International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

Consensus Mechanisms in Blockchain Technology: A Review

Sankaliya Shraddha

Department of Computer Engineering, Ldrp-Itr sector 15, Gandhinagar, India

Abstract: ***A Blockchain is an Accessible to all, distributed ledger that can record transactions between two parties fast and scalable and in everyone check the validity of the information and permanent way. Blockchain, the foundation of Bitcoin, has received massive attentions recently. Cryptocurrencies such as Bitcoin enable users to submit payment transactions without going through centralized trusted Associations. Blockchain based applications are springing up, covering many 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 Block chain architecture firstly and consensus algorithms used in different Blockchains. And also In this paper we modify tendermint consensus algorithm.***

Keywords: Blockchain, Consensus, Tendermint

1. Introduction

a) Blockchain Architecture

A decentralized computation and information sharing platform that enables multiple parties domains, who do not trust each other, to cooperate, coridinate and collaborate in a clear decision making process.

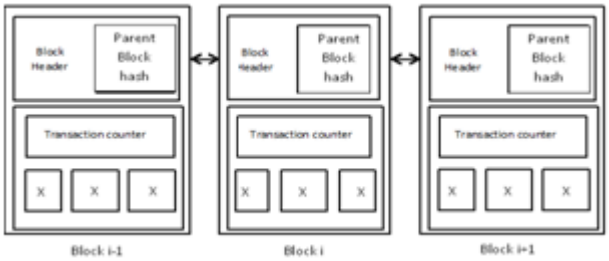


Figure 1: An example of blockchain which consists of a continuous sequence of blocks.

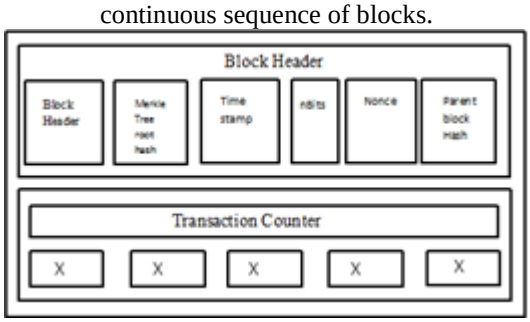


Figure 2: Block structure

Blockchain work like a public ledger.we wants to secure a number of different aspects. protocols for commitment is ensure that every valid transaction from the clients are committed and include in the Blockchain within a finite time. Consensus is secure that the local copies are consistent and updated. Security is the data needs to be tamper proof. And note that clients may act maliciously or can be compromised. The data (or transaction) belong to various clients: privacy and authenticity needs to be ensured.[1]. 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 a blockchain. 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 [15]. The first block of a blockchain is called genesis block which has no parent block. We then explain the internals of blockchain in details.

b) Block

A block consists of the *block header* and the *block body* as shown 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 transactions in the block.
- Timestamp: current time as seconds in universal time since January 1, 1970.
- nBits: target threshold of a valid block hash.
- Nonce: an 4-byte field, which usually starts with 0 and increases for every hash calculation.
- 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.

c) Background/history

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 [16]. 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 [17]. 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.

d) Applications of blockchain

Provenance tracking - tracking the origin and movement of high-value items across a supply chain, such as luxury goods, pharmaceuticals, cosmetics and electronics. 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 [18], [19]. Additionally, it can also be applied into other fields including smart contracts [20], public services [21], Internet of Things (IoT) [22], reputation systems [23] and security services [24]. Those fields favorblockchain 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.

