Journal of Intelligent Computing and Mathematics (ISSN Online: 2771-9952)
April 2022 Vol.1, No.1, pp. 8-16
DOI: https://doi.org/10.55571/jicm.2022.04012

4D Publishing Group

Bitcoin and Ethereum: The Crypto Currencies

Srinjoy Mahato[1], Tanmoy Khatua[2] and Tathagata Roy Chowdhury[3,*]

[1]Department of Computer Science, Techno India University, Kolkata, India
[2]Department of Computer Science & Engineering, Brainware Group of Institutions, Kolkata, India
[3]Department of Computer Science & Engineering,, Elitte College of Engineering, Kolkata, India

[*]Corresponding author's e-mail: tathagatamtech13@gmail.com

Abstract. Here we discuss about different cryptocurrencies those are very much important in network security market. As we know cryptocurrencies are digital assets which can be designed to work as exchange that can use strong cryptography to protect all the transactions, here the main Two aspects of those: Bitcoin and Ethereum, is discussed with their all functionalities, their methods of work, their advantages over each and other and more over their concepts of architecture.

Keywords. Cryptocurrency; Bitcoin; Etherum; SHA algorithm; ETHASH algorithm

Citation: Mahato S., Khatua T. and Chowdhury T. R. (2022). Bitcoin and Ethereum: The Crypto Currencies. Journal of Intelligent Computing and Mathematics, Vol.1, No.1, pp 8-16. https://doi.org/10.55571/jicm.2022.04012

Publication Date: 25 April 2022

1. Introduction

A cryptocurrency is a digital or virtual currency that is secured by encryption. Because of this security feature, counterfeiting a cryptocurrency is difficult. Blockchain technology, a distributed ledger created by a distant network of computers, was supported by various cryptocurrencies and decentralized platforms. The organic aspect of a cryptocurrency, which is probably its most appealing feature, is that it is not issued by any central authority, making it in principle immune to government intervention.

Bitcoin was the first blockchain-based cryptocurrency, and it is still the most popular and valuable. There are thousands of different cryptocurrencies available today, each with its own set of features and specs. Some of them are Bitcoin clones, while others are forks, or new cryptocurrencies that split from an existing one. Cryptocurrencies are online payment systems that are denominated in terms of a virtual "token" that represents ledger entries within the system itself. The term "crypto" refers to the

use of various encoding algorithms and cryptography techniques, such as elliptical curve encoding, public-private key pairs, and hashing functions. In the next parts, we will go through two commonly used Cryptocurrencies.

2. Commonly Used Cryptocurrency

2.1. Bitcoin

Bitcoin is a digital money that was first introduced in January 2009. It is based on the principles expressed in a white paper by Satoshi Nakamoto, whose genuine identity has yet to be established. Bitcoin, unlike government-issued currencies, guarantees low transaction costs and is controlled by a decentralised authority. There are no real bitcoins; instead, balances are maintained on a cloud-based public ledger, which, like all Bitcoin transactions, is validated by a tremendous amount of processing power. Even though it is not legal cash, Bitcoin is extremely popular, and it has sparked the creation of rival virtual currencies known as Altcoins.

2.2. Ethereum

Ethereum, which was launched in 2015, is one of the world's most popular programmable blockchains. It's a decentralised, distributed, and open-source computing platform with a Turing complete contracting language that lets us build smart contracts and decentralised apps. VitalikButerin, Mihai Alisie, Anthony Di Iorio, and Charles Hoskinson made up the first Ethereum development team. Ethereum, like other cryptocurrencies, has its own virtual money token called Ether.

There are three basic layers that make up Ethereum: The framework/backbone layer is made up of a wide network of computers that execute transactions and keep a shared database up to current over time (the blockchain). On top of that, there's the software layer. It aids with the execution of "smart contracts" on the Ethereum blockchain, which are written in a JavaScript-like programming language known as "Solidity." The uppermost layer is a collection of all the applications that provide Ethereum users with various services. The advantage of utilising Ethereum is that the applications created with it are totally decentralised. As a result, they lack a core point of connection, and the odds of failure are small to none, if at all. It is also free of government control because the ledger is present on each node independently.

