A hybrid and robust approach for secure and scalable protocols in cryptocurrency

Dr. Geetha J, Associate professor, Ramaiah institute of technology, geetha@msrit.edu
Varun BV, Computer science Student, Ramaiah institute of technology, varunbeekanvk@gmail.com
S Sri venkatesh, Computer science Student, Ramaiah institute of technology, *srivenkatesh1999@gmail.com*
Nitesh kumar J , Computer science Student, Ramaiah institute of technology, *niteshsingh2097@gmail.com*
Raviteja jagadish, Computer science Student, Ramaiah institute of technology, ja.raviteja.11@gmail.com

Abstract:
Cryptocurrencies recently are getting more popular, globally, and has a huge market value which is more than many reputed companies, crypto currencies are just like a digital asset which can be transferred between parties, there are various protocols which govern the working of the crypto currencies, and it uses blockchain the the underlying technology, to secure the transactions , it uses digital signatures to authenticate the transactions, there are many digital signature schemes with each of them offering different advantages and disadvantages, the main algorithms or protocols are the consensus algorithm and the digital signature scheme, In this paper we have shown a hybrid method to gain few advantages over existing protocols of cryptocurrencies, we show how schnorr digital signatures are better than the ESCDA digital signature. We have made new protocols or rather modifications on the proof of Work consensus protocol to reduce the time and energy consumed in the mining process of the blocks.

Keywords: Blockchain, cryptocurrencies, digital signature, Digital asset, Cryptography, Digital Signatures, Schnorr Digital Signature.

Introduction:
Blockchain, cryptocurrency, cryptography are connected and we explore the concept of digital signatures and the blockchain consensus protocol, However in this paper we address the major disadvantages of current bitcoin protocol, and other protocols, the speed, the computation energy required, the carbon footprint, scalability issues, environment issues of bitcoin mining, with keeping these factors in account we approached to develop a protocol which can address the above said issues about the current bitcoin protocol, we have used the same concept as proof of work with adding additional features such as micro transactions and capping the hardness of the mathematical problem, to enhance the speed and thus reducing the carbon footprint due to mining, also we have made use of the latest digital signature called the schnorr digital signature which tends to have various advantages over the current digital signature ie. ECSDA. (Elliptical curve digital signature algorithm. We have also shown our results when compared to the existing protocols and techniques.

Related Works

Proof of work: it is a protocol where the computation work done is considered as a proof to add valid transactions into the block, nodes also called miners competent with each other to solve the mathematical problem using computation power, and the first who solves with the most computation power is considered as the best trusted miner, and he receives a reward, POW also checks double spending.

Proof of stake: Unlike proof of work in proof of stake the node which will mine the next, is chosen based on its stake in the network, stake here means number of coins it has, but there is a problem , what if the same miner keeps getting more stake and always gets selected next, to counter this problem several methods are proposed, select nodes in random based on highest stake and lowest hash value, but in this method we can predict the next node because the stake is present in public, another method is that the next node is selected based on how long a node has held its stake.

Delegated Proof of Stake: this is a little different from Proof of stake, her they try to improve the scalability and productivity by reducing the number of nodes which does validation, the nodes which are called validators are selected by means of voting, this way the strain on the network is reduced, nodes which owns token are eligible to vote, the weightage of votes is based on their stakes in the network, there is also one more mechanism where the tokens can be transferred to another node in the network, here the voters can vote for witness and also vote for delegates if they find out there is any kind of malicious activities happening, by this way we can use the word democracy and equal weightage to poor and rich nodes,.