e) Issues in blokchain

- Complexity: Blockchain technology is associated with tremendous complexity and an array of highly-specialized terms**.[3]**
- Network growth: A Blockchain's network of users is vast and constantly growing**,**which facilitates a stronger response to attacks. In case a Blockchain does not have a robust network with well distributed grid of nodes, it may not be possible to reap the full benefit of such a technology. However, there still is a risk of internal defects occurring and let us also not forget that there are physical limitations, because all the data has to be physically stored.[3]
- Risk of error: There is always a risk of error occurring, as long as the human factor is involved. In case a Blockchain serves as a database, all the incoming data has to be of high quality. If all occurring events are not originally registered with accuracy, then the trustworthiness of the stored data could be seriously in doubt. In case unreliable, incorrect information goes into the Blockchain, then unreliable, incorrect data will also go out from it.[3]
- Security flaw: Bitcoin as well as other Blockchains are associated with one considerable security flaw, which was first brought to light by Satoshi Nakamoto when the cryptocurrency was launched. The flaw, also known as a "51% attack", refers to a situation when a group of "miners" somehow take control of more than half of the Blockchain network's computing power.[3]
- Speed and cost of transactions Blockchain Bloat:during the first several years following Bitcoin's launch, transactions in this digital currency were considered as "nearly free**"**. As of now, however, transaction costs associated with Bitcoin are notable. At the end of 2016, for instance, every single transaction in Bitcoin cost approximately $0.20 and allows users to store 80 bytes of data.[3]
- Another aspect open for debates: There is also a political aspect to blockchains. Since their protocols allow for governance models digitization and since miners represent another type of incentivized governance model, public disagreements between community sectors are very likely. Such disagreements can be concentrated mostly on a topic such as Blockchain forking, or a procedure aimed to update the Blockchain protocol, in case most of the users within the network have reached a consensus to do so.[3]

f) Introduction about consensus mechanism

A consensus mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies. It is useful in record-keeping, among other things. Introduced to the world through cryptocurrencies, the technology which has been seeing increasing adoption in the mainstream financial, health, and logistics industries, to name a few achieves decentralization through consensus mechanisms built into the technology to introduce trust to traditionally trustless interactions between humans.

g) Consensus in detail

In any centralized system, like a database holding key information about driving licenses in a country, a central administrator has the authority to maintain and update the database. The task of making any updates – like adding/deleting/updating names of people who qualified for certain licenses – is performed by a central authority who remains the sole in-charge of maintaining genuine records.
Public blockchains that operate as decentralized, self-regulating systems work on a global scale without any single authority. They involve contributions from hundreds of thousands of participants who work on verification and authentication of transactions occurring on the Blockchain, and on the block mining activities.

In such a dynamically changing status of the Blockchain, these publicly shared ledgers need an efficient, fair, real-time, functional, reliable, and secure mechanism to ensure that all the transactions occurring on the network are genuine and all participants agree on a consensus on the status of the ledger. This all-important task is performed by the consensus mechanism, which is a set of rules that decides on the contributions by the various participants of the Blockchain.[4][5]

2. Related Work

a) Proof-of-Work (PoW):

PoW was the first consensus protocol to be introduced and is quite popular. It's highly scalable, making it suitable for a variety of applications.PoW is energy intensive. It's costly and requires plenty of computing power. It is vulnerable to the notorious 51% attack – meaning 51% malicious miners could capture the network and gain dominance, thereby making decentralization a failure.[6]

b) Proof-of-Stake(PoS):
Higher speed – Transactions are processed faster compared to PoW. Lesser energy consumption as there is no need for supercomputers.Lesser hardware requirements as users can participate, even without setting up a supercomputer.

It's still vulnerable. A person with enough money to invest can purchase an insane amount of coins thereby reducing the decentralization of the system.The rich get richer syndrome. Only the richest can have control of the consensus. There are several variations of the PoS; the most popular one is the DPoS.[6]

c) Proof-of-Capacity (PoC):
Livial energy consumption.Fairer than PoS, since disks are cheap and available = lower barrier entry.Proof-of-capacity is vulnerable to centralization due to participants outsourcing the file storage to an external provider.[7]

d) Proof-of-Burn (PoB):
It is well-suited for the introduction and distribution of new cryptocurrencies. It consumes less energy than Proof of Work and is more environmentally friendly.Coins created cannot be monopolized by mining pools or ASIC miners and thus distribution is fairer than Proof of Work.The process of burning promotes an investor's long-term commitment to the project.