2.2.1. Ethereum layers: Blockchain

Almost every website on the internet is hosted on a server in a data centre somewhere around the world. When we try to connect to a website, our computer establishes a connection with the servers and downloads the content that we have requested. When the internet was designed to connect a single host to multiple things, such as our computers, this worked perfectly. However, we now demand client computers to be directly connected to other client computers (Web 2.0). A peer-to-peer network is a huge network of connected computers that exchange information.The Ethereum hardware layer is a peer-to-peer computer network that computes transactions and keeps them in order in a shared ledger. A node is a machine in this network that validates new transactions and organises them into blocks that are broadcast to the Ethereum network as a whole. Both value and information can be included in the transaction. The value component is Ether, the Ethereum platform's digital currency. And the data is in the form of code that can pass data and initiate operations.

2.2.2. Software Layer: Solidity

The Ethereum software layer was created to solve Bitcoin's currency-based constraint. Ethereum can be used in a variety of transactions, from currency exchange to home purchases. To do this, a new programming language called Solidity was created to create Smart Contracts, which specify the logic or flow of a specific transaction (s). Solidity is a programming language for the Ethereum Virtual Machine that is inspired by C++, Python, and JavaScript (EVM). A smart contract is a programmed

Journal of Intelligent Computing and Mathematics (ISSN Online: 2771-9952)
April 2022 Vol.1, No.1, pp. 8-16
DOI: https://doi.org/10.55571/jicm.2022.04012

agreement that executes automatically and is stored on the Ethereum blockchain.

"Smart contracts are apps that execute exactly as planned without the risk of downtime, censorship, fraud, or the Ethereum Foundation," according to the Ethereum Foundation.

Ethereum makes it simple to create new digital currencies, known as tokens, that can be traded over the Ethereum network. This simplifies and secures transactions at retail malls. All of Ethereum's source code is open source, making it easily accessible to the general public. This has aided in the development of a community of users/developers who can resolve errors and add new features. As a result, the procedure is completely transparent. An ever-evolving platform, the codebase is constantly being changed to make it better.

Every smart contract's code is open to the public, thus we can always be sure the transaction will go well. The fact that it is open to the public and free of government control makes it a very attractive choice for enterprises, as it eliminates large transaction fees.

2.2.3. Application Layers: DApps

Third-party apps run on the Ethereum network's hardware and software layers. As previously said, DApps are not solely focused on finance. As of this writing, there are approximately 2200 DApps, with about 1500 of them live. Because of the open and transparent nature of the Ethereum platform, many developers are working on DApps. Since last year, the number of DApps has nearly doubled.

There are a few things to remember with Ethereum:

- It is Transparent in the First Place: Anyone, from anywhere, can look at the codebase. All transactions, as well as the method in which they occurred, are made public and tracked.
- It's Resilient: It's nearly impossible to shut down all of the Ethereum platform's computers/nodes, and because it's a shared ledger, shutting down the entire Ethereum network is unrealistic.
- Malleable code: Ethereum's code is far more changeable due to its open-source nature. Because the code is publicly available, any bug or exploit must be patched right once, as it makes it much easier to be exploited. Hackers are always hunting for exploits, and having the code readily available to them only makes their job easier.

2.3. Advantage of both Bitcoin and Ethereum

The advantages of bitcoin are**:-**

- **Freedom**
  Bitcoin was designed with freedom in mind. Most importantly , freedom from governing authorities controlling the transactions, imposing fees and being in charge of people's money. When it comes to buying things, cryptocurrency became just as legitimate as flat currency in recent years, and considering the existence of numbers deep-web markets that only accept Bitcoins, you may be able to buy some things easier with BTC than any other currency.
- **High portability**
  One of the main characteristics of money is it can be used and hold everywhere where we want. As Bitcoin is totally digital, practically any sum of money can be stored in a flash drive or online.
- **Choose your own commission**
  Another indisputable advantage of the Bitcoin network is possibility of choosing the transaction fee amount , or choosing not to pay it at all. The miner received the transaction fee after a new block is generated with successful hash. Usually, the sender pays the full fee, while deducting this fee from the recipient could be considered an incomplete payment..
- **Safety and Control**
  Bitcoin users are capable to monitoring their transactions; no one can withdraw money from my account without my knowing and agreeing to it, like sometimes happens with other ways of payment, and on one can steal your pay information from merchants.
- **Transparent and neutral**
  Every transaction or piece of information about all of them can be made available to everyone in

a blockchain that can be used in real time. Because the BTC protocol is secure, no one can change or control the data with the organisations, and the network is already decentralised. As a result, Bitcoin is always neutral.

