White Paper

Bitcoin Real (BTCR)

Code is law.

This is not a prospectus of any sort

This document and any other documents published in association with this whitepaper relate to a potential token offering (i.e. the BTCR token) to persons (contributors) in respect of the intended development and use of the network by various participants. This document does not constitute an offer of securities or a promotion, invitation or solicitation for investment purposes. The terms of the contribution are not intended to be a financial services offering document or a prospectus. The token offering involves and relates to the development and use of experimental software and technologies that may not come to fruition or achieve the objectives specified in this white paper. The purchase of tokens represents a high risk to any contributors. Tokens do not represent equity, shares, units, royalties or rights to capital, profit or income in the network or software or in the entity that issues tokens or any other company or intellectual property associated with the network or any other public or private enterprise, corporation, foundation or other entity in any jurisdiction.

The token is not therefore intended to represent a security interest.

Index

ABSTRACT

When the great Revolution that is Bitcoin began, the anonymous genius desired to test two parameters - a trustless, decentralized database (a distributed ledger or Blockchain) protected by the everlasting security of cryptography and a robust transaction system capable of sending value across the world without intermediaries.
Yet, the past 9 years have excruciatingly shown the lack of a third missing feature, which brought the community to take action upon this vacancy, ending up with the creation of endless Bitcoin forks or “real” Bitcoins”, such as Bitcoin Cash, Bitcoin Green, Bitcoin Gold, Bitcoin Private and Bitcoin Diamond. All of these coins have been created because of how this third and fundamental feature is missing. Bitcoin lacks innovation. Or rather it has innovation, it simply is extremely slow and cautious, and in the cryptocurrency innovation is moving fast, the fastest possible.
Then, bearing the heavy and preponderant names of “New Bitcoin”, “Decentralized Revolution”, “Cryptocurrency 2.0” and so on, came Ether from the Ethereum Project. The brilliance of the idea of adding a built-in fully fledged Turing-complete programming language to the Blockchain, enabling the creation of Smart Contracts and so further automating the process of moving value was extremely well received, making Ethereum’s crowdfunding event one of the most successful ever. This innovation didn’t come without risks, as the infamous DAO-Hack[1] was executed, leading to a loss of most of the funds from early investors. This then lead to further problems, which can be summarized in this simple statement: Code is law.
The Ethereum Project was split between people who didn’t want to “make money re-appear magically[2]”, thus invalidating the Code is law principle (which was fundamental in a coding-oriented platform) and people who had fears the project would die without the money that was lost. The Ethereum Classic Project was then made, supported by the people who put moral value above money, while the Ethereum Project “created value from nothing” and “rejected any principle for which Code should be considered law, thus potentially invalidating any smart contract running on that platform.
Moral and technical problems affect the top 2 cryptocurrencies of today, giving space to newer cryptocurrencies to leap ahead.

[1] https://www.coindesk.com/understanding-dao-hack-journalists/
[2] https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee

Introduction

Bitcoin Real is a fully decentralized peer-to-peer electronic cash system which supports the latest and greatest technological innovations which are continuously proposed by the community for the community, but which never make it into the Bitcoin “Core” Code, because of the preponderant lack of innovation which afflicts Bitcoin (see ABSTRACT). There is full support and integration of the Proof of Stake 3.0 algorithm, coupled with Masternodes for the highest level of security available to-date. The Block size is augmented up to 64MBs (which is made possible by advanced Blockchain pruning and superior hardware running on Nodes) and the Lightning Network is fully actuated. The mining algorithm is X16R, which is fully ASIC resistant, and so any possibility of a 51% Attack on the network is completely and utterly eliminated, since Masternodes and ASIC resistance make it impossible to control the network.

More experimental and cutting edge features of Bitcoin Real are the revolutionizing Distributed Decentralized Artificial Intelligence (ddAI) which is going to be a cutting-edge Artificial Intelligence running on top of each full node. It will do important tasks such as Double Spending Protection (by using the full potential of big data analysis at which machines currently excel) and will be eventually tasked with communicating between its other instances to modify things such as Block Time, Difficulty and alleviate network congestion on a need basis. It will be fully decentralized and autonomous, not giving any party superiority over the whole network. Once evolved, there are plans on training the ddAI in data centres to make it even more quick and responsive and to give it new features. The last step is that of coordinated Decentralized Autonomous Organization (DAO), run entirely by ddAI.

Another experimental yet revolutionizing is the Graphene Protocol, a highly efficient and extremely promising new technology which could boost the transactions per second of BTCR to almost 100’000[3] (Data

[3] https://bitshares.org/technology/industrial-performance-and-scalability/

lab tests) or also 1.5 Million[4] (1’500’000) (Extremely controlled and experimental data lab tests)
For a quick comparison Bitcoin tops at 7, Ethereum tops at 15/20, Visa tops at 24’000 and Mastercard at 38’000.[5]

Once a BTCR masternode owner you have the ability to cast a vote on what direction you want the coin to move towards. As a community we move together and fulfill objectives chosen together. This is part of the Decentralised Government Platform, which will enable all node operators to vote freely with no censorship nor limit to their ideas and the subsequent expression.

By simply having your wallet online and running you will contribute to securing the network by PoS mining and will receive a reward for doing so. No need for expensive hardware produced by a single powerful entity.