Burning of coins can be considered a waste of previously-established value. It has the similar problem of Proof of Stake, in that whoever owns more coins to be burned can earn more coins, and thus has better chances to earn more of the new coins. There is no guarantee that PoB miners will be able to recover the value of the burned coins. Therefore, burning is also a risky investment. In some PoB systems, anyone who has ever burned coins gets a lifelong right to be allowed to generate new blocks. This means that their probability of getting the reward for the next block increases with the number of coins they have been burned over time. This problem is also paralleled with the Proof of Stake consensus algorithm.[8]

e) Proof-of-Importance(PoI):
The rich may not unfairly keep getting richer on the platform because the amount of cash possessed by an individual is not the only factor to consider when measuring the reputation of an account. One burning issue with this method is the use of fake transactions which would have people rewarded for sending back and forth transactions to cheat the algorithm. Use of dummy transactions is an issue that NEM and other major players are yet to exhaust.[9]

f) Proof-of-Activity (PoA):
High throughput; scalable. No mining mechanism like in PoW, PoA uses identity as the sole verification of the authority to validate. PoA is suited for both private networks and public networks. PoA only allows non-consecutive block approval from any one validator, meaning that the risk of serious damage is minimized. By identifying validators it is a centralized system.[10]

g) Proof-of-Weight (PoWeight):
Customizable; scalable. And Incentivization can be a challenge.[11]

h) Delegated-Proof-of-(DPoS):
Better distribution of rewards – People only elect delegates who offer them the most rewards. This means everyone earns and not just the rich. Thus, the DPoS is more decentralized than both PoS and PoW. Secure Real-time Voting – If users find any signs of malicious activity, they can immediately vote to oust the offending delegate. Cartel Formation – Chances are that witnesses could form cartels and rule the network. · Vulnerability – Since only a few people are in charge of keeping the network alive, it becomes easier for a 51% attack. Centralized – Power is in the hands of a select few.[6]

i) Leased Proof-of-Stake (LPoS):
A decentralized blockchain platform that allows for the creation of custom tokens. It attempts to address the "rich get richer" issues. It also aims to improve security, given that network security is better when there are more participants. To those ends, it seeks to incentivize those with fewer coins to lease out their balances to nodes.

The coins make the node stronger — or gives it more "weight," — increasing its chances of being allowed to add a block to the blockchain. The rewards received are shared with those who leased their coin balance to the "winning" node. [12]

3. Our Proposal

a) We are planning to modify tendermint consensus algorithm. We will modify tendermint consensus algorithm which are implemented using JavaScript and node_js in visual studio code.
b) Architecture/Existing framework: (Tendermint Consensus algorithm: without mining) [25]

Tendermint is a proof-of-stake consensus protocol that is Byzantine fault tolerant. Participants in the protocol are called validators. There is no concept of miners in Tendermint and thus, validators are also responsible for the creation of new blocks. The height of the chain increases every time a block is added to the chain. Validators are chosen in a round-robin manner to become the proposer who is in charge of creating and proposing a block for the current round. Validators are required to post a bond transaction that will lock a set amount of his coins (stakes) for a set duration. If the validator is found to be involved in any malicious activity within this duration, it can be punished by slashing away its deposited stake. After this duration, stakes is unlocked and returned to the validator.

Consensus Algorithm: The consensus algorithm consists of five steps - Propose, Prevote, Precommit, Commit and NewHeight.

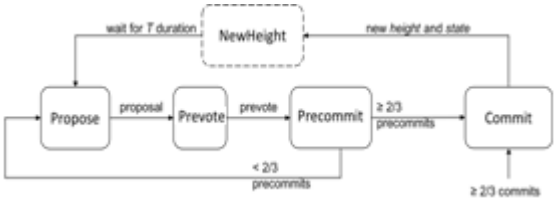


Figure 3: State machine of the consensus protocol, adapted from Tendermint: Consensus without mining

In the Propose step, the proposer broadcasts a proposal to its peers. A proposal includes the block, the signatures of the validators who have validated theblock, the signature of the proposer as well as the round and the height information. If the proposer has already locked on a block during the precommit of the previous round, that block will be used for proposal. Otherwise, a new blockwill be created. All nodes will gossip the proposal to their neighbouring peers during this period.