Proof of Elapsed Time: PoET was developed in 2016, by intel, it uses less computer resources, since there is not much computation required, the main idea in this protocol is that at every node there is a timer which decides whether the node is going to participate in mining the block or not.
But before this elapsed time which decides the node takes place, there is a protocol called Software guarded extension, which acts as the verifier and does the attestation, it protects the code and secures it from outside interaction, it makes sure the nodes download the correct code and also attest it , and generates a pair of security keys, the nodes signs and forwards this signed attestation,

Practical Byzantine Fault Tolerance: Byzantine fault tolerance means even though there are faulty or malicious nodes in the network, the distributed system still reaches the consensus this skill of the distributed network is called the Byzantine fault tolerance, the practical Byzantine fault tolerance, is used as giving an immunity

against these faults due to the malicious nodes in the network also called traitors, to provide the immunity against this fault, all the honest nodes, come together and make sure all the messages are valid and coming from a specific node, this is doen ins sequentially arranging the node and selecting one node as the leader and other nodes as backup nodes, also the condition assumed is that the fault nodes cant exceed one third the population of honest nodes, or equal to one third

Proof of Authority: In this system of protocol a group of nodes or individual users who wish to become authorities have to go through a strict selection, also it should be equally likely for all the long term committed nodes to be the validators or the authorities , those who wish to be at the authority position will have to reveal all the information such has their holdings and stakes to the public, also the number of such authority nodes must be small, of course this looks like decentralised system so the POA is applicable in only small private network rather than in public chains or networks.

Leased Proof of Stake (LPoS):
This protocol is similar to proof of stake with a slight change, here the stakeholders can lease or we can call as “recruit” other small miners to mine a full node or a part of the node and get a percentage of reward, this allows the stakeholders to get rewarded without mining, this concept of leasing is the major concept of this protocol,

Proof of Importance (PoI):

Unlike proof of work and proof of stake where the miners or nodes are given the chance to mine based on the computation power they have or based on the amount of cryptocurrency they hold also know as stake, so this is a clear picture of biased decentralised working nature. hence in 2015 an foundation called NEM.io introduced proof of importance, in the proof of importance to overcome this partiality the nodes which have a history of more transactions and is active in the network, and using many such factors like the amount of money vested, net transfers, cluster activity, , they give each node a importance score, based on these score, they are given the chance to mine, this also encourages more use of cryptocurrency and hence makes it more fungible in the future.

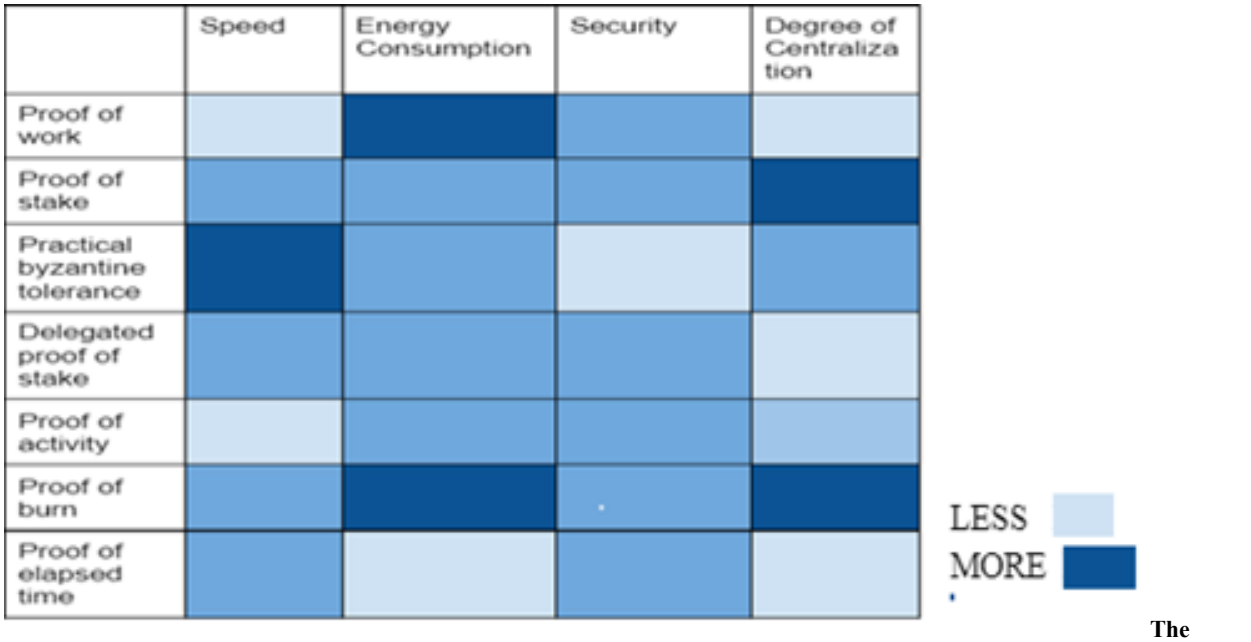
Proof of Activity:
Proof of Activity is attempting to combine the best aspects of proof of work and proof of stake.
In this mechanism initially the protocol follows the proof of work concept to create a block to be added next, in this step miners have to compete using their computation power, and for a attack to take place, any single entity should have more than 51% of the computation power.
Now after this initial stage they we make use of the PoS concept to select the next miners, as described in the PoS, the next miner is chosen based on his stake , here stake means the number of coins that node holds, but to avoid the same node being chosen again and again, they use a random selection process, which is a part of PoS protocol. So the first step PoW is used to find a block, the second

