An Expandable Anonymous Currency System

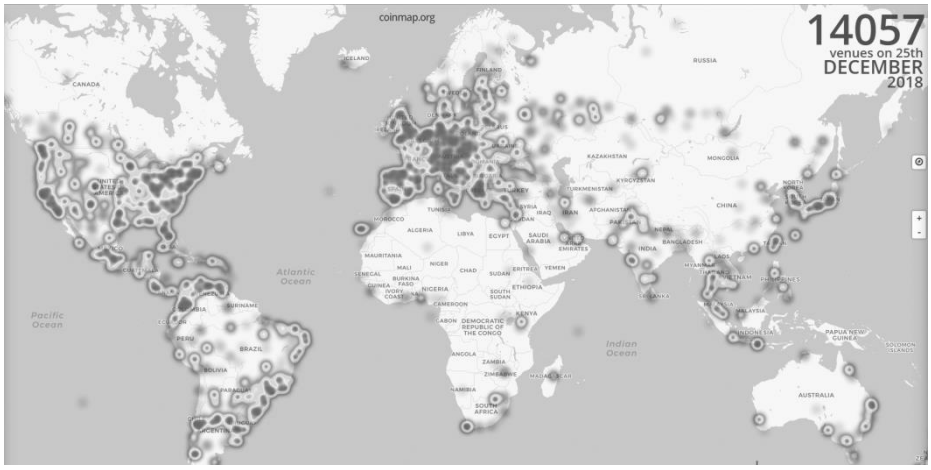
Based on POC Consensus

Description: After ten years of evolution since the birth of Bitcoin (BTC), BTC has been widely popularized and implemented, proving the feasibility of distributed, transparent and unchangeable point-to-point payment[1]. But the way BTC implements the proof of work(POW) and the maintenance of the entire network, determined to waste a lot of resources, has made BTC a game between few mine overlords since the emergence of ASIC mining machines which lead to a higher threshold of BTC mining. As time goes on, the distribution of BTC is becoming more and more aggregated, far away from the decentralization idea of Satoshi Nakamoto. Boomcoin is a new currency brought out recently based on Proof-of-Capacity(POC). POC consensus abandons many defects of POW and the electricity consumed in each transaction of Boomcoin is about one in hundreds of thousands of BTC. Boomcoin optimizes the mining mode of POC consensus with efficient transaction dealing, flexible architecture and perfect Turing protocol, developers can create advanced applications within Boomcoin.

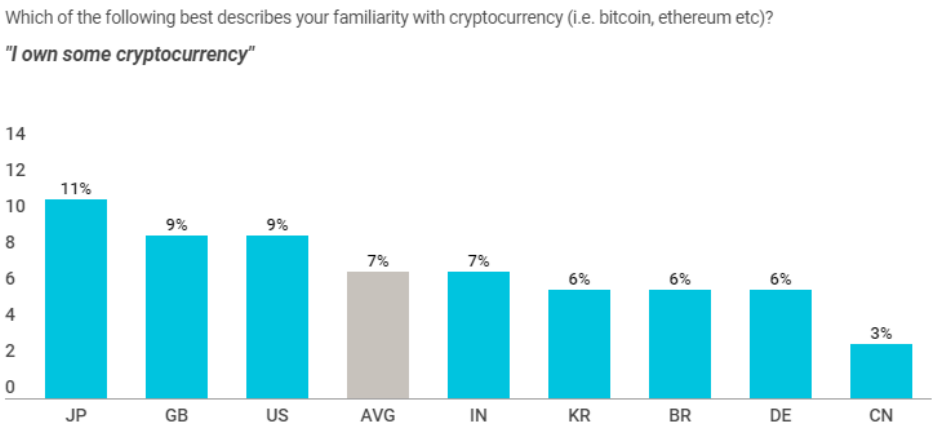
Keywords：Boomcoin– PoC — Smart Contract – Lightning-Network – zk-SNARK — POC3

Contents

1 Introduction



As of December 25, 2018, there are 14,057 venues that accept BTC payment, including retailer, ATM, attractions, cafe, food, grocery and more. (Source: coinmap.org)



The results shown are based on a survey of 29,492 internet-connected respondents from the US, UK, Germany, Brazil, Japan, South Korea, China and India, which was conducted by Dalia Research in March 2018[1].

What we found is that, among the 29,000+ internet-connected respondents across all countries, about 7% of them say that they own some cryptocurrency. This shows that cryptocurrencies are not only a media phenomenon, but actually owned by a notable chunk of the population, and now it may be a sign that a majority of the early adopters are already on board. Roughly 40% of the Americans were willing to use Bitcoin for transactions and shopping[2]. BTC has proved the feasibility of decentralized point-to-point payment successfully, and it seems BTC is evolving in a

[1] https://daliaresearch.com/blog-cryptocurrency-ownership/

wonderful direction.However, the last decade has seen a lot of problems with BTC.

1.1 Energy waste

1.1.1 ASIC – an autistic patient

It needs huge computing power to confirm current transactions and mine new BTC for circulation, and these should be done continuously. Currently, the mining architecture which supports this kind of BTC network is astonishing, and this computing power is provided by these so-called ASIC mining machines operated by miners. BTC ASIC mining machines are like autistic patients and they could only handle the computing of BTC blocks, besides which they could do nothing. In November 2018, news broke out that mining machines could be sold according to dumping prices since the selling prices of mined BTC could not offset the electricity cost consumed in mining which is caused by the fall of BTC price[2].

But for Boomcoin based on POC consensus, everyone could buy and mine BOOM easily. What's more, everyone needs hard disks and its value is protected.

1.1.2 Electricity waste

The continuous block mining cycle incentivizes people all over the world to mine Bitcoins. As mining can provide a solid stream of revenue, people are very willing to run power-hungry machines to get a piece of it. Over the years this has caused the total energy consumption of the Bitcoin network to grow to epic proportions, as the price of the currency reached new highs.

COUNTRY / TERRITORY	ANNUAL ELECTRICITY CONSUMPTION (TWH)
World	21776
China	6310
United States	3911

[2] https://www.ccn.com/bitcoin-miners-are-selling-old-asics-for-scrap-metal-as-price-decline-hastens-obsolescence

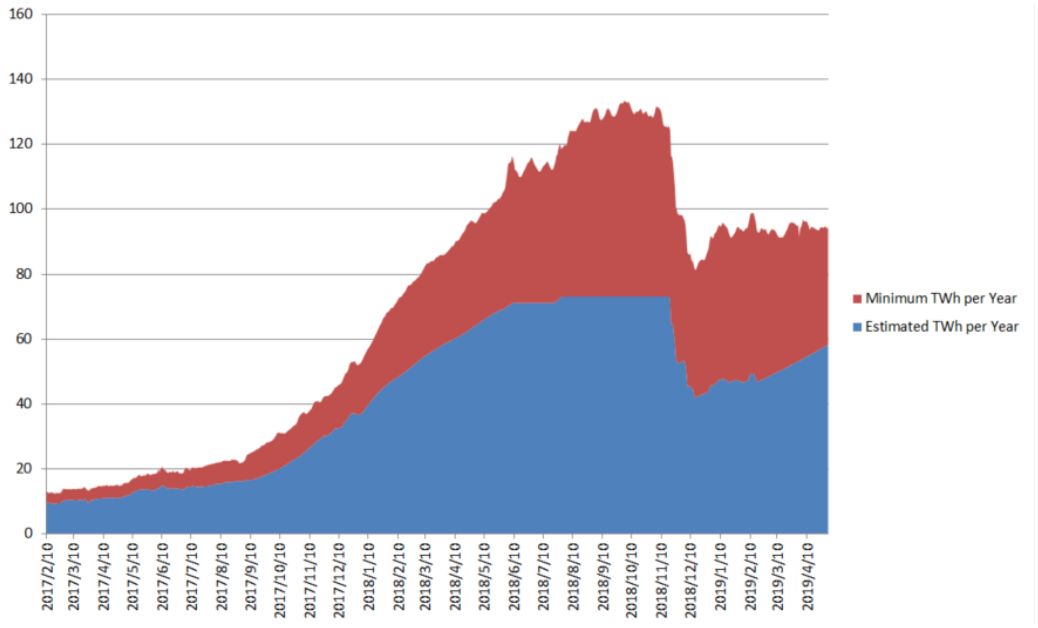
…	
Venezuela	78
Bitcoin Mining (high)	73.1
Austria	69.8
…	
Switzerland	58
Bitcoin Mining (low)	55.6
Bangladesh	55.5
Kuwait	54
…	
Turks and Caicos Islands	0.2
Gibraltar	0.2

Contrast between BTC and annual electricity consumption of all countries in the world[3]

According to the energy consumption index estimation from Digiconomist Bitcoin, currently, the power consumed for Bitcoin mining is between 55.63 and 73.12 TWh. This means that power consumed for Bitcoin mining is now more than that consumed in 175 or 181 countries/territories (159 last year).Bitcoin mining has consumed power that is as much as 33% of that consumed in Australian, 24% in UK, 14% in Canadian or 2% in US. Only 38 countries now have consumed more power than that used for Bitcoin mining.

In addition, the power consumed by BTC miners are four times as much as that in 2017[4] and is more than the magnitude several years ago, and currently these numbers are increasing exponentially. There is no evidence that this increasing speed will slow down. The power consumed by BTC in 2018 is 768KWH per transation, while it was only 169KWH in 2017[3].