- **It can't be counterfeited**
  In the digital era, one of the most common ways to simulate is to use the same money twice, making both transactions false. It's known as a 'double spend.' To combat this, Bitcoin, like most other cryptocurrencies, makes use of Blockchain technology as well as numerous consensus processes built into the BTC algorithms. Apart from providing the general benefits that an ordinary blockchain possess, Ethereum has more to offer. Here are some benefits that are listed below.
- **Immutable:**
  Once the data has been confirmed and recorded into the ledger, all transactions on the Ethereum blockchain are unchangeable. After data or transaction information has been posted, no one is allowed to change it..
- **Decentralized:**
  The transaction's validity is determined by the consensus mechanism that allows blockchain to survive. This implies that the acts must be carried out without the use of a trusted middleman. Smart contracts are self-executing, and before being published to the Ethereum blockchain, each transaction is confirmed by a validator. The proof of stake method, which will be deployed as a hard fork in Ethereum 2.0 or Ethereum Constantinopole, is expected to decentralise the blockchain network. It's a completely new method that, ideally, overcomes various disadvantages of the Proof-of-Work algorithm, which is utilised in Bitcoin..
- **Fast Transactions:**
  There is no block limit on the Ethereum blockchain. The quantity of transactions written into a block is determined by the miners' efforts. Currently, each block in Ethereum takes 10-20 seconds to mine, and there are roughly 15 transactions per second..
- **Currency and much more:**
  While Bitcoin and Ether are both digital currencies, unlike Bitcoin, the primary purpose of the Ethereum blockchain is not to establish itself as a payment alternative. The Ethereum algorithms are used by developers to build and run DApps or Decentralized Applications. These applications run on distributed computing systems and are popularized by distributed ledger technologies.
- **Secure:**
  On the Ethereum network, all transactions are cryptographically secure. Ethereum has almost three times as many nodes confirming transactions as Bitcoin. A node is a machine that is linked to the Ethereum network and is responsible for enforcing Ethereum's consensus rules. As a result, there are nearly three times as many miners available to verify transactions on the Ethereum blockchain.
- **Turing Completeness:**
  Ethereum is programmed in a way that ensures Turing completeness. If a piece of software or a programme can run any universal code given enough resources, it is said to be Turing complete/computationally universal. This eliminates the need for specialised software or computers that can only run specific programmes. As a result, Ethereum has an advantage over Bitcoin because Bitcoin uses a Turing-incomplete system that can only perform a limited range of tasks.
- **Rich Statefulness:**
  Vitalik Buterin describes Ethereum's ability to remember and maintain more state at the blockchain level by using this term. Bitcoin is considered stateless as it is only able to deal with transactions. On the contrary, Ethereum can deal with contract code and data on top of keeping a balance.

Journal of Intelligent Computing and Mathematics (ISSN Online: 2771-9952)
April 2022 Vol.1, No.1, pp. 8-16
DOI: https://doi.org/10.55571/jicm.2022.04012

4D Publishing Group

3. Explanation of SHA Algorithm and Ethash Algorithm

3.1. Encryption Technology

SHA 256 algorithm, a part of encryption technology is used in blockchain to get a constant hash of 256 bits every time. In the figure below, we see the prototype of algorithm containing some data called IV which is of 256 bits.

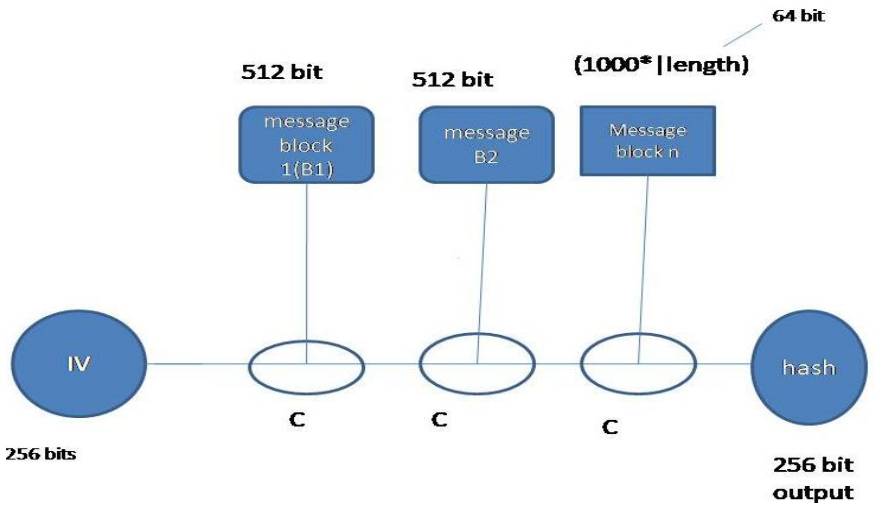

Figure 1. Protype of Algorithm

The very large input will be break in size of 512 bits which will always be not a perfect multiple of 512 bits, so some part of input will be left. We concatenate the left input with 10* bits before padding it. So now we have a perfect multiple of 512 bits input, which is added to 256 bits IV for a total of 768 bits, which is then compressed using the 'c' function to get an output of 256 bits only.