step PoS protocol is used to validate or sign a block,

Proof of Capacity:
This protocol was created to counter the energy considerations of PoW and hoarding of coins in the PoS protocol, in this protocol the miners in the network are allowed to use their own computer hardware to store the possible solutions values, so that they can match later with the hash value required, its similar to a lottery winner, if a person can collect or have as many as lottery tickets his probability of winning will be more

Proof of Burn:
Proof of Burn is an alternative consensus algorithm with minimal energy consumption, compared to other proof such as PoW . On proof of burn, the coins are burned in the process by sending the coins to an eater address. It uses virtual mining rigs to validate transactions, miners initiate coin burns as a way to show their participation in the network and be allowed to mine. The more coins burned by the miner, the bigger their virtual mining rig will be.

Proof of weight:
. In this protocol , weight is assigned to a randomly selected group of nodes , For example In the Filecoin ,weight is based on the interplanetary file system data stored among the nodes.The advantage of this protocol is that is it customizable , and can be made scalable , the random group of nodes in the network which are selected run a consensus algorithm while obeying the rules of decentralization and security,



The figure 1: shows the comparison of various consensus protocols, with respect to speed block validation, energy consumed for mining, security of the protocol, the degree of centralization, we can see from the figure that speed of Practical byzantine tolerance protocol has the best speed, PoW and proof of burn has the highest energy consumption, the security of Practical byzantine tolerance protocol is the least, PoS and proof of burn has the highest degree of centralization

Table 1: Shows the applications of various protocols which are used.

Sl No:	Protocol	Applications
1	Proof of work	Bitcoin, Litecoin, ethereum
2	Proof of Stake	ShadowCash, Qora, Black coin, peer coin, ethereum 2.0, Nxt
3	Delegated Proof of Stake	BitShares, STeem, STeemit, EOSIO
4	Proof of Elapsed Time	Hyperledger, sawtooth
5	Practical Byanzitine Fault tolerance	Zilliqa, Ripple, Hyperledger fabric
6	Proof of Authority	Aura, clique, microsoft azure
7	Leased proof of Stake	Waves Platform
8	Proof of Importance	NEM
9	Proof of Activity	Decred espers
10	Proof of capacity	Storj, burst, chia, spacemint
11	Proof of burn	Slim coin, TG coin, Bootstrapping auxiliary currency
12	Proof of weight	File coin

Digital signatures:

Schnorr requires relatively lower computation and storage than ECDSA while also allowing for better privacy. The additional feature that schnorr provides over ECDSA is Batch Validation which improves the time, computation resources required to validate multiple transactions.

The linearity nature of schnorr enables multi signatures. SInce there are more operations in ECDSA it is slower than schnorr digital signature. this along with batch validation makes schnor a faster algorithm. The reason that bitcoin had not already used schnorr over ECDSA was due to schnorr being patented., Since shorter size signatures require lower time and computational resources than the longer ones, micro transaction or transactions with amount smaller than regular transaction can be made to use smaller signatures to provide faster validations for transactions, thereby optimising the security and speed of the system as lower stake addresses/transactions do not require nearly as much security than higher stake addresses/transactions.