[3] https://digiconomist.net/bitcoin-historic-sustainability-performance/



Bitcoin Energy Consumption Index Chart

1.2 Unfair mining

1.2.1 Cost of devices

Many miners are both device manufacturers and miners.In April 2017, an attempt to figure out Bitmain's profitability was made by Jimmy Song, a Bitcoin developer and entrepreneur, who looked into the production cost of Antminer S9 for this purpose. Song concluded that the production cost of Antminer S9 was "roughly $500", and the retail price of Antminer S9 was above $2,700 per machine at the end of December 2017[5]. While BITMAIN is a super miner owning 7 large-scale mining fields[4], it also owns mining machines manufacturers such as avalon and Canaan. An BTC mining machines has a huge profit margin, up to 400% because there is little competency in the market.

When miners hold ASIC mining machines, they need to be aware of the huge fluctuation of mining machines. In 2018, along with the drastic fall of BTC price, the price of Antminer S9 fell from a summit of USD 2,700 to 100.

[4] https://en.wikipedia.org/wiki/Bitmain

Boomcoin uses hard disks to mine with POC consensus. Hard disks are electronic products which can be bought everywhere in the world, and the popularization of POC consensus could not affect the prices of hard disks. At the same time, hard disks are electronic products everyone needs, thud its value can be maintained, which could be sold at a discount price of 50%. Also, BOOM mining could run with load in 95% of the total time, which could cause little harm to hard disks.

1.2.2 Electricity cost

From the above, mining BTC could cost a lot of electricity and the cost of electricity could determine the profit or whether it is worthing mining BTC. Electricity price in each country in the world has a significant difference which is impacted by the country policy. According to statistics in March 2018, in 67% of all countries in the world, the mining cost is below the price of a BTC(USD 11,455). While today, the price of BTC is USD 3,722. The number is still increasing, which makes mining BTC much more far away from most users in the world[5]. While miners with large mining volume could cooperate with electricity producers and pay electricity with one fifth of the price of common users. Let's go back to the idea of Satoshi Nakamoto, to mine with the idle CPU circle of one person today will cause net loss due to the cost of electricity. This phenomenon damages the stability and safety of the original distributed design.

COUNTRY	PRICE PER KWH (US CENTS)	COST PER BITCOIN (USD)
Kuwait	1.7	1415.09
Venezuela	1.9	1629.5
…		
Bahrain	4.2	3627.78
China	4.3	3644.93
…		

[5] https://powercompare.co.uk/bitcoin-electricity-cost/

Indonesia	10.3	8807.88
Albania	10.4	8903.25
…		
Uganda	19.3	16517.99
Mexico	19.3	16535.14
…		
Sweden	23.8	20422.61
Austria	24	20570.3
…		
Belarus	83.6	71698.01
Solomon Islands	93.5	80188.57

List of Electricity Cost Of Mining One Bitcoin By Country

But BOOM mining depends on the running of hard disks. If we spend USD 10,000 in buying Antminer s9, the total power could reach 40kwh, while with the same money on hard disks, we could buy 45 hard disks of 8T, they cost only 0.33KW when fully loaded (In fact, in 95% of the time of hard disks, they are in hibernation with a lower power consumption). So, everyone could attend BOOM mining, and the electricity cost has little impacts on the profit of BOOM mining.

1.3 Mining environment

In terms of heat, mining Bitcoin with ASIC miner will be faced with heat and ventilation problems at the residence, unless you're in a climate cold enough, a garage or somewhere with no neighbors. In case that the temperature of each miner has been up to a heat load of 1.32KW, the temperature in the room will rise rapidly if there is no proper airflow. In addition, each Antminer s9 will produce a noise of up to 79DB. A lot of news break out due to noises. As a consequence, the mining fields will be forced to close or add more investment in buying noise reduction devices[6]. High

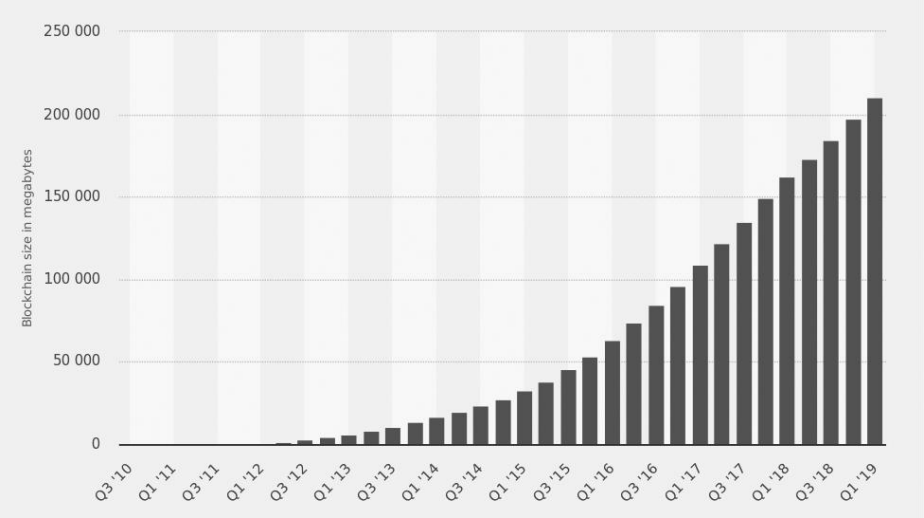
[6] https://www.coindesk.com/norwegian-crypto-mining-farm-might-have-to-suspend-operations

noise and high heat determine that mining BTC could not be done at home or in offices, which could impact the life of people around you. BOOM mine BTC with hard disks producing little noise and the heat equals to that of computers, which would not affect your work and your life. POC consensus of Boom is an important step for the exploration of cryptocurrency which is useful to both miners and coins. It can allow common people to mine with low energy consumption without worrying about high cost or over heat. It can bring a better power delegation of mining power for BOOM, because you do not need to compete with powerful companies with professional hardware of BTC. It is more energy-save than most mining protocols while it can maintain the safety.

1.4 Trading speed of BTC

At the end of 2018, the number of transactions being processed on the Bitcoin network was peaking at 360,000 per day, which is about 4 transactions per second (TPS). At present, the standard Bitcoin block size is 1 MB, and the full node clients generate it every ten minutes (on average) and limit the maximum capacity of the current Bitcoin network to about 7 TPS. Comparing this with the VISA network's capacity to handle 10,000 TPS, you will see that Bitcoin is not as competitive as it is now. Increasing public use of the Bitcoin system will soon cause Bitcoin to hit its transaction-per-day limit and halt further growth. In theory, BTC has a trading value of 80 TPS on the chain, and the speed increases 11 time than before. By increasing the block size, Boomcoin could have a larger TPS. But currently, transactions of Boomcoin can not fulfill its theoretical capacity initially. 80 TPS is not the ultimate upper limit, since the block size of Boomcoin is about 0.175M. We can resize the block size to 1M at any time and enable the ability of 480TPS, or we could resize it to 32M, which can give us the ability of 14000tps. But, in the future we could have solutions more intelligent and more expandable than the method to increase block size.

1.5 Block Size



Size of the Bitcoin blockchain from 2010 to 2019, by quarter (in megabytes)[6]

The Bitcoin blockchain is the collection of complete data blocks generated sequentially, containing the electronic ledger book for all Bitcoin transactions occurring since its launch in January 2009. Four years later, in January 2013, the size of the Bitcoin blockchain was about 4 GB. Eighteen months later, in July 2014, the size of the Bitcoin blockchain had swelled to about 5 to 19 GB. The size of BTC blockchain is keeping increasing highly, and to April 2019, it reaches about 210 Gigabytes. Compared with constantly iterating hard disks, the size of BTC is not large. But if the data in all the blocks are synchronized, it needs a long time. Initially BTC is a system aims to realize point–to–point payment, but it is hard to achieve the goal with current trading speed and data in the blocks.Provided that you would like to support 100 million people world–wide to be able to use a cryptocurrency like Bitcoin, and there is only one transaction per day on average, you would need a 400MB blocksize to meet that demand, implying that a blockchain growth of over 56GB per day should be available.

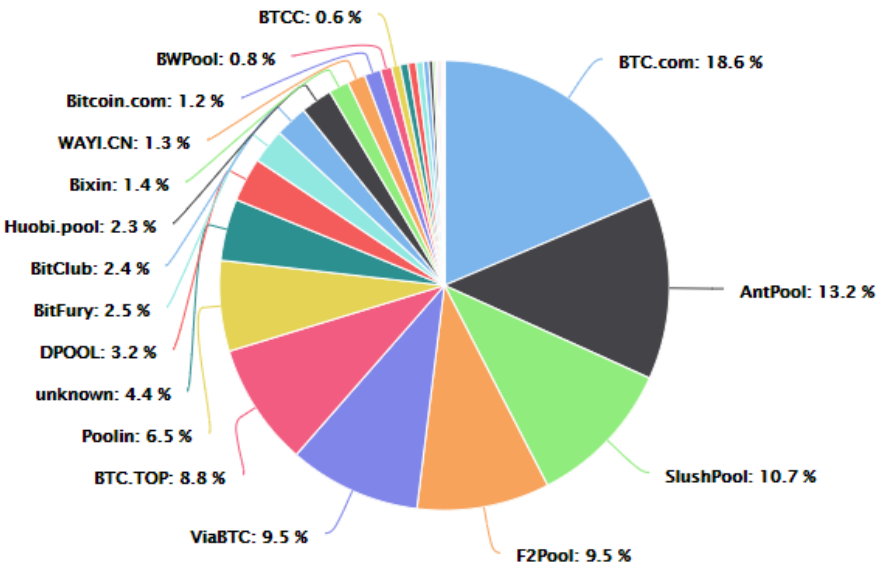
For Boomcoin, the block size is only 0.175 MB, one eighth of BTC. Users can synchronize all the blocks and attend in BOOM nodes with less time and less space.

