to tamper	Could be tampered	Could be tampered
Centralized	No	Yes	Partial
Consensus	Permissionless	Permissioned	Permissioned

Comparisons among public blockchain, consortium blockchain andprivate blockchain

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

Consensus process. Everyone in the worldcould 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 at- tract 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. Currently Hyperledger [18] isdeveloping business consortiumblockchain frameworks. Ethereum also has provided tools forbuilding consortium blockchains [19].

CONSENSUS ALGORITHMS

In blockchain, how to reach consensus among the untrust- worthy nodes is a transformation of the Byzantine Generals (BG) Problem, which was raised in [20]. In BG problem,a group of generals who commands a portion of Byzantine

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

army circle the city.Some generals prefer to attack while other generals prefer to retreat. However, the attack wouldfail if only part of the generals attack the city. Thus, theyhave to reach an agreement to attack or retreat. How to reach a consensus in distributed environment is a challenge. It is also a challenge for blockchainas the blockchain network is distributed. In blockchain, there is no central node that ensures ledgers on distributed nodes are all the same. Some protocols are needed to ensure ledgers in different nodes are consistent. We next present several commonapproaches to reach a consensus in blockchain.

Approaches to consensus

PoW (Proof of work) is a consensus strategy used in the Bitcoin network [2]. In a decentralized network, someone has to be selected to record the transactions.The easiest way is random selection. However, random selection is vulnerable to attacks. So if a nodewants to publish a block of transactions, alot of work has to be done to prove that the node is not likely to attack the network. Generally the work meanscomputer calculations. In PoW, each node of the network is calculating a hash value of the block header. The block header contains a nonce and miners would change the nonce frequently toget different hash values. The consensus requires that the calculated be value must equal to or smaller than a certain givenvalue. 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. Nodes that calculate the hash values are called miners and the PoW procedure is called miningin Bitcoin.

In the decentralized network, valid blocks might be gen- erated simultaneously when multiple nodes find the suitable nonce nearly at the same time. As a result,branches may be generated as shown in Figure 3. However, it is unlikely that two competing forks will generate next block simultaneously. In PoW protocol,a chain that becomes longer thereafter is judged as theauthentic one. Consider two forks created by simultaneously validated blocks U4 and B4. Miners keep mining their blocks until a longer branch isfound. B4,B5 forms a longer chain, so the miners on U4 would switch tothe longer branch.

Miners have to do a lot of computer calculations in PoW, yet these works waste too much resources. To mitigate the loss, some PoW protocols in which works could have some side-applications have been designed. For example, Primecoin[25] searches for special prime number chains which can beused for mathematical research.to PoW. Miners in PoS have toprove the ownership of the amountof currency. It is believed that people with more currencies would be less likely to attack the network. The selection based on account balance is quite unfair because the single richest person is bound to be dominant in the network.As a result, many solutions are proposed withthe
combination of the stake size to decide which oneto forge the next block.In particular, Blackcoin[26]usesPoS (Proof of stake) is an energy-saving alternativerandomization to predict thenext generator. It uses a formula that looks for the lowest hash value in combination with the size of the stake. Peercoin[21] favors coin age based selection. In Peercoin, older andlarger sets of coins have a greater probability of mining the next block. Compared to PoW, PoS saves more energy andis more effective. Unfortunately, as the mining cost is nearly.For instance, ethereum is planing to move from Ethash (a kind of PoW)[27] to Casper (a kind of PoS) [28].

PBFT (Practical byzantine fault tolerance) is a replication algorithm to tolerate byzantine faults [29]. Hyperledger Fabric[18] utilizes the PBFT as its consensus algorithm since PBFT could handle up to 1/3 malicious byzantine replicas. A new block is determined in a round. In each round, a primary wouldbe selected according to some rules. And it is responsible for ordering the transaction. The whole process could be divided into three phase: pre- prepared, prepared and commit. In eachphase, a node would. Like PBFT, Stellar Consensus Protocol (SCP) [30] is also a Byzantine agreement protocol. In PBFT, each node has to query other nodes while SCP gives participants the right tochoose which set of other participants to believe. Based on PBFT, Antshares [31] has implemented their dBFT (delegated byzantine fault tolerance). In dBFT, some professional nodes are voted to record the transactions DPOS (Delegated proof of stake). The major difference between PoS andDPOS is that PoS is direct democratic while DPOS is representative democratic. Stakeholders elect their delegates to generate and validate blocks. With significantly fewer nodes to validate the block, the block could be confirmed quickly, leading to the quick confirmation of transactions. Meanwhile, the parameters of the network such as block size and block intervals could be tuned by delegates. Additionally, users need not to worry about the dishonest delegates as they could be voted out easily. DPOS is the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