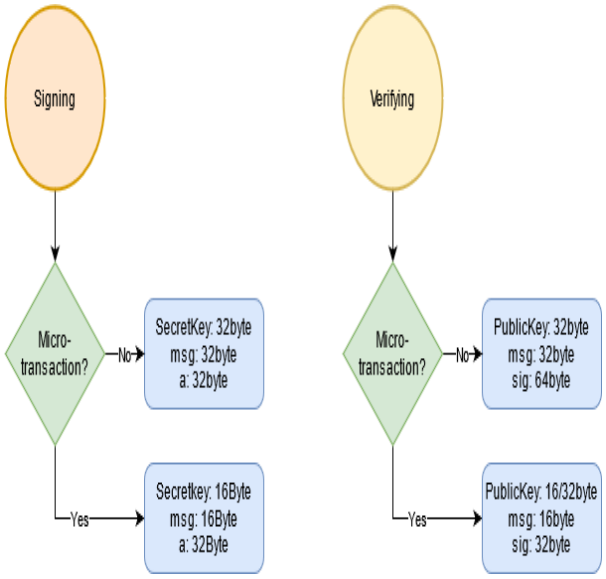


Figure 1: Microtransactiosn vs macro transactions.

A Consensus mechanism is required to settle the valid blocks and the order of those blocks in the blockchain by cooperation of all nodes on a rule. The requirement for a proof is that to have a voting system for the blockchain in which the order of the blocks will be decided on the majority of the votes. But in a blockchain system the votes are based on the resource consumed, the more resource consumed, the heavier the vote. It is different from the typical voting system by which it is conducted by numerical superiority, because in a system such as this, numerical superiority can be faked by just creating numerous virtual machines that act as a single entity, thereby jeopardizing the use for voting. When proof-of-work is implemented the effect of a high computational node is high, in proof-of-stake instead of computation the number of coins or the stake of that node in the system is considered.

Proof of work or stake is a consensus algorithm where the consensus algorithm itself is decided by the hash of the block.

When the block is finished, it gets hashed, the last digit of the hash is taken and checked if divisible by 2 or even number. When even, proof-of-stake is used, else proof-of-work is used as consensus.

The probability of the last digit of a block being odd or even is random but over time the blocks mined with proof-of-work or proof-of-stake will converge to 50% and 50%.

Implementations:

Figure 2 shows the Micro transactions are implemented in a way that they are 16-byte separate addresses for those smaller transactions. a 16-byte address can send to only another 16-byte address but a 32-byte can send to either 16 or 32-byte address.

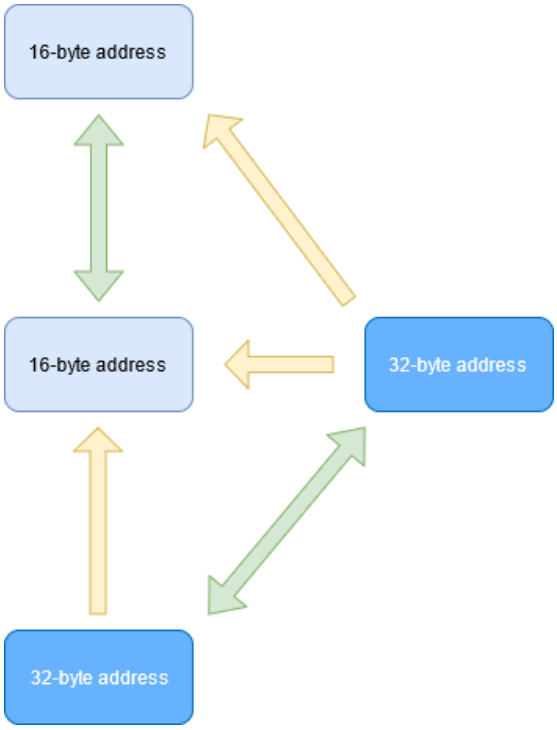


Figure 2: Macro transaction address size split up.