In addition, it is questionable whether the purchasing transaction for a bag of rice made in china in 2017 should be permanently saved in the blockchain or in the bulk-storage memory with all the participating nodes worldwide. In the future, Boomcoin will implement a Blockchain Pruning feature (still under discussion) that will reduce blockchain size by selectively removing information on permanent blocks, and by deleting other non-persistent data, such as Arbitrary Messages.

1.6 Centralization of computing power

The difficulty of Bitcoin and the increase of network hashrate has created a high barrier for newcomers, what's more, returns from existing mining machines is decreasing. The block reward incentive adopted by Bitcoin has driven the installation of special ASIC miner and the dependency on few large-scale mining pool. This has resulted in a centralization effect of hashrate, where large amount of mining power are concentrated in the control of a decreasing number of people. Not only does this create the kind of Centralised structure that Bitcoin was designed to circumvent, but also presents the real possibility for the minority that they could accumulate 51% of the network's total mining power and execute a 51% attacks.

In early January 2014, GHash.io began voluntarily decreasing its own mining power because it was approaching the 51% level. After a few days, the pool's mining power was reduced to 34% of the total network hashrate, but the rate immediately began to increase again, and once reached the dangerous level in June 2014.



Pool Distribution (calculated by blocks)[7]

Bitmain contains two mining pool, Btc.com and Antpool.com. In addition, Viabtc.com is also invested by Bitmain. The mining ability of Bitmain can reach 41%, which is a dangerous signal. But nobody pays any attention.

In May 2018, the BTG network was manipulated in 51% attack. For the assault, the exchange lost a lot of money. A number of exchanges have lost capital, including Binance, Bitinka, Bitfinex, Bittrex, Bithumb and Hitbtc. The hacking has resulted in a total loss of some 388,000 BTC, which is valued at some USD18 million[8].

For the low mining threshold of Boomcoin, anyone can dig their mines in the scenario of families, offices or other occasional environment, assuring the dispersion of the computing power of Boomcoin.

2 POS vs POC

2.1 Decentralization

[7] https://btc.com/stats/pool?pool_mode=year
[8] https://news.bitcoin.com/bittrex-to-delist-bitcoin-gold-over-51-attack/

The biggest drawback of POS is the decentralization. Decentralization is the biggest driving force of cryptocurrencies and their revolutionary. Two problems are raised by POS system: initial distribution and mining reward.

In POS system, initial distribution of the coins is made through ICO, IEO, airdrops or similar processes. As a result, distribution happens in a short period of time. At the very beginning, the coins were already concentrated in the hands of minority. Moreover, POS people who have more coins could get more coins. With this self-reinforcing process, this monetary distribution system fosters inequality.

In POC system, coins are distributed to miners over a long period of time through mining. Comparing with using dedicated hardware necessary for POW cryptocurrency, everybody can mine, because only a computer and free HDD space is needed. Barriers for entry are very low. In POC system, miners will gain returns fairly in proportion to the disk capacity they use.

2.2 Energy Consumption

This is the main argument behind POS: it is often praised for its very low energy consumption compared to Proof-of-Work. However, POC shares that advantage of energy efficiency with POS. In fact, with POS you still have to run a computer which includes a hard drive. Mining with POC will consume more energy because miners often have to PLOT multiple HDDs, but the energy consumption difference is very little, and decentralization is easier than that of POC, so it is more secure.

2.3 Risks of 51% Attacks

In extreme cases, it will give rise to centralization. The safety of POS mechanism need to be guaranteed by shareholders, whose working principle depends on the interweaving of interests. Under such scenario, people without BTC will not pose a

threat to POS. The security of POS relies on the holder and has nothing to do with other factors. In terms of the POS mechanism, people with more BTC and longer participation will have more influence on the generation of new blocks. To put it simply, it means that the longer you own BTC, the more likely you will have access to the book-entry right. POS is easy to incur the Matthew Effect, i.e., people with more BTC may obtain more BTC reward. Consequently, the gap between the rich and the poor will be exacerbated, resulting in the centralized node surpassing the mark of 50%. That gives rise to the unexpected centralization. For example the 51% attack will allow them to manipulate transactions according to their preferences.

3. The Emergence of POC

Proof-of-Capacity is a consensus algorithm where miners will "PLOT" their hard drives in order to take part in transaction verification. In other words, the miners will compute and store the solutions for the mining problems before mining. These solutions have to be calculated in advance as they are too complicated to solve in real time. Moreover, the block times are really short at an average of 1 block every 4 minutes (compared to Bitcoin's 10 minutes). This is why the solutions to the hashing algorithm must be saved in advance. The way in which a miner is able to increase his / her chances of winning the block reward is making sure that they have the most solutions (plots) saved on their hard drives beforehand, which will be the fastest chance for increasing your solutions. It is worth noting, that slower plotting ability correlates with increase in ASIC resistance. This is why plotting is made via Shabal256 algorithm; this algorithm is very I/O intensive and thus too slow for ASIC to yield any economic advantage.

3.1 PLOT

There are two components that make up the Proof-of-Capacity, these are PLOT

and the mining on the hard drive.[7]

PLOT is the first stage and this involves that you creat your unique PLOT files. PLOT makes use of a hashing function called Shabal. This hashing algorithm is much harder to compute than SHA 256 algorithm used in the Bitcoin protocol. Hence, the miners will compute the solutions to the Shabal algorithm in advance and save them on the hard drive.

Boom will calculate a qualified hash in the process of Plot to determine whether the given nonce is valid. If it is valid, it will randomize the number by means of another hash.

Nomenclature

Block Forging — To generate a block for the Boomcoin blockchain.

Mining — Performs work for the blockchain in the way of computing and supplies the resulting values to the blockchain network.

Nonce — Data groups resulting from the Shabal algorithm.

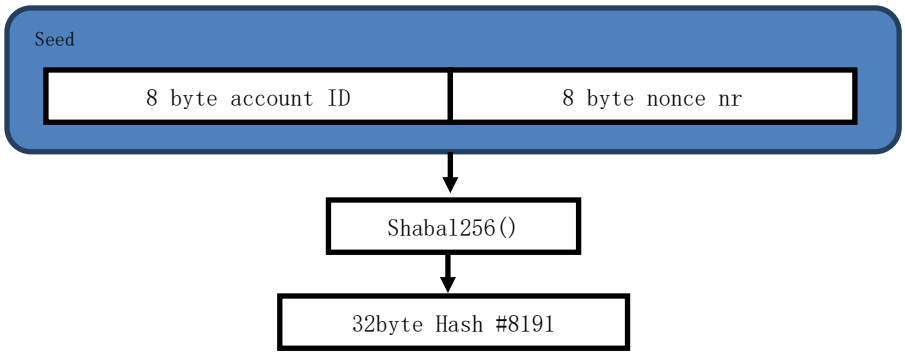
Scoop — Data saved within nonces, 4096 scoops make up every nonce.

Deadlines — Resulting values from processing of scoops during mining.

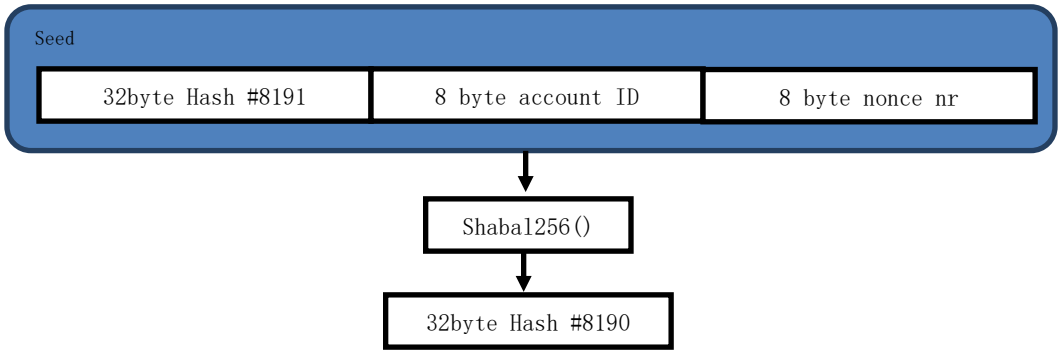
Plot file — File used for the mining process which contains precomputed nonces.

3.1.1 Generating a Nonce

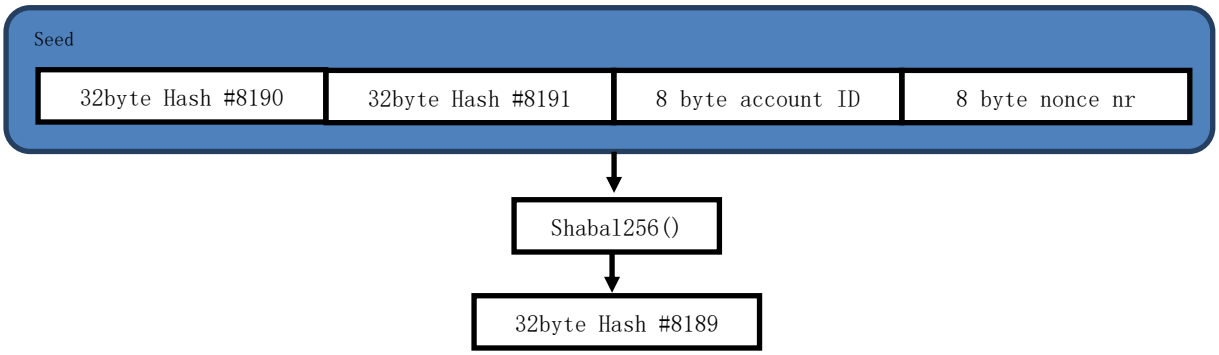
The first step for creating a nonce is to make the first seed. The seed is a 16byte long value containing the account ID that we will use to generate a nonce and the nonce number. When this is done we start to feed the Shabal256 function to get our first hash.