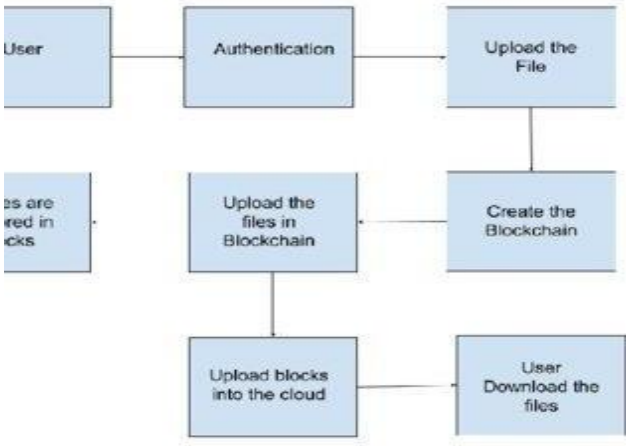
backbone of Bitshares [22].Ripple [23] is a consensusalgorithm that utilizes collectively- trusted subnetworks within the larger network. In the network, nodes are divided into two types: server for participating consensus process and client for only transferring funds. Each server has an Unique Node List (UNL). UNL is important to the server. When determining whether to put a transaction into the ledger, the server would query the nodes in UNL and if thereceived agreements have reached 80%, t

hetran saction would be packed into the ledger. For a node, the ledger will remain correct as long as the percentage of faulty nodes in UNL is less than 20%.Tendermint [24] is a byzantine consensus algorithm. A newblock is determined in a round. A proposer would be selected to broadcast an unconfirmed block in this round. It could be divided into three steps:

1) Prevote step. Validators choose whether to broadcast a prevote for the proposed block.

2) Precommit step. If the node has received more than2/3 of prevotes on the proposed block, it broadcasts aprecommit for that block. If the node has received over 2/3 of precommits, it enters the commit step.

3) Commit step. The node validates the block and broadcasts a commit for that block. if the node has received 2/3 of the commits, it accepts the block. Contrast to PBFT, nodes have to lock their coins to become validators. Once a validator is found to be dishonest, it would be punished.



An scenario of blockchain branches (the longer branch would be admitted as the main chain while the shorter one would be deserted)

B. Advances algorithms comparison

Different consensus algorithms have differentadvantages and disadvantages. Table II gives a comparison between d-different consensus algorithmsand we use the properties given by [32].

Node identity management. PBFT needs to know the identity of each miner in order to select a primary in everyround while Tendermint needs toknow the validators in order to select a proposer in each round. For PoW, PoS, DPOS and Ripple, nodes could join the network freely.

Energy saving. In PoW, miners hash the blockheader continuously to reach the target value. As a result, the amount of electricity required to process has reach an immense scale. As for PoS and DPOS, miners still have to hash the block header to search the targetvalue butthe work has been largely reduced as the search space is designed to be limited. As for PBFT, Ripple and Tendermint, there is no mining inconsensus process. So it saves energy greatly.

Tolerated power of adversary. Generally 51%of hash power is regarded as the threshold for one to gain control of the network. But selfish mining strategy [10] in PoW systems could help miners to gain more revenue by only 25% of the hashing power. PBFT and Tendermint is designed to handle up to 1/3 faulty nodes. Ripple is proved to maintain correctnessif the faulty nodes in an UNL is less than 20%.

Example. Bitcoin is based on PoW while Peercoin isa new peer-to-peer PoS cryptocurrency. Further, Hyper- ledger Fabric utilizes PBFT to reach consensus. Bitshares, a smart contract platform, adopts DPOS as their con- sensus algorithm. Ripple implements the Ripple protocol while Tendermint devises the Tendermint protocol.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

PBFT and Tendermint are permissioned protocols.Node identities are expected to be known to the whole network, so they might be used in commercial mode rather than public. PoW and PoS are suitable forpublic blockchain. Consortium or private blockchain might has preference for PBFT, Tender-mint, DPOS and Ripple.