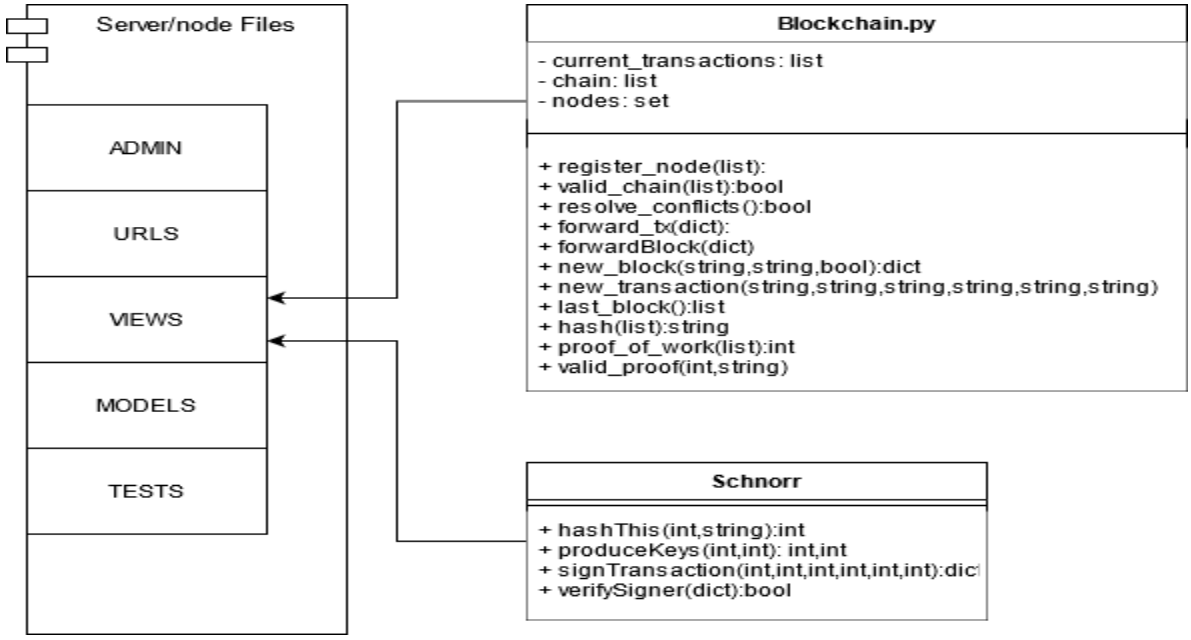


Figure 3: shows the python modules used for implementation of the blockchain network and the digital signatures using python, the whole model simulates the real time working of the coins. From which the results are obtained and compared.

Pseudocode 1:
In the below pseudo code,
If the transaction amount of any transaction is greater than 1000, we use a 128 bit, prime key. Else a smaller 64 bit key. This accounts to the trade off between speed and security.

```
tx <- new transaction

IF tx.amount < 1000
        prime <- 64-bit
        IF verifySigner(tx, prime)
                addTransaction(tx)
        ELSE
                verificationError()
        END IF
ELSE
        prime <- 128-bit
        IF verifySigner(tx, prime)
                addTransaction(tx)
        ELSE
                verificationError()
        END IF
END IF
```

Pseudo code 2:
Below code about the usage of hybrid protocol, for better security and less carbon foot print.

```
hash <- sha256(block)

    If hash[-1] % 2 == 0:
        proofOfWork()
    Else
        proofOfStake()
     EndIf
```