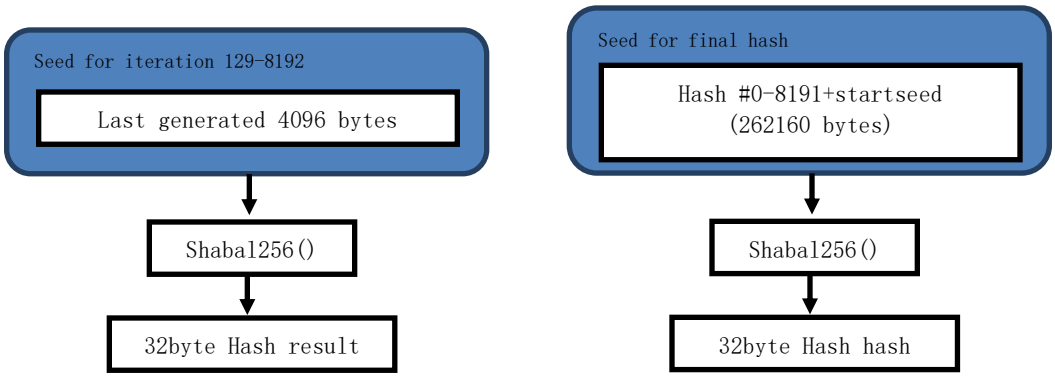
We have produced the first hash. This is the last hash (Hash #8191) in the nonce. Now we take this produced hash (#8191) and pre-append it to the starting seed. The result will now be our new seed for the next round of shabal256 computation.



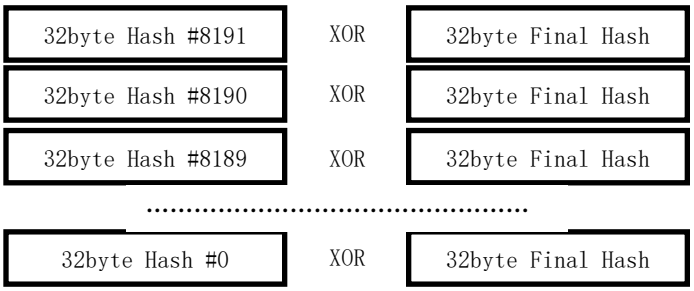
We now have produced two hashes, Hash #8191 and Hash #8190. This time we pre-append Hash 8190 to the last seed we used. The result will now be a new seed to Shabal256.



Once again, we have created a new hash. This procedure of pre-appending resulting hashes to a new seed will continue for all 8192 hashes we create for a nonce. After iteration 128 we have reached more than 4096 bytes in the seed. For all remaining iterations we will only read the last 4096 generated bytes.

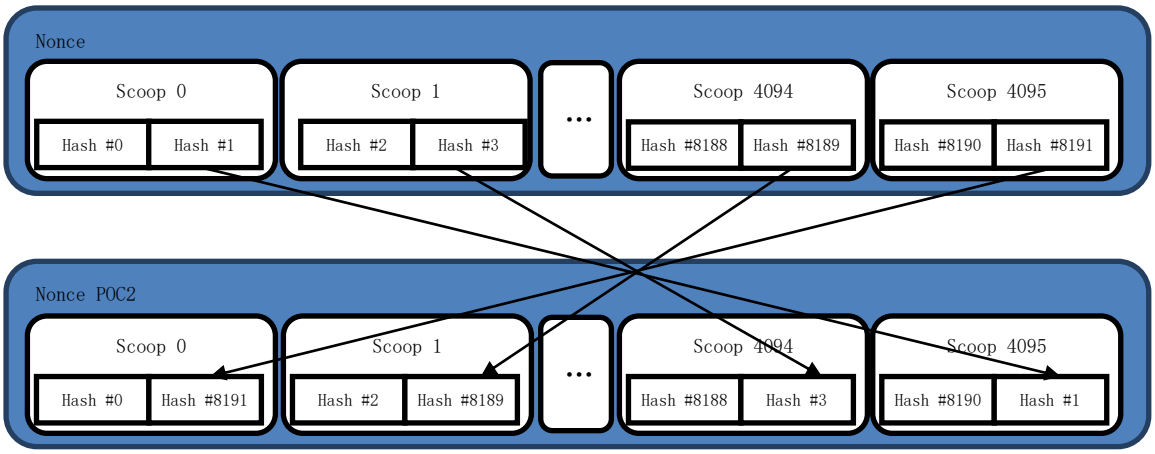


Once we have created 8192 hashes, we will make a final hash. This is done by using all 8192 hashes and the first 16bytes as seeds. The final hash is now used to xor all other hashes individually.



We have now created our nonce and can save it in a plot file before we continue to the next nonce.If we divide the nonce into 2 halves we will get the ranges 0–2047 and 2048–4095. Let's call 0–2047 the low scoop range and 2048–4095 the high scoop range. To shuffle the data into correct place we take the second hash from a scoop in the low range and swap it with the second hash in its mirror scoop found in the high range. The mirror scoop is calculated like this:

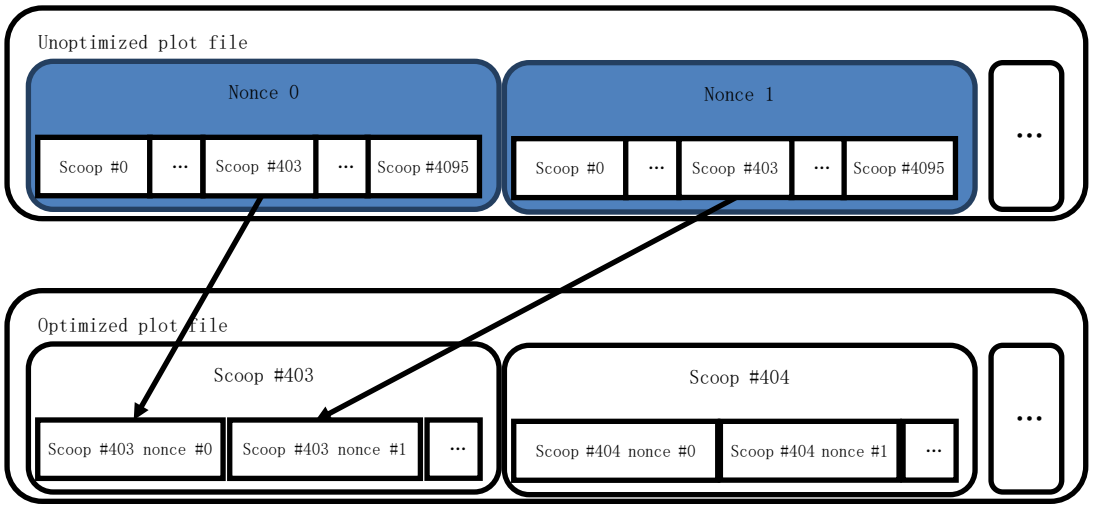
MirrorScoop = 4095 – CurrentScoop



3.1.2 PLOT Structure

When we are mining, we read from one or more PLOT files. The miner software will open a PLOT file and seek the scoop locations to read the scoops data. If the PLOT file is unoptimized the scoop locations will be on more than one place. In the following example the miner will be seeking and reading scoop #403.

This is not the most effective way since the miner will spend a lot of time to seek new locations on the storage device to be able to read the scoops. To prevent this, we can optimize PLOT or use plotter software that creates optimized plots from the beginning. Optimization is done by reordering the data in the PLOT file and grouping all data from the same scoop number together.



Basically, what we have done is to divide the plot file into 4096 portions where we split up all the nonce data based on scoop data. When the miner now wants to read Scoop 4096 it only seeks one time and read all data sequentially. This provides better performance.

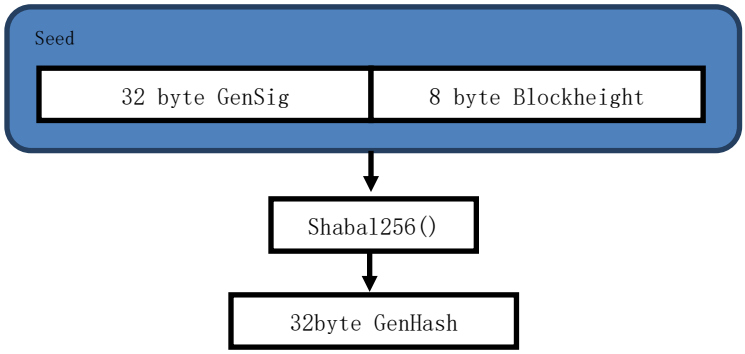
3.2 Mining and Block Forging

With most cryptocurrencies that are not based on Proof–of–Stake, there is a process called mining. This process is the foundation for a blockchain to grow and secure transactions within the network. Boomcoin is not different, except that you use precomputed hashes to find values that can be used to forge a block. This document is intended to summarize the processes. It is technical information, but not deep enough to be used as a reference for a programmer since information regarding subjects like AT, subscriptions, and assets is missing.