Advances on consensus algorithms

A good consensus algorithm means efficiency, safty and convenience. Recently, a number of endeavors have been made to improve consensus algorithms in blockchain. New con- sensus algorithms are devised aiming to solve some specific problems of blockchain. The main idea of PeerCensus [33] is to decouple block creation and transaction confirmation so thatthe consensus speed can be significantly increased. Besides, Kraft [34] proposed a new consensus method to ensure thata block is generated in a relatively stable speed. It is known that high blocks generation rate compromise Bitcoin's security. So the Greedy Heaviest-Observed Sub-Tree (GHOST) chain selection rule [35] is proposed to solve this problem. Insteadof the longest branch scheme, GHOST weights the branches and miners could choose the better one to follow. Chepurnoy et al. [36] presented a new consensus algorithm for peer-to- peer blockchain systems where anyone who provides non- interactive proofs of retrievability for the past state snapshots is agreed to generate the block. In such a protocol, minersonly have to store old block headers instead offull blocks.

CHALLENGES & RECENT ADVANCES

Despite the great potential of blockchain, it facesnumerous challenges, which limit the wide usage of blockchain. We enumerate some major challenges andrecent 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 ofthe current transaction is unspent or not. Besides, dueto 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 sinceminers prefer those transactions with high transactionfee.

There are a number of efforts proposed to address thescalability problem of blockchain, which could becategorized into two types:

Storage optimization of blockchain. Since it isharder for node to operate full copy of ledger, Bruce proposed a novel cryptocurrency scheme, in which theold transactionrecords are removed (or forgotten) by the network [37].A database named account tree is used to hold the balance of all non-empty addresses. Besides lightweight client could also help fix thisproblem. A novel schem named VerSum [38] was proposed to provide another way allowing lightweightclients to exist. VerSum allows lightweight clients to outsource expensive computations over large inputs. It ensures the computation result is correct through comparing results from multiple servers.

Redesigning blockchain. In [39], Bitcoin-NG (Next Gen- eration) was proposed. The main idea of Bitcoin-NG isto 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 keyblock 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, blockchainis redesigned and the tradeoff between block size and network security has been addressed.

Privacy Leakage

Blockchain can preserve a certain amount of privacy through the public key and private key. Users transactwith their private key and public key without any realidentity exposure. However, it is shown in [40], [5] that blockchain cannot guarantee the transactional privacysince 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. [11] presented an method tolink user pseudonyms to IP addresses even when users are behind Network Address Translation (NAT) or firewalls. In [11], eachclient can be uniquely identified by a set of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

nodes it connects to. However, this set canbe learned and used to find theorigin of a transaction. Multiple methods have been proposed to improveanonymity of blockchain, which could be roughlycategorized into two types:

Mixing [42]. In blockchain, users addresses are pseudony- mous. But it is still possible to link addresses to user real identity as many users make transactions with the same address frequently. Mixingservice is a kind of service which provides anonymityby transferring funds frommultiple input addresses to multiple output addresses. For example, user Alice with address A wants to send some funds to Bob withaddress B. If Alice directly makes a transaction with input address A and output address B, relationship between Alice and Bob might be revealed. So Alice could send funds to a trusted intermediary Carol. ThenCarol transfer funds to Bob with multiple inputs c1, c2, c3, etc., and multiple output d1, d2, B, d3, etc. Bob's address B is also contained in the output addresses. So itbecomes harder to reveal relationship between Alice and Bob. However, the intermediary could be dishonest and reveal Alice and Bob's private information on purpose.It is also possible that Carol transfers Alice's funds to her own address instead of Bob's address. Mixcoin [43] provides a simple method to avoid dishonest behaviours. Anonymous. In Zerocoin [46], zero-knowledge proofis used. Miners do not have to validate a transactionwith 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.

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 thehashing power is used to cheat. Inselfish mining strategy, selfish miners keep their mined blocks without broadcasting and the private branch would be revealed to the public onlyif 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 aremining their private chain without competitors. So selfish miners tend to get more revenue.

Based on selfish mining, many other attacks have beenproposed to show that blockchain is not so secure. In stubborn mining [48], miners could amplify its gain bynon-trivially composing mining attacks with network-level eclipse attacks. The trail-stubbornness is one of the stubborn strategy that miners still mine the blockseven if the private chain is left behind. Yet in some cases, it can result in 13% gains in comparison with anon-trail-stubborn counterpart. [49] shows that there are selfish mining strategies that earn more money andare 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. To help fix the selfish mining problem, Heilman [50] presented annovel approach for honest miners to choose which branch to follow. With random beacons and timestamps, honest miners would select more fresh blocks. However, [50] is vulnerable toforgeable timestamps. ZeroBlock [51] builds on the simple scheme: Each block must be generated and accepted by the network within a maximum time interval. Within ZeroBlock, selfish miners cannot achieve morethan its expected reward.