This 256-bit output is combined with the 512-bit input from block B2. To get a 256-bit output, the sum is again processed through the compression method. This loop continues until the last block is reached (block n).

3.2. Characterization of Bitcoin-Decentralization

The network's independence from any regulatory body was one of Satoshi Nakamoto's key goals when he created Bitcoin. It is set up in such a way that every individual, business, and computer involved in mining and transaction verification becomes a part of a large network..

3.3. Characterization of Bitcoin-Anonymous

Banks nowadays know practically everything about their customers, including their credit histories, addresses, phone numbers, and purchasing habits. Bitcoin is a little tricky because the wallet isn't meant to be linked to any personal information. While some people simply do not want their finances to be managed and tracked by any authority, others may argue that the drug trade, as well as other unlawful and unhealthy activities, will be divided in this relative support.

3.4. Characterization of Bitcoin-Transparent

Every single BTC transaction is recorded on Blockchain for future reference. When our wallet address was made public, we were able to figure out how much money was in it by looking at the blockchain ledger. However, tracking a Bitcoin address to a specific individual is extremely hard. Those who prefer to remain anonymous during their transaction might take steps to do so. The sorts of wallets that prioritise convenience over security and cryptography, such as those that can be used by several addresses and don't allow large sums of money to be sent to a single wallet or record.

Journal of Intelligent Computing and Mathematics (ISSN Online: 2771-9952)
April 2022 Vol.1, No.1, pp. 8-16
DOI: https://doi.org/10.55571/jicm.2022.04012

3.5. Characterization of Bitcoin-Fast

The Bitcoin payment process is almost so quick, it generally takes few minutes for someone to receive the money from the other side of the world, but general bank transfers can take few days.

3.5. Characterization of Bitcoin-Non-repudiable

Once we send our Bitcoins to someone, there is no way of getting them back, unless the recipient would want to send them back to us. This ensures the reception of a payment, meaning that whoever we're trading with can't scam us by claiming that they never got the money.

3.6. Characterization of Ethash Proof work Algorithm

ETHASH is based on a Proof-of-Work Algorithm constructed by the Ethereum network and cryptocurrencies based on Ethereum. In spite of being formed over the previous Dagger-Hashimoto algorithm, it has advanced enough to be considered an entirely new algorithm. See Figure 2 below.

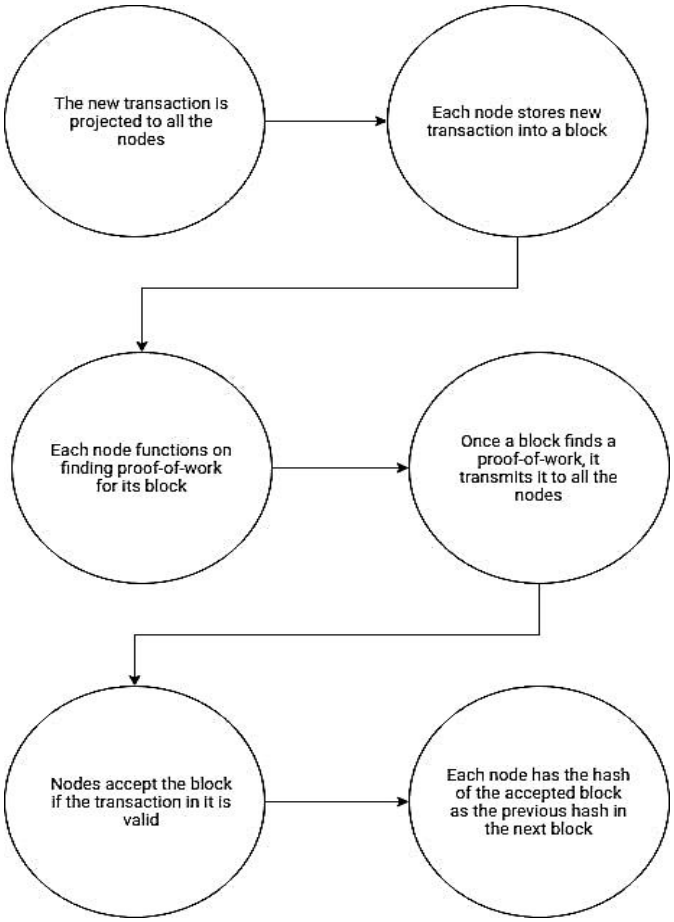

Figure 2. ETHASH algorithm working procedure.