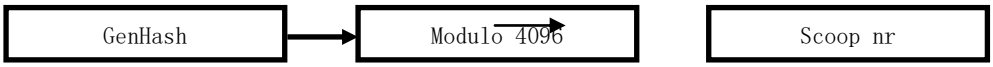
3.2.1 Mining Process

The first thing that happens when you start mining, is that the miner talks to the wallet and asks for mining information. This information contains a new generation signature, base target, and the next block height. Before the wallet sends over this information, it creates the generation signature by taking the previous generation signature together with previous block generator and runs this through shabal256 to

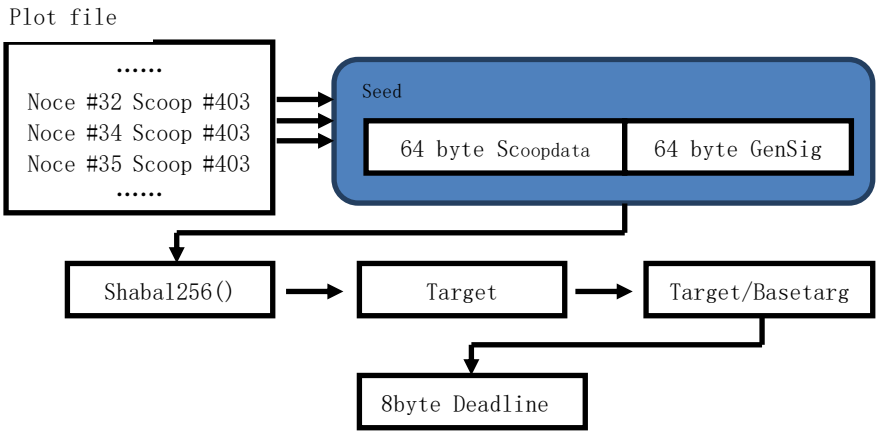
get the new hash. The miner now takes the new 32byte generation signature, and the 8byte block height, and put them together as a seed for Shabal256. The result will be a hash value called Generation hash.



Now, the miner will do a small mathematical operation on this hash to find out which scoop number to use when processing the PLOT files. This is done by taking the generation hash modulo 4096, as there are only that many scoops.



Next step for the miner is to read all the 64–byte long scoops from all nonces in all PLOT files. It will process them individually through shabal256 together with the new generation signature to get a new hash called target. This target is now divided by base target and the first 8 bytes of the result is the value deadline.



To prevent so–called “nonce spamming” to the wallet, the miner usually checks if the current deadline found is lower than the lowest one it has found so far. Usually

there is also a max value that can be set, as ridiculously large deadlines are of no use to anyone. After these checks, the miner submits information to the wallet. This information contains the numeric account ID bound to the PLOT file, and the nonce number that contains the scoop data used to generate the deadline. If you are solo mining the miner also sends over the passphrase for the account ID used in PLOT files. If the password is not sent when solo mining, the wallet would be unable to forge blocks for that account. During pool mining, the password for the pool account ID is used.

3.2.2 Block Forging Process

Deadline

The wallet has now received the information submitted by the miner, and will now create the nonce to be able to find and verify the deadline for itself. After this is done, the wallet will now check and see if an equal amount or more seconds has passed as defined by the deadline. If not, the wallet will wait until it has. If a valid forged block from another wallet is announced on the network before the deadline has passed, the wallet will discard the mining information submitted since it is no longer valid. If the miner submits new information, the wallet will create that nonce and check if the deadline value is lower than the previous value. If the new deadline is lower, the wallet will use that value instead. When the deadline is valid, the wallet will now start to forge a block.

Forging

There are two limits for a block. First, a block can contain max. 255 transactions. The second is that a block payload can have max. 179,520bytes (175KiB). The wallet will start by getting all of the unconfirmed transactions it has received from users or from the network. It will try to fit as many of these transactions possible until

it hits one of the limits, or until all transactions are processed. For each transaction the wallet reads, it will do checks. For example, if the transaction has a valid signature, if it has a correct timestamp, etc., the wallet will also sum up all of the added transactions amounts and fees. The block itself will only contain the Transaction ID of each transaction and one Sha256 hash of all the transactions included. Complete transactions are stored separately. Beside this, a block contains many different sets of values.

3.3 The Improved POC Consensus Model

POS's interest-bearing model with BTC ensures the deflation model of market liquidity. It is an advantage of POS, which greatly helps to stabilize the rights and interests brought about by currency. However, most of POS's currency fall into the category of inflation model, i.e., the overall sum of currency has no upper limit.

We may envision a scenario as follows: we create a new smart Contract A on the basis of ETH and issue a currency via it, which is assumed as Currency A. In the Contract A, Currency A will also be rewarded in the new block. In the meantime, Currency A generated from rewarding is directly proportional to Gas consumed by Contract A. If ETH switches to the POS mechanism, the reward of Currency A will be distributed to users who have bet on it. If the price of Currency A is high enough, Currency A can then obtain the most resources of ETH. Transactions concerning currency, like remittance will be prioritized. At that time, ETH will become a basic platform for Currency A. It can be explained that for users who have participated in the POS consensus mechanism, the benefits generated by Currency A has exceeded that of ETH. (Under the PoW mechanism, minders may take into the account of the short-term speculation value of Currency A and factors like the future value of ETH. For the reason, they may be prone to maintain the long-term value of the mechanism and will be more rational regarding the options for the implementation of contracts.)

In terms of the current situation, the POS protocol is more biased toward users. They have no need to invest in a large number of hardware. When they pursue profits, they will prefer short–term benefits. However, the short–term benefit may cause damage to the basic platform of blockchain, which may make 51% attack more likely to happen. The reason is that the short–term speculation of Currency A is easier that the bulk purchasing of ETH from the market. Therefore, from the perspective of Token economics, more careful and detailed design shall be given when it comes to the code implementation of the consensus mechanism of POS. Boomcoin learned from the coin–holding model of POS and increases mortgage for mining with Boom. Users will purchase Boom in the market for mining; however, the purchasing has its end. When there is a upper limit for the investment in hardware equipment, it will become a multi–party game in the market.

Users: They constitute the largest community in the ecology of Boom and serve as the nodes for wallet. They also provide minders with Boomcoin during the process of mining.

Miners: They purchase hardware to dig up the minds in the mode of solo or pool.

Developers: They give technological support in the ecology of Boom.

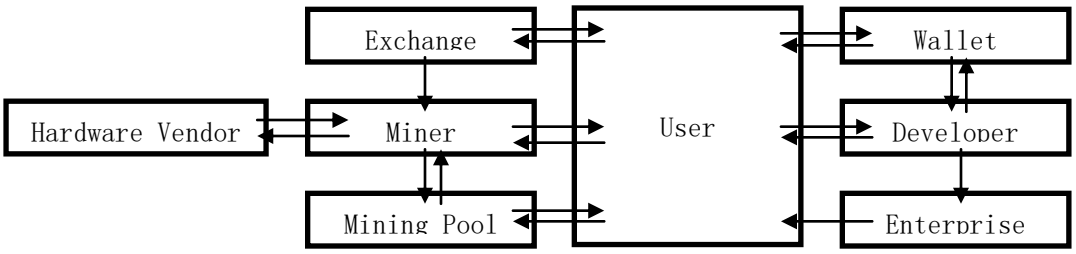
Mine pools: They are venues for mining. Generally, they also provide coin lending services.

Hardware service providers: They provide hardware support concerning hard disks and mining machines.

Enterprise: It provides the Boomcoin application for users.

Wallet: It is equipped with core functions like storage, remittance, asset issuance and crowd–funding.

Exchange: It serves as the venue for purchasing and selling Boomcoin.



The Ecology of Boom

4 Core Features

Boomcoin is a currency based on POC consensus. It is modeled after the multiple functions of Burst, containing features like smart contract, asset exchange, digital shop and crowd-funding system. Boomcoin boasts of acute structure with the capacity of indefinite expansion. The following content is a detailed introduction to the core functions of Boomcoin, please enjoy it.

4.1 Smart Contracts

Smart contracts are computer programs that can automatically execute the terms of a contract. Anyone familiar with computer programming would be aware of what is known as an if-then-else statement, where a program executes a certain task if certain conditions are met and does not if the conditions are not present. Smart contracts implement this on the blockchain in a completely decentralized and trustless way.

Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.

With BOOM, smart contracts are implemented using Automated Transactions (AT), a technology created by the CIYAM developers. Automated Transactions are turing-complete and thus have a potentially infinite number of use cases

If you are interested in BOOM smart contracts and want to learn how to create one yourself, please have a look at the documentation provided by CIYAM[8].

4.2 Asset Exchange

To exchange cryptocurrencies and other digital assets, you have to sign up for an account on a centralized platform such as Kraken/Bter/etc, transfer your assets to them and then pay them transaction fees. This brings in a large concern: a centralized exchange could just bail with everyone's deposits. BOOM has developed a peer–to–peer exchange software, allowing for decentralized trading which eliminates this trust point. It also eliminates trading fees.

The same technology that allows you to trade BOOM for many other digital assets can allow you to trade BOOM for almost any commodity.

This feature is based on the "colored coins" concept. Since the blockchain provides a trustworthy record of transactions, it can be leveraged to provide a record of trade of items other than BOOM. To do this, BOOM allows the designation or "coloring" of a particular coin, which builds a bridge from the virtual crypto–currency world to the physical world. The "colored coin" can represent property, stocks/bonds, commodities, or even concepts. As a result, the BOOM network could be used to trade almost anything.