In the Prevote step, each validator will vote for a block and gossip it tothe neighbours. A vote consists of the hash of the voted block, the signature ofthe voter, type of vote - whether it is a prevote or a precommit plus the roundand the height information. The block to be included is chosen in the followingorder - (1) a locked proposed block from prior rounds and (2) a valid acceptableblock from the current proposal. If neither is available, a special NIL prevote is broadcast to the neighbours. All nodes will gossip all prevotes for the round to their neighbouring peers. In the Precommit step, the validator checks if it has received more than 2/3 of prevotes for an acceptable block. If there is one, the validator releases the existinglock, instead locks onto this block and signs and broadcasts a precommit vote for this block. The validator also packages the prevotes for the locked block intoa proof-of-lock which will be used to create the block in the next Proposal. Inthe case where there are fewer than 2/3 prevotes, the validator will neither signnor lock on any block. During this period, all nodes will gossip all precommits for the round to all neighbouring peers. At the end of Precommit, if the node has received more than 2/3 of precommits for a particular block, it will proceedto Commit step. Otherwise, it transits to the Propose step of the next round.In the Commit step, two parallel conditions must be fulfilled before the consensus algorithm can cycle back to Propose step. First and foremost, the node must have received the block from one of its peers so that it can sign and broadcast a commit to other peers. Second, the node must wait until at least 2/3commits of the block are received by the network. Once these are satisfied, thenode will set the CommitTime to current time and move on to NewHeight step where the nodes will stay for axed duration. The purpose is to allow the nodesto wait for additional commits of the committed block which were not receivedin Precommit due to network latency issues. After the set duration is up, thealgorithm starts again from Propose. At any time during the consensus process, ifa node receives more than 2/3 commits for a particular block, it will immediatelyenter the Commit step.

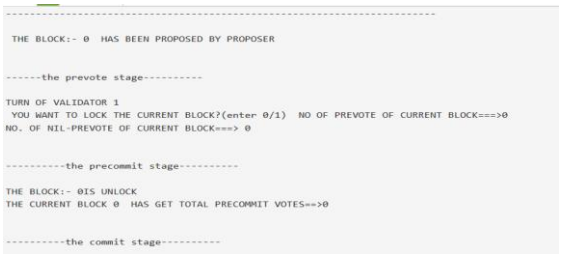
4. Experimentation and Result

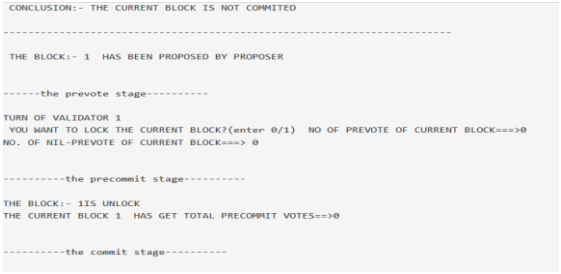
We are statically creating a tendermint consensus algorithm in c++ language.