POSSIBLE FUTURE DIRECTIONS

Blockchain has shown its potential in industry and academic

We discuss possible future directions with respect to four areas: blockchain testing, stop the tendency tocentralization, big data analytics and blockchain application.

Blockchain testing

Recently different kinds of blockchains appear and over 700 cryptocurrencies are listed in [52] up to now. However, some developers might falsify their blockchain performanceto attract investors driven by the huge profit. Besides that, when users want to combine blockchain into business, they have to knowwhich blockchain fits their requirements. So blockchain testing mechanism needs to be in place to test different blockchains.

Stop the tendency to centralization Blockchain is designed as a decentralized system. Howev,there is a trend that miners are centralized inthe mining pool. Up to now, the top 5 mining poolstogether owns larger than 51% of the total hash powerin the Bitcoin network [53]. Apart from that, selfishmining strategy [10] showed that pools with over 25% of total computing power could get more revenue thanfair share. Rational miners would be attracted into theselfish pool

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

and finally the pool could easily exceed51% of the total power. As the blockchain is notintended to serve a few organizations, some methodsshould be proposed to solve this problem.

Big data analytics

Blockchain could be well combined with big data. Here we roughly categorized the combination into twotypes: data management and data analytics. As for data management, blockchain could be used to store important data as it is distributed and secure. Blockchain could also ensure the data is original. For example, if blockchain is used to store patients healthinformation, the information could not be tampered and it is hard to stole those private information. When it comes to data analytics, transactions on blockchain could be used for big data analytics. For example, user trading patterns mightbe extracted. Users can predict their potential partners' tradingbehaviours with the analysis.

Blockchain applications

Currently most blockchains are used in the financial domain, more and more applications for different fields are appearing. Traditional industries could take blockchain into consideration and apply blockchain into their fields to enhance their systems. For example, user reputations could be stored on blockchain. At the same time, the up-and-coming industry could make use of blockchain to improve performance. For example, Arcade City [51], a ridesharing startup offers an open marketplace where riders connect directly with drivers by leveraging blockchain technology.

A smart contract is a computerized transaction protocol that executes the terms of a contract [54]. It has been proposed for long time and now this concept can be implemented with blockchain. In blockchain, smart contract is a code fragment that could be executed by miners automatically. Smart contract has transformative potential in various fields like financial services and IoT.

III. 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. We first givean overview of blockchain technologies including blockchain architecture and key characteristics of blockchain. We then dis- cuss the typical consensus algorithms used in blockchain. We analyzed and compared these protocols in different respects. Furthermore, we listed some challenges and problems that would hinder blockchain development and summarized some existing approaches for solving these problems. Some possible future directions are also proposed. Nowadays blockchain- based applications are springing up and we plan to conduct in-depth investigations on blockchain-based applications in thefuture.

ACKNOWLEDGEMENT

The work described in this paper was supported by the National Key Research and Development Program (2016YF-B1000101), the National Natural Science Foundation of China under (61472338), the Fundamental Research Funds for the Central Universities and Macao Science and Technology Development Fund under Grant No. 096/2013/A3. The authors would like to thank Gordon K.-T. Hon for his constructive comments.

REFERENCES

[1]. "State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available: http://www.coindesk.com/state-of-blockchain-q1- 2016/

[2]. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[3]. G. W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective," 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn. 2646618

[4]. Apache NiFi

[5]. Apache NiFi Documentation

[6]. GitHub Repository:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

[7]. User Mailing List:
[8]. Apache NiFi Users Mailing List
[9]. NiFi Registry Documentation:
[10]. NiFi Wiki:
[11]. Stack Overflow:
[12]. NiFi Blogs:
[13]. NiFi Processor Documentation:
[14]. [iot] Wikipedia. Internet of Things [online]. Retrieved: from: http://en.wikipedia.org/wiki/Internet_of_Things
[15]. [bigdata] Wikipedia. Big Data [online]. Retrieved:, from: http://en.wikipedia.org/wiki/Big_data