4.3 Marketplace

The BOOM Marketplace provides a protocol for decentralized, peer–to–peer stores for any kind of digital goods like software, music or video. If you browse the sellers' products, place an order, the seller will send you information of how to download the good.

4.4 Crowdfunding System

Crowdfunding is the practice of funding a project or venture by raising monetary contributions from a large number of people. The BOOM crowdfunding feature allows you to create a decentralized crowdfund in a few clicks, and to donate just as easily. Creating a crowdfund is a child's play; the next step is finding people willing to pay for it.

The crowdfunding system is a nice and useful addition to the BOOM ecosystem and emphasizes the community spirit that drives all BOOM users.

4.5 Arbitrary Messages

This feature allows BOOM users to send small amounts of data through the decentralized network. These data can be encrypted. This feature can be used to send simple text messages, but can also be used to send up to 1000 bytes of any data.

Arbitrary messages are limited only by length. Any string can be transmitted, using any data structure or form of data encryption. Encoding, decoding, linked messages, data structures, and more can be implemented by any application that uses the system.

The base implementation allows for the transmission of simple, unencrypted text messages between accounts, but since the messages are truly "arbitrary" the range of possible applications is vast. For example, the secure messaging, torrent applications, voting systems, data storage systems and even simple distributed applications.

4.6 Alias System

The Alias System feature of BOOM essentially allows one piece of text to be substituted for another, so that keywords or keyphrases can be used to represent

other things — names, telephone numbers, physical addresses, web sites, accounts, email addresses, product SKU codes... almost anything you can think of.

For example, you could ask BOOM to associate ”search” with ”www.google.com”. Once this is done, all you have to do to get to Google is type ”boom:search” into a boom–capable browser, and it will translate your request in one for ”www.google.com”.

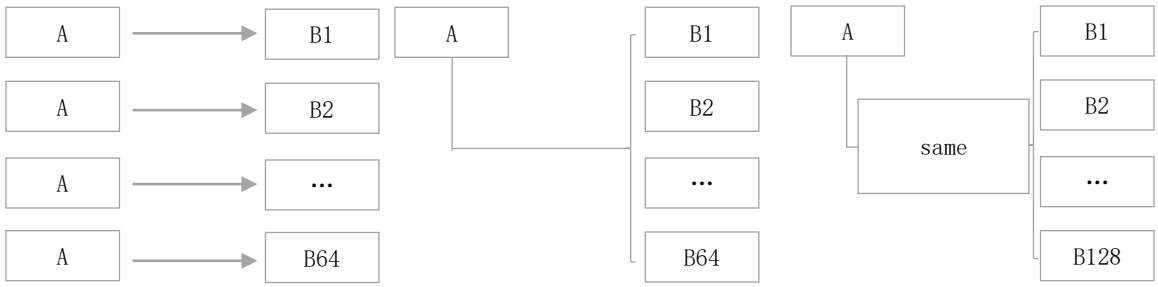
Immediate applications are simple: you can create an easy–to–remember alias for your BOOM account, for example. But since the Alias System is open–ended, it can be used to implement a decentralized DNS system, shopping cart applications, and more.

Alias can be sold to either specific BOOM Accounts or to the general public. To sell an alias, you can set the price to sell for every alias.

4.7 Multi–out Transactions

The most basic characteristic of any cryptocurrency is its ability to transfer tokens from one account to another. It serves as the basic transaction model for Boom, which allows for the function of basic payment. In the meantime, Boomcoin has the Multi–Out function, allowing for one operation to send the Boomcoin to N recipients.

Each individual BOOM transaction takes 176 bytes in a block. In its current state, the blockchain can support 1020 transactions per block. Each block will have a payload of 1020 * 176 bytes (179,520 bytes in total). BOOM Multi–Out transactions, allowing to send boomcoins to N recipients in only one operation. 64 ordinary payments take 64 * 176 bytes = 11264 bytes. If pools make their payout to miners, they nowadays have to issue e.g. 64 of these transactions, pay 64 BOOM transaction fees and occupy 1/16 of the block for this.



With the new Multi–Out transactions, a pool can simply issue one transaction (176 bytes) and name up to 64 recipients and the amount they shall get (8–byte recipient–ID + 8–byte amount = 16 bytes per recipient). A Multi–Out to 64 recipients takes 176 + 64 * 16 = 1200 bytes. So it costs 1/64 of BOOM transaction fees, and takes up roughly 1/150 of the new block. This payment is not exclusively for mining pools. Assume you would like to send money from your account to Bob and Alice. You could do 2 ordinary payments (2 * 176 bytes = 352 bytes) and pay 2 transaction fees or you could issue a Multi–Out to Bob and Alice at once (176 + 32 bytes = 208 bytes) and pay just one transaction fee. The more recipients you have, the more efficient a Multi–Out is for you (less tx fees) and the blockchain (less space taken).With the raised block size and these Multi–Out transactions, we can effectively have 9600 transactions in a block — 40 transactions per second.

Another type of Multi–Out transactions exists: the Multi–Out Same transactions. Instead of sending individual amounts to 64 recipients, it is also possible to send the same Boomcoin amount to up to 128 recipients and take up the same space in the blockchain (176 bytes + 8 bytes per recipient). This is especially useful for faucets. A faucet can serve 128 people in one single transaction, can send each 0.1 BOOM and spend on that transaction itself 0.1 BOOM . Total cost: 12.9 BOOM, taking up 1/150 of the block, and the recipients can comfortably perform 3–4 transactions with that 0.1 BOOM they got. With this type of transaction, the theoretical limit becomes 19,200 transactions per block — 80 transactions per second. BOOM will be able to perform at least 367,200 and a maximum of 6,912,000 on–chain transactions a day.

For comparison, BTC can do a maximum of 604,800 transactions a day. BOOM will be a lot more energy efficient than it is now, and incredibly — more efficient than BTC.

4.8 Offline Transaction

Offline Transaction Signing [offline device]

The term ”offline transaction” refers to the practice of keeping the private keys on an offline device (not connected to the internet), and signing on individuals transactions. The signature is then copy–pasted from this device into a connected device, and broadcast into the network. Assuming the offline computer is malware–free, then this practice is virtually risk–free of theft.

Online Transaction Signing [local device]

In addition to signing your transactions from an offline device, the signing can also be done on an online device but still performed locally. Assuming the computer is malware–free, this is the most convenient option while still keeping your private keys secret. For example the BOOM wallet uses this form of signing for its wallet interface through locally running javascript.

Online Transaction Signing [server side]

Just don’t do it. Although it’s possible, it would only be considered ”safe” to do this using a local host. Especially if you are developing/distributing software; do not present online signing as an option to your clients. You will make them a potential target for malicious actions.

5 Technical Roadmap

5.1 Anonymous Transaction

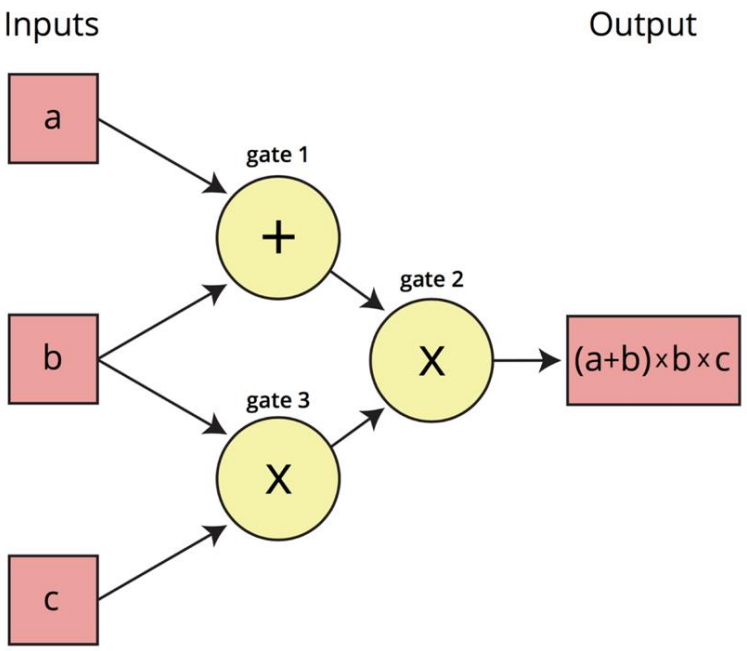
5.1.1 Zk-SNARKs

The acronym zk-SNARK stands for “Zero-Knowledge Succinct Non-Interactive Argument of Knowledge,” and refers to a proof construction where one can prove possession of certain information, e.g. a secret private key, without revealing that information, and without any interaction between the certifier and verifier. The value of zk-Snarks in modern blockchain technology is clear. It smoothly integrates with the smart contract technology. A smart contract is basically an escrow of funds which gets activated once a particular function is done. When the tasks that need to be done are multi layered and confidential, problems arise. You could potentially be required to conduct multiple steps in order to receive your payment. Zk-Snarks proves that those steps have been taken in the smart contract without revealing what they actually are.. It can just reveal part of the process without showing the whole process itself and prove that you are being honest about your claims.In order to have zero-knowledge privacy in Zcash, a mathematical function determines the validity of a transaction (determined the network’s consensus rules) by returning the answer of whether the transaction is valid or not, without revealing any of the information it performed the calculations on. This is done by encoding some of the network’s consensus rules in zk-SNARKs. The steps for achieving this encoding are as follows:

Computation → Arithmetic Circuit → R1CS → QAP → zk-SNARK

The first step in the process of creating a mathematical representation of the transaction validation rules is creating an “arithmetic circuit” by breaking down all the logical steps into smallest operations. Just like in a boolean circuit, where a program is compiled down into single steps like AND, OR, NOT, when a program is converted to an arithmetic circuit, it’s broken down into single steps consisting of the basic arithmetic operations of addition, subtraction, multiplication, and division.