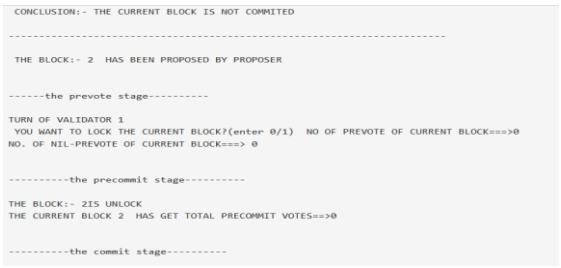
```
#include<iostream>
using namespace std;
struct Block{
        int id;
        char data;
        intprecommit=0;
        intprevote=0;
        intnil_prevote=0;
        int commit;
        int lock=0;
};
class voters
{
        public:
                int id;

 };
void propose(int s )
{    cout<<"\n----------\n";
        cout<<"\n THE BLOCK:- "<< s <<"  HAS BEEN PROPOSED BY PROPOSER\n";
        cout<<"\n\n------the prevote stage----------\n\n";
}
voidprevote(struct Block *b, voters* v , int n)
{
  //cout<<"\n\nTURN OF BLOCK:- "<<n<<"\n";
for(inti=n;i==n;i++)
  {
                //cout<<"for block"<<i+1<<"\n";
                int n;
                cout<<"TURN OF VALIDATOR 1\n ";
                cout<<"YOU WANT TO LOCK THE CURRENT BLOCK?(enter 0/1)  ";
                cin>>n;


                if(n==1)
                {
                b[i].prevote++;
                b[i].lock=1;
                                for(int k=2;k<4;k++)
                        {

                                cout<<"  TURN OF VALIDATOR : "<<k<<" \n";
                                cout<<"VALIDATOR 1 HAS LOCK THE BLOCK, DID YOU WANT TO PREVOTE THIS BLOCK?\n";
                                //cout<<"did you want to prevote this block?";
                                int j;
                                cin>>j;
                                if(j==1)
                                {
                                        b[i].prevote++;
                                }
                                else
                                {
```

```
		b[i].nil_prevote++;
                                        }

                                }
                        }
                        cout<<"NO OF PREVOTE OF CURRENT BLOCK===>"<<b[i].prevote<<"\n";
                        cout<<"NO. OF NIL-PREVOTE OF CURRENT BLOCK===> "<<b[i].nil_prevote<<"\n";
                        break;

        }
        cout<<"\n\n----------the precommit stage----------\n\n";
}
voidprecommit(struct Block *b, voters* v, int n)
{
for(inti=n;i==n;i++)
 {
 //       cout<<"\n\n\nturn of block:- "<<n<<"\n";
for(int k=1;k<4;k++)
   {
        int r=2;
                if(b[i].prevote>=r)
                {
                        cout<<"THE VALIDATOR:- "<<k<<"HAS PRECOMMIT THE CURRENT BLOCK\n";
                        b[i].precommit++;
                }
                else if(b[i].nil_prevote>=r)
                {
                        b[i].lock=0;
                }
                else
                {
                        b[i].lock=0;
                }


        }
        if(b[i].lock==0)
                {
                        cout<<"THE BLOCK:- "<<i<<"IS UNLOCK\n";
                }

        cout<<"THE CURRENT BLOCK "<<n<<" HAS GET TOTAL PRECOMMIT VOTES==>"<<b[i].precommit<<"\n";
        cout<<"\n\n----------the commit stage----------\n\n";
        break;
}
 }
void commit(struct Block *b,int a)
 {
        if(b[a].precommit>=2)
        {
                cout<<"\n\n CONCLUSION:- THE CURRENT BLOCK IS FINALLY COMMITED\n";
         }
        else
         {
                cout<<"\n\n CONCLUSION:- THE CURRENT BLOCK IS NOT COMMITED\n";
         }
 }

int main()
{
        struct Block b[3];
        voters v[4];
        for(inti=0;i<4;i++)
        {
                v[i].id=i+1;
        }

        for(int a=0;a<3;a++)
        {
propose(a);
                        prevote(b,v,a);
                        precommit(b,v,a);
                        commit(b,a);
        }
  /* for(int a=0;a<3;a++)
        {
                        precommit(b,v,a);
        }*/
}
```

Result:







5. Conclusion

In this paper, we wish to propose a modified consensus algorithm which is intended to provide Scalability, Energy, Cost, Number of miners utilized in mining process, Throughput. We formally modelled a simple consensus

algorithm for a proof-of-stake blockchain based on Tendermint and verified that the algorithmis deadlock free. We also proved that it takes > 2/3 of the network to reachconsensus and it takes > 1/3 of the network to censor the majority of the nodes from publishing a new block.

6. Future Work

We are interested in attacks and verifying more complex security properties.