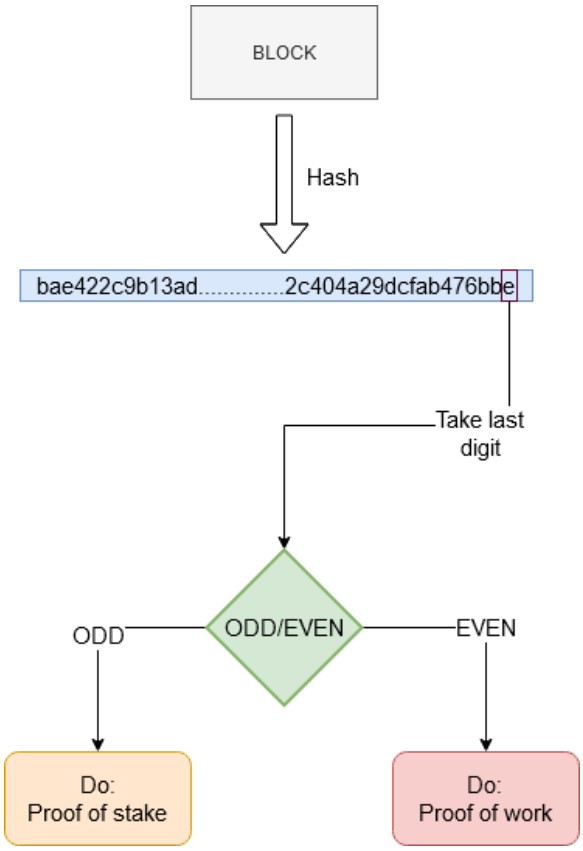


Figure 3: overall design of the modified consensus algorithm

Figure 3shows that a block is getting hashed and considering the last digit , we choose the protocol.based on odd or even.

Results:

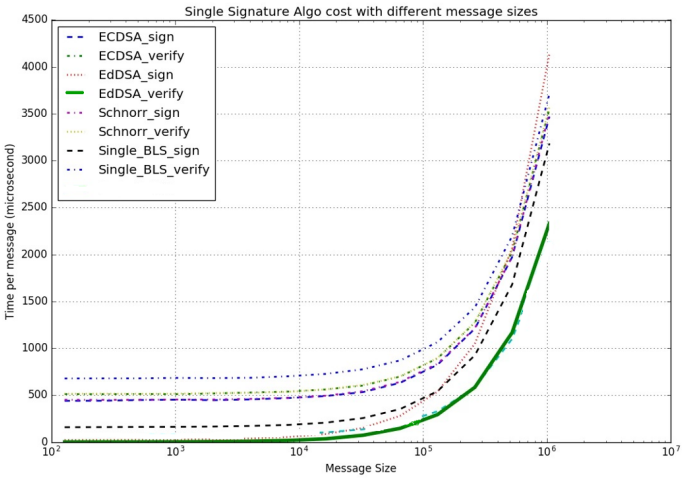


Figure 4: Shows the comparison of different digital signatures wrt verify and sign.

By implementing the elliptical curve digital signature algorithm and the schnorr digital signature algorithm, and integrated it to work with the blockchain consensus protocol, the figure 4shows the time taken by both algorithm wrt signing and verifying process, when the message length increases. We can see that schnorr takes less time than ECDSA , this is due to the many advantages which schnorr has, schnor has less number of multiplication operations than ECDSA, the schnorr can do batch validation since it is linear in nature.

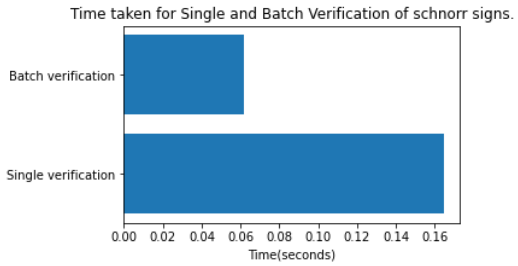


Fig 5- batch and single verification of 5 transactions.

The figure 5 shows the time taken by single schnorr verification vs the batch verification

time taken by schnorr digital signature, due to the linear nature of the schnorr , batch verification is possible which reduces the time.

Conclusion:

We have used proof of work as the main protocol, and have used the schnorr digital signature which has various advantages over the already existing ECDSA. Along with a novel modification of the proof of work algorithm to make micro and macro transactions to save time and trading it over security, and capping the hardness of the problem which has a positive environmental effect by reducing the computational power required for mining processes. Comparing the performances of both ECDSA and schnorr with the similar environment of the proof of work protocol we can clearly see that schnorr performs better, and faster, the implementation of micro and macro transactions performance is also been implemented and tested for along with graphical results. Which has a major impact on the energy being consumed. Thus we can say the new proposed protocol with the help of the schnorr digital signature, can have a good impact on the energy and environment considerations.