Here is an example of what an arithmetic circuit looks like for computing the expression (a+b)*(b*c):



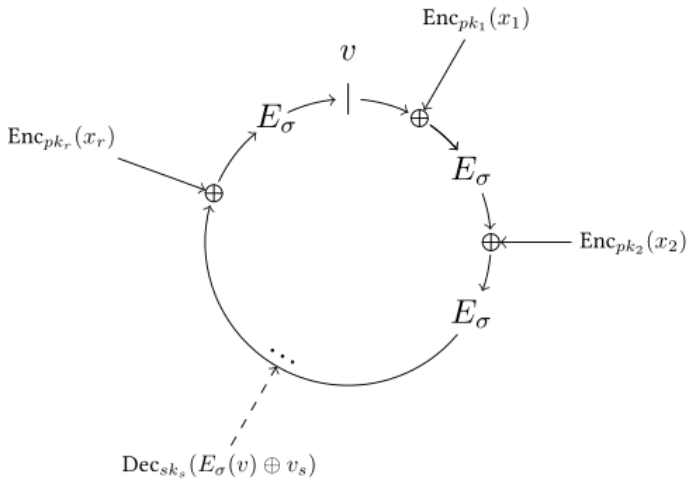
Input a, b, c and “travel” the values left–to–right on the wires towards the output wire. A Rank 1 Constraint System, or R1CS, is required to confirm that the values are “traveling correctly”. In this example, the R1CS will confirm that the value coming out of the addition gate where a and b went in is a+b[9].

5.1.2 Ring Signatures

A ring signature allows for secure signing of messages without compromising the anonymity of the signer. This works by hiding the identity of the signer within a group of users that each have keys that can be used to make the signature, then using cryptography to make it computationally infeasible for anybody to determine which set of private keys was used to produce the signature in any given transaction.

Ring signatures offer privacy improvements over a predecessor protocol called group signatures. Group signatures are centrally managed/coordinated and require setup procedures, while ring signatures groups don’t need to be managed and don’t have initial setup procedures.

The cryptocurrency Monero implements a linkable ring signature scheme to ensure that transactions on its blockchain are private. Used along with stealth addresses, this ring signature scheme makes all transaction outputs in Monero untraceable while ensuring that the network can't decipher which outputs are spent or unset.



Behaviour of the Rivest, Shamir, Tauman ring signature scheme

During anonymous transactions, both ring signatures and zk–snark has their respective advantages and disadvantages, which enable any of their functions can be optional for the anonymous plan for Boomcoin.[10]

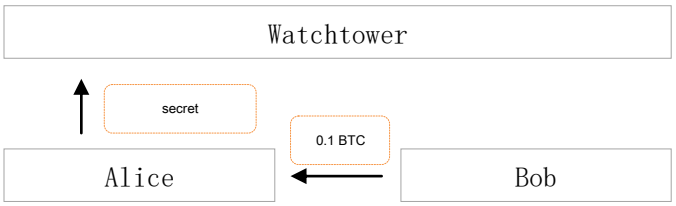
5.2 Transaction Acceleration

5.2.1 Lightning Network

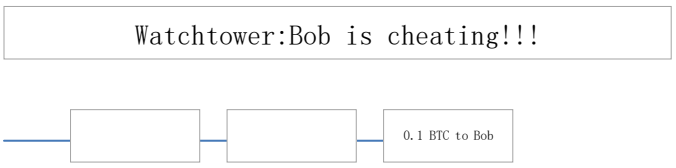
The Lightning Network is probably the most highly anticipated technological innovation to be deployed on top of Bitcoin. The payment layer, first proposed by Joseph Poon and Tadge Dryja about a year ago, promises to support a virtually unlimited number of off–chain transactions among users, at nearly no cost — while leveraging the security offered by Bitcoin[11].

Lightning Network implementation

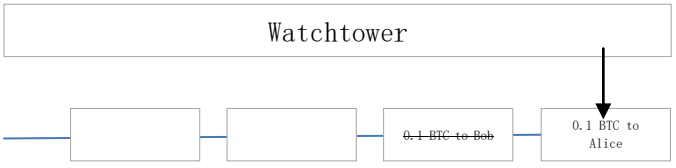
When Alice's payment channel state gets updated (Bob transfers 0.1 BTC to Alice), Alice sends to a LN watchtower encrypted signatures authorizing the movement of all channel's funds back to Alice. The package sent by Alice has no info about state's balances, so Alice's privacy should be safe (disputable), unless the channel will be closed unilaterally.



Basically, Alice is pre-signing a transaction of all channel's funds back to her, so she can be offline at the time the breach happens. Each sent package also contains a "hint" about how to find potential breaching on-chain transaction, so the LN watchtower constantly watches blockchain by checking all new transactions against its hash table of "hints".



Bob decides to cheat Alice by closing LN channel unilaterally with old state (i.e. a state before he sent 0.1 BTC to Alice). When the LN watchtower spots the breaching transaction, it's able to decrypt the signatures from Alice's package and reconstruct the penalty transaction which moves all funds back to Alice.



Since a channel was closed unilaterally, there is a time-lock on funds, so LN watchtower has some time to react, before Bob would be able to spend the "stolen"

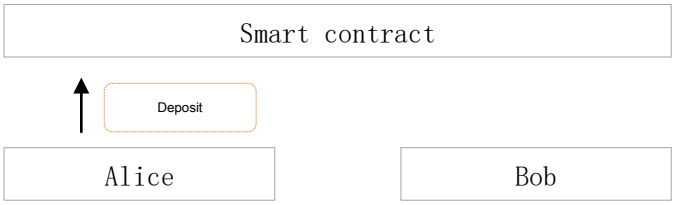
funds.

5.2.2 Raiden Network

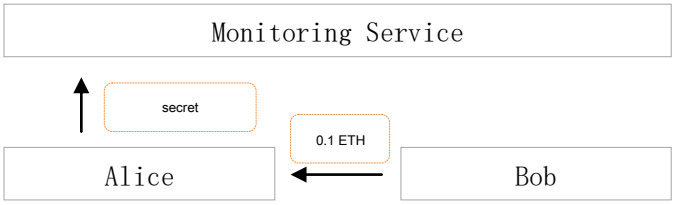
The Raiden Network is an off-chain scaling solution for performing ERC20-compliant token transfers on the Ethereum blockchain. It is Ethereum's version of Bitcoin's Lightning Network, enabling near-instant, low-fee, scalable micropayments. Raiden Network monitoring service is still a research area, so let's look at the latest proposed design[12].

Raiden Network implementation

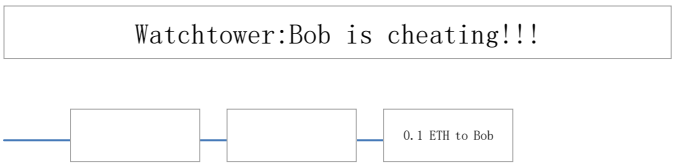
Alice deposits some tokens to a smart contract, which can be retrieved by a RDN monitoring service in case of successful defeat of Bob's attack.



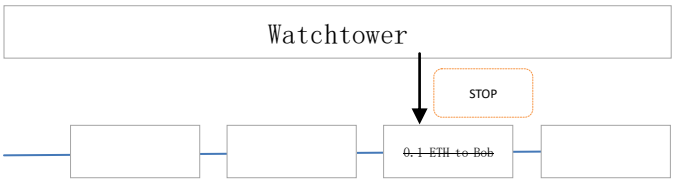
When Alice's payment channel state gets updated (Bob transfers 0.1 ETH to Alice), Alice publishes balance proofs including the token network, channel ID, a nonce and a hash of transferred amount into a public chat room. The sent message has no information about state channel's balances (only a hash), so Alice's privacy should be preserved (very disputable).



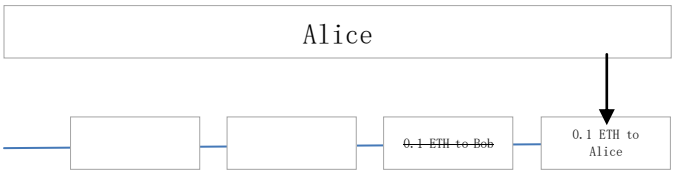
Since each sent message contains a channel ID, monitoring services can listen to 'channel close' events regarding this particular channel.



Similarly, Bob decided to cheat Alice by closing the RDN channel unilaterally with old state, in which he didn't send 0.1 ETH to Alice. Once the channel is set to be closed (within the challenge period), the RDN monitoring service will stop a settlement because the balance proof it holds for Alice is different from the one that Bob used for closing a channel (i.e., Bob's balance proof has a lower nonce).



Alice comes back online and closes a payment channel with the latest balance proof.



Key differences of Raiden Network implementation:

Alice has to deposit some tokens to a smart contract, which can later be used to pay for the RDN monitoring service.

RDN monitoring service knows which exact channel it watches and can link together all state updates made by the same user (on-chain address).

RDN monitoring services cannot reconstruct penalty transactions, so Alice has to come online to close the payment channel with the latest balance proof.

(However) Cheater is not risking to lose any additional funds as a penalty.