ETHASH uses Keccak-256 and Keccak-512 hash algorithms, and it creates confusions over the simultaneous development of SHA-3, also known as the Secure Hash Algorithm. SHA-3 is a standard part of Keccak. With ETHASH, the output created during the hashing procedure must result in a hash value, which is below a particular threshold. This system is known as difficulty, and its purpose is to increase or decrease the threshold of the Ethereum network in order to control the rate of the number of blocks that are mined on the network. Therefore, if too many blocks are mined in a short amount of

Journal of Intelligent Computing and Mathematics (ISSN Online: 2771-9952)
April 2022 Vol.1, No.1, pp. 8-16
DOI: https://doi.org/10.55571/jicm.2022.04012

time, the network automatically increases the difficulty, i.e., it will lower the network threshold, resulting in reducing the number of valid hashes that can be found. Precisely the opposite happens when the rate of mined blocks decreases. The network threshold increases to produce increasing numbers of correct hash values that can be found. This system of difficulty is important for getting rid of an ideal situation where the time required to create new blocks drastically decreases, thus proportionally increasing the rate of payouts in the reward system. With the Ethereum Algorithm, the difficulty gets dynamically adjusted in such a way that, on an average, one block is generated by the network every 12 seconds.

Ethereum is advancing towards a major upgrade around January 2020, named as Ethereum 2.0, which is expected to radically change the way how the billion-dollar network produces blocks and verifies transactions. Dubbed as phase Zero, the first phase is supposed to launch Ethereum's new Proof-of-Stake algorithm strictly. Proof-of-Stake is based on consensus algorithms for public blockchains that rely on validator's economic stake in the network.

3.6.1. Explanation of ETHASH ALGORITHM

The ETHASH algorithm is dependent on a randomly generated 1GB Dataset known as a DAG(Directed Acyclic Graph). The DAG is updated once every epoch (30000 blocks). The size of the DAG will continue to grow as the blockchain keeps increasing.

The block header which is derived from the latest block and the current nonce are combined using the Secure Hashing Algorithm to create the 128-byte mix.

The mix is used to compute which 128-byte page from the DAG needs to be retrieved. It is represented by the Get DAG Page block.

Then the mix is combined with the DAG page that has been retrieved. This is achieved using a specific mixing function of ethereum to generate another mix. Let's name it as mix 1.

The steps two and three are repeated 64 times on mix 1, which yields another 64-byte mix.

The 64-byte mix is further processed into a shorter 32-byte mix. This is the final mix. This mix is compared to the predefined 32-byte target threshold. If the final mix is less than or equal to the target threshold, the current nonce is considered successful, and it will be broadcasted onto the ethereum network. Otherwise, the current nonce will be held invalid, and the algorithm will be rerun using a different nonce, either by increasing its value or by picking a value at random.

3.7. Significant features for New Algorithm

Stake – Only a select number of people who deposit money as a security deposit in the Ethereum network will be allowed to work on checking transaction blocks.

Therefore, the more money potential validators deposit into the Ethereum network, the higher his/her chances to be allocated a block that needs to be verified. The block rewards are to be delivered in proportion to the amount of money staked. The only way to increase the reward is to increase the stake deposit.

Penalty – The validators will receive a penalty if their work is found to be fraudulent, which will be deducted from the money they deposited. This helps the users of Ethereum to find trust in the working of the network and also the validators.

Decentralization – As the algorithm is not up and running yet, we still do not know how decentralized it can make the network, but to launch a 51% attack, the people planning on that have to rely on extreme monetary holding instead of computational power. The more money kept as a stake in the network, the higher the chances to be selected as a validator. It is yet to uncover how the factor of penalty plays in stopping such attacks. It is believed that the code can be modified to create economic incentives that discourage the formation of groups that can launch the 51% attack. It is yet to be understood how the introduction of penalty plays into stopping such attacks, as any fraudulent activity will be detected in the network and result in loss of ethers, and the only way to launch attacks is to acquire new ethers.