References

[1] Inasiti,Macro:Lakhani, Karim R.(Januaray2017).”The truth of Blockchain”. Harvard Business Review. Harvard University.
[2] https://en.bitcoin.it/wiki/
[3] http://www.binarytribune.com/bitcoin-guide/limitations-and-issues-of-blockchain-technology/
[4] https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp
[5] https://www.kryptographe.com/a-guide-to-blockchain-consensus-mechanisms/
[6] https://yourstory.com/mystory/pros-and-cons-of-different-blockchain-consensus-pr-6246ttm3e7
[7] https://tokens- economy.gitbook.io/consensus/chain-based-proof-of-capacity-space/proof-of-capacity-poc
[8] https://coinclarity.com/know-your-crypto-proofs-pob/?__cf_chl_jschl_tk__=a4cc6c7bc88e784eb7caf6a05cd446d5fce067dc-1577611100-0-ARcB8u8j3WZL10QJgyyQznb_msX9NbaZaUnxtK1qxkwFSG2ueUDXM7XqXC05MXfZo2G2G65GGkE4DGW-MqbcVHYh2O8HzlJcnrwWnu-kMbwlQJAciab5d1-4RekcOMzxuagmudEc5pxYfhpOh8yhWguRMpwDvT8sDZJQeDm7QitkHebBD5hlcUDai2qSVEZjsnFXs2KI9_06c5sNalINrMKLxwo2N2fXbyAcucZDQqj99Mw6hBARRwKVHZo9RHxAe-PUyFIKbkH7L0HgA4yU_zpXofJ7S_6M2g3ZikC37VFD
[9] https://cryptodigestnews.com/blockchain-basics-pow-vs-pos-vs-poi-10a9b7c67d51
[10] https://tokens-economy.gitbook.io/consensus/chain-based-hybrid-models/proof-of-authority-poa
[11] https://tokens-economy.gitbook.io/consensus/chain-based-proof-of-capacity-space/proof-of-weight-poweight
[12] https://www.verypossible.com/blog/pros-and-cons-of-different-blockchain-consensus-protocols
[13] NRI, “Survey on blockchain technologies and related services,” Tech.Rep., 2015. [Online]. Available: http://www.meti.go.jp/english/press/2016/pdf/053101f.pdf
[14] D. Lee KuoChuen, Ed., *Handbook of Digital Currency*, 1st ed.Elsevier, 2015. [Online].Available:http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170
[15] V. Buterin, “A next-generation smart contractand decentralized applicationplatform,” *white paper*, 2014.
[16] “State of blockchain q1 2016: Blockchain funding overtakes bitcoin,”2016.[Online].Available:http://www.coindesk.com/state-of-blockchain-q1-2016/
[17] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.[Online].Available:https://bitcoin.org/bitcoin.pdf
[18] G. W. Peters, E. Panayi, and A. Chapelle, “Trends in crypto-currenciesand blockchain technologies: Amonetary theory and regulation perspective,” 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn.2646618
[19] G. Foroglou and A.-L. Tsilidou, “Further applications of the blockchain,”2015.
[20] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk:Theblockchain model of cryptography and privacy-preserving smartcontracts,” in *Proceedings of IEEE Symposium on Security and Privacy(SP)*, San Jose, CA, USA, 2016, pp. 839–858.
[21] B. W. Akins, J. L. Chapman, and J. M. Gordon, “A whole new world:Income tax considerations of the bitcoin economy,” 2013. [Online].Available: https://ssrn.com/abstract=2394738
[22] Y. Zhang and J. Wen, “An iot electric business model based on theprotocol of bitcoin,” in *Proceedings of 18th International Conference onIntelligence in Next Generation Networks (ICIN)*, Paris, France, 2015, pp. 184–191.
[23] M. Sharples and J. Domingue, “The blockchain and kudos: A distributedsystem for educational record, reputation and reward,” in *Proceedings of11th European Conference on Technology Enhanced Learning (EC-TEL2015)*, Lyon, France, 2015, pp. 490–496.
[24] C. Noyes, “Bitav: Fast anti-malware by distributed blockchain consensusand feedforward scanning,” *arXiv preprint arXiv:1601.01405*, 2016
[25] Formal Analysis of a Proof-of-Stake Blockchain Wai Yan MaungMaung Thin1, Naipeng Dong1, Guangdong Bai2, and Jin Song Dong1 1 National University of Singapore 2 Singapore Institute of Technology.