References:

[1] G. Maxwell, “Coinjoin: Bitcoin privacy for the real world,” Available: https://bitcointalk.org/index.php?topic=279249.0, Mar. 2013.

[2] T. Ruffing, P. Moreno-Sanchez, and A. Kate, “Coinshuffle: Practical de- centralized coin mixing for bitcoin,” in ESORICS 2014: 19th European Symposium on Research in Computer Security. Springer International Publishing, 2014, pp. 345–364.

[3] M. Andreas, Mastering Bitcoin: Unlocking Digital Crypto- currencies, O’Reilly Media, Inc., London, UK, 2014.

[4] A. Kiayias, A. Russell, B. David, and O. Roman, “Ouroboros: a provably secure proof-of-stake blockchain protocol,” 2017.

[5] K. Qin and A. Gervais, An Overview of Blockchain Scalability, Interoperability and Sustainability, Hochschule Luzern Imperial College London Liquidity Network, New York, NY, USA, 2018.

[5]A. Corso, “Performance analysis of proof-of-elapsed-time consensus in the sawtooth blockchain framework,” 2019.

[6] M. Castro and B. Liskov, “Practical byzantine fault tolerance,” OSDI, vol. 99, pp. 173–186, 1999.

[7] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” Future Generation Computer Systems, vol. 107, pp. 841–853, 2020.

[8] X. Liu, G. Zhao, X. Wang et al., “Mdp-based quantitative analysis framework for proof of authority,” 2019.

[9] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, ‘‘On blockchain and its integration with IoT. Challenges and

opportunities,'' Futur. Gener. Comput. Syst., vol. 88, pp. 173–190, Nov. 2018
[10] NEM Foundation. (Feb. 23, 2018). NEM: Technical Reference. Accessed: Jul. 14, 2018. [Online]. Available: https://nem.io/wpcontent/themes/nem/files/NEM_techRef.pdf
[12] S. Gauld, F. Von Ancoina, and R. Stadler, ''The burst dymaxion an arbitrary scalable, energy efficient and anonymous transaction network based on colored tangles,'' in Proc. CryptoGuru PoC SIG, 2017
[13] F. Tschorsch and B. Scheuermann, ''Bitcoin and beyond: A technical survey on decentralized digital currencies,'' IEEE Commun. Surveys Tuts., vol. 18, no. , pp. 2084–2123, 3rd Quart., 2016
[11] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, ''Proof of activity: Extending bitcoin's proof of work via proof of stake,'' IACR Cryptol. ePrint Arch., vol. 452, no. 3, pp. 1–19, 2014

[14] C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," in Stabilization, Safety, and Security of Distributed Systems: 17th International Symposium, SSS 2015. Springer International Publishing, 2015.
[15] P. McCorry, M. Moser, S. F. Shahandasti, and F. Hao, "Towards bitcoin ¨ payment networks," in Information Security and Privacy. Springer, 2016.
[16] G. Malavolta, P. Moreno-Sanchez, A. Kate, M. Maffei, and S. Ravi, "Concurrency and privacy with payment-channel networks," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '17. ACM, 2017.
[17] J. Herrera-Joancomart´ı and C. Perez-Sol ´ a, "Privacy in bitcoin trans- ` actions: New challenges from blockchain scalability solutions," in Modeling Decisions for Artificial Intelligence. Springer, 2016.
[18] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions," in Financial Cryptography and Data Security. Springer, 2016.
[19] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in Financial Cryptography and Data Security: 19th International Conference. Springer Berlin Heidelberg, 2015, pp. 507–527.
[20] L. Luu, R. Saha, I. Parameshwaran, P. Saxena, and A. Hobor, "On power splitting games in distributed computation: The case of bitcoin pooled mining," in 2015 IEEE 28th Computer Security Foundations Symposium, July 2015, pp. 397–411.