Cheap – If appropriately decentralized, this can prove to be a much cheaper way to mine/validate ethers than the traditional Proof-of-Work algorithm, as expensive mining equipment will not be required.
Backup – In case a validator fails to turn up for the job, it can easily be assigned to anyone from a number of backup validators available.

3.8. Advantages of one currency over other

When it comes to the cryptocurrencies that we are discussing today, extra emphasis should be paid to how mining works for each. Bitcoin mining uses a proof-of-work algorithm, whereas Ethereum mining uses a proof-of-stake algorithm. In PoW, each miner competes for computational power against other miners, but in PoS, the block validater earns the network fees and there is no other competition.

Ethereum has a faster block time than Bitcoin, which takes a little longer. Bitcoin has also outperformed Ethereum in the cryptocurrency market.

4. Conclusions

As we can see, there is a lot to learn about both Bitcoin and Ethereum, the two most popular cryptocurrencies at the moment. When it comes to cryptocurrencies, it's critical to understand the underlying differences, characteristics, architectures, and benefits. They are currently two of the most well-known networking projects on the market, with over two thousand different ones and its unique identification. There are currently a variety of restrictions in place, with Bitcoin's legal status varying greatly from country to country. The usage and exchange of BTC is encouraged in some nations, while it is prohibited in others.

There has been a lot of concerns regarding Bitcoin’s appeal to criminals, some news outlets have even stated that its popularity rests entirely on the ability to spend it on illegal goods. When the Silk Road was shut down, Bitcoin's value plummeted. However, we continue to strive to collect all of the information we can from all sources and books. We want to assist all students who, like us, will be able to use this data in their study. As a result, we compile a list of all the details that can assist the reader and reviewer with future projects or help them expand their knowledge.

Acknowledgements

The authors indicate that there is no funding available for this research work. Here, we the authors, would like to express our sincere respect to our college and faculties of Elitte College of Engineering for the co-operation in writing this paper.

Conflicts of Interest

The authors declare that there is no conflict of interest.

References

[1] D. Chaum, “Untraceable electronic main, return addresses, and digital pseudonyms,” in Communications of the ACM, vol. 24, no. 2, pp. 84-88, February 1981
[2] L. Law, S. Sabett, and J. Solinas, “How to make a mint: the cryptography of anonymous electronic cash,” American University Law Review, vol. 46, no. 4, pp. 1131-1162, 1996
[3] C. Dwork and M. Naor, “Pricing via processing or combatting junk mail,” in 12th Annual International Cryptology Conference, pp. 139-147, 1992
[4] W. Dai, “B-money,” 1998, available at: http://www:weidai:com/bmoney
[5] H. Finney, “RPOW,” 2004, available at: http://nakamotoinstitute.org/finney/rpow/
[6] N. Szabo, “Bit Gold,” 2005, available at: http://unenumerated.blogspot.rs/2005/12/bit-gold.html
[7] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: a technical survey on decentralized digital currencies,” IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123,

March 2016
[8] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer, "KARMA: A secure economic framework for peer-to-peer resourse sharing," 1st Workshop on Economics of Peer-To-Peer Systems, 2003
[9] N. Szabo, "Secure property titles with owner authority," 1998, available at: http://nakamotoinstitute.org/secure-property-titles/
[10] D. Malkhi and M. Reiter, "Byzantine quorum systems," Distributed Computing, vol. 11, no. 4, pp. 203-213, 1998
[11] J. Douceur, "The Sybil attack," in Proceedings of IPTPS '01 Revised Papers from the First International Workshop on Peer-to-Peer Systems, pp. 251-260, March 2002
[12] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008, available at: https://bitcoin.org/bitcoin.pdf
[13] Ethereum Community, "A next-generation smart contract and decentralized application platform," White Paper, available at: https://github.com/ethereum/wiki/wiki/White-Paper
[14] A. Back, "Hashcash – a denial of service counter-measure," 2002, available at: http://www.hashcash.org/papers/hashcash.pdf
[15] D. Eastlake, 3rd and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)," RFC 6234 (Informational), May 2011, available at: http://www.ietf.org/rfc/rfc6234.txt
[16] R. Merkle, "A digital signature based on a conventional encryption function," In: Pomerance C. (eds) Advances in Cryptology — CRYPTO '87. CRYPTO 1987. Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg, pp. 369-378, 1987