Conclusion

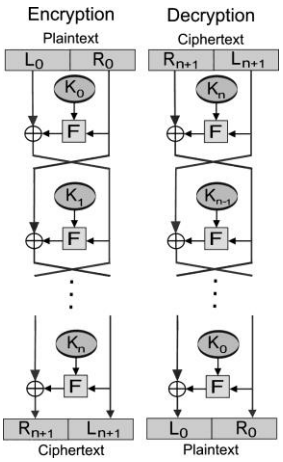
The Raiden Network is still in its development. Under the help of powerful intermediaries/mediators with a lot of financial resources, the operation of LN is available and viable. As for the speed–up plan for Boom's LN, it will not only face the competition from coins generated by different blockchains, but compete with centralized payment solutions. Those centralized solutions allow for instantaneous transactions without commissions, which are available for refund occasionally (such as Visa, Alipay, WeChat Pay and PayTM).

5.3 Dual–use Data Storage

The theory is conjured up by burstcoin[13].

The advantages of POC in comparison to POW or POS have been mentioned and examined under multiple perspectives already. While POC are energy–efficient, which in our opinion is the only sustainable way for a cryptocurrency with global impact, the space used for the POC consensus is of no other use than to perform mining and tx validation for the BOOM blockchain. Critics have pointed out that the disk space used for Boom is "lost" or "wasted" otherwise as plots are not really usable for anything else. This is formally true and because of this we propose establishing a Proof–of–Capacity 3.0 consensus.

This POC3 will exist in parallel to POC2. It will be based on dual–use data instead of the Boom mining–only plots of POC2. Dual–use means real–world data, like movies, audio, Wikipedia archive files, OpenStreetMap GIS data and more. In general, large immutable files of permanent interest to all – not the private word document, holiday picture or browser cache.



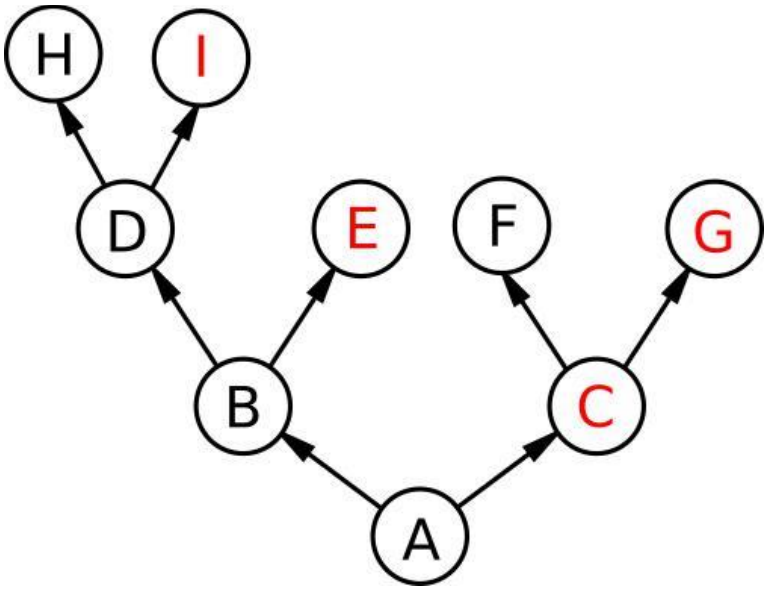
Symmetric Feistel cipher transformation for individualization of a PoC3 plot file.

The protocol would allow these files to be announced to the network (sha256, size) and voted on by nodes for validation inclusion. If a very high percentage (say 95% threshold) of the nodes would vote in favor of adding these files to the pool of "dual-use plots" which also implies storing these files themselves, each node would find deadlines in these files based on a succinct test of values of a virtual hard-to-pebble trees laid over individualised versions of these files. Once in the pool of accepted plots, POC3 plots would need to remain there, be-cause while for mining their presence is optional, for ab-initio validation of the blockchain when re-syncing their presence is mandatory. (For the future, we can picture a situation with a distinction of "full POC nodes" containing all POC3 and being able to make such a resynchronization and "restricted PoC nodes" being able to sync blockchain from the full nodes.)

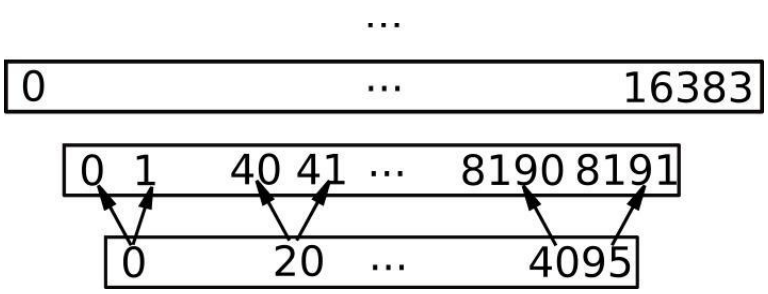
First, each POC3-accepted file would undergo a Feistel cipher transformation with the numeric ID of an account to individualize it as plot and counter grinding attacks. The mining process would assume the file being mapped on a RB-Tree layout.

Let the basic operation of the Feistel encryption with the round function F and sub-keys K0; K1; : : : ; Kn for the rounds (0, 1, …, n) be as follows:

Split the plaintext block into two equal pieces, (L0; R0), in our case two 32–byte blocks.



Red–Black binary tree structure for traversing POC3 plots. Each node being a 64–byte data block, each depth represents next level as depicted in the data layout of the next figure.



Data layout of a POC3 “PLOT”. Each level twice the size of the original data, maximum 64 levels allow for a plot size up to 2 YiB (yobibyte).

Using Feistel ciphers allows for individualization, yet loss–less retrieval of arbitrary data. The symmetry guarantees the cipher being of same length as the original data, paving the way for a dual–use POC.

We will not give detailed introduction here. However, readers are encouraged to browse the excellent introduction in the white paper of burstcoin.

The following problems are still troubling POC3.0:

1. For the differences in the size of bandwidth and the space of hard disks concerning each node, it is worthy of discussions about the issue that whether all the nodes are in need of participation in POC 3.0. For example, rewards can be used to encourage the participation into POC 3.0.

2. As for malicious, unnecessary and non-persistent data in POC3's PLOTS, it is worthy of consideration about whether it is necessary to trim and how to trim.

The BOOMCOIN will thus not only form the fundamental layer for a truly global transaction network, it can also take over a custodian role in globally distributed redundant storage. This means it can be used for the safe preservation of all information that has been acquired by our civilization and that is of permanent interest. It is quite a grand plan.

6 Technical Parameters

Block size: 0.175MB

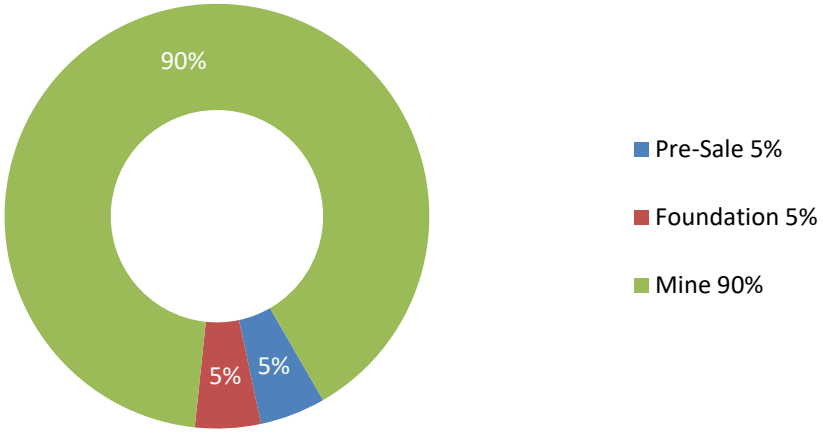
Block generation rate: 4 minutes

Halving cycle: 4 years

Initial TPS: 80 transactions per second

Mortgaged mining: 30 Boom will be held for each T, with a return rate of 95%. Otherwise, the return rate will only be 20%.

Coin Distribution



A total of 210 million chips

Pre-sale: 5% will be used for system development and early promotion.

Foundation: 5% will be generated during the process of mining. It will be used to cover payment generated by marketing, operation, iterative system upgrading and others alike.

---

[1] Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf

[2] Bitcoin – Statistics & Facts, https://www.statista.com/topics/2308/bitcoin/

[3] Countries That Consume More Or Less Electricity Than Bitcoin Mining In Late 2018, https://powercompare.co.uk/bitcoin-mining-electricity-map/

[4] Bitcoin Energy Consumption Index, https://digiconomist.net/bitcoin-energy-consumption

[5] Bitcoin's Growing Energy Problem, https://www.cell.com/joule/fulltext/S2542-4351(18)30177-6

[6] Size of the Bitcoin blockchain from 2010 to 2019, by quarter (in megabytes), https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

[7] Burst Wiki, https://burstwiki.org/

[8] Automated Transactions (AT), http://ciyam.org/at/

[9] Github: libsnark: a C++ library for zkSNARK proofs, https://github.com/scipr-lab/libsnark

[10] Github: Linkable-Ring-Signature , https://github.com/apuljain/Linkable-Ring-Signatures

[11] The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, https://lightning.network/lightning-network-paper.pdfs

[12] Raiden Network , https://messari.github.io/research/profiles/RaidenNetwork(RDN).pdf

[13] The Burst Dymaxion: An Arbitrary Scalable, Energy Efficient and Anonymous Transaction Network Based on Colored Tangles, http://www.burst-coin.org/wp-content/uploads/2017/07/The-Burst-Dymaxion-1.00.pdf