Native implementation in C++ of smart-contracts through peg-chains and drive-chains (such as RSK) will permit the execution of secure and affordable smart contracts, which will be easily coded since no additional knowledge is needed, you can program BTCRs blockchain in your favourite C++ IDE.

Full anonymity is assured by the implementation of the SwiftTX protocol together with Privatesend and future Instantsend, which will also provide full Quantum Resistance.

---

[4] https://steemit.com/blockchain/@andrecronje/cryptocurrency-scaling-ethereum-to-1-5-million-tps

[5] https://steemit.com/cryptocurrency/@cyberblock/top-9-market-cap-blockchains-ranked-in-order-by-transaction-speed-lets-see-where-steem-fits-in

Bitcoin & Bitcoin Forks

Creation

Bitcoin was first created by Satoshi Nakamoto in 2009 as a decentralized peer-to-peer cash system, which had as true and only breakthrough, the implementation of the Proof of Work algorithm as a means of trustlessly securing the decentralized distributed ledger which is the Blockchain.
9 long years have passed since the initial code was wrote, yet substantially it remains the same. The inability of the Core dev teams has created a variety of problems, such as mining electricity costs inflating over even the wildest of expectations. Currently the environmental risks associated to mining Bitcoin are extremely high. The network congestion before the implementation of the Lighting Network was another fault of the Core team, and again sprung up different forks. The same goes for ASIC resistance. All of these problems show the utter inability to adapt to any type of situation of the Core team. Here we will analyze the problems and the subsequent community solutions better.

Motivation

- ASIC predominance and centralization of components required to mine Bitcoin. As of today, the only way to mine Bitcoins is through *Application-Specific Integrated Circuits* (or ASICs). These are produced by big factories and are sold at a prohibitive price. The main producers (Bitmain,Bitfury) could decide to execute a 51% attack if they wanted to produce as many as they needed. These concerns have been heard by the BitcoinGold (BTG) dev team, which have implemented an ASIC-resistant algorithm, Equihash, and removed SHA-256.

(Currently Equihash isn't ASIC resistant anymore, and we have seen a variety of 51% Attacks being executed on the network. A solution we have proposed will be discussed later on.)[6]

- Low Throughput of about 3-4 (theoretical max of 7) Transactions per Second (TPS). This problem has been around for a long time, and has evolved in the endless debate of bigger-blockers vs off-chainers. Bigger Blockers want to increase the Block size of Bitcoin, effectively making the TPS higher, but making the storage and computation power required more performant, while off-chainers look for scalability options off-chain, through sidechains or coloured coins (Lighting Network). The debate has sprung two different cryptocurrencies, BitcoinDiamond (BCD) and BitcoinCash (BCH).
- High Usage of Electricity because of PoW mining. The process of "mining" or securing the Blockchain was first used by Satoshi Nakamoto in 2009, and answered the concerns over security and decentralization which previous attempts at cryptocurrencies (Wei Dai's b-money and the computationally intensive HashCash). As thoroughly demonstrated Proof of Work is an unexploitable way to secure a network over Ddos or spam attacks, but requires an immense amount of electricity to execute its function, creating a scaling issue over time and difficulty. Currently all Bitcoin mining consumes 70.25 TWh of energy, or almost as much as Chile. This poses big problems looking to the future and so it has been advocated for a change in the securing method, from Proof of Work to Proof of Stake. This concern has been addressed by the popular BitcoinGreen (BITG) fork.
[7]

Inefficiencies and Failures

Whereas it is difficult to analyze where exactly these coins have failed, we can all say that they only took into consideration a single failing aspect of Bitcoin and made it better. This may be considered the only proper failure which all these Forks have in common.

[6] https://cryptovest.com/news/zencash-zen-the-next-victim-to-51-attack/
[7] https://digiconomist.net/bitcoin-energy-consumption

The solution we have found was to analyze all of these popular forks and come up with an Ultimate Solution, which we then dubbed Bitcoin Real.

Bitcoin Real

Philosophy

Bitcoin Real follow the much debated and controversial statement “Code is Law”, which divided Ethereum for instance, and which was mostly explored by Lawrence Lessig, known American academic, attorney, and political activist, who worked for years in this space.

Here is a small snippet of one of his “Basic Books” introductions, fundamental works of his which are important to understand the whole concept of a “Code == Law” deterministic approach.

“Every age has its potential regulator, its threat to liberty. Our founders feared a newly empowered federal government; the Constitution is written against that fear. John Stuart Mill worried about the regulation by social norms in nineteenth-century England; his book On Liberty is written against that regulation. Many of the progressives in the twentieth century worried about the injustices of the market. The reforms of the market, and the safety nets that surround it, were erected in response.
Ours is the age of cyberspace. It, too, has a regulator. This regulator, too, threatens liberty. But so obsessed are we with the idea that liberty means "freedom from government" that we don't even see the regulation in this new space. We therefore don't see the threat to liberty that this regulation presents.This regulator is code--the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned. It affects who sees what, or what is monitored. In a host of ways that one cannot begin to see unless one begins to understand the nature of

this code, the code of cyberspace regulates.This regulation is changing. The code of cyberspace is changing. And as this code changes, the character of cyberspace will change as well. Cyberspace will change from a place that protects anonymity,free speech, and individual control, to a place that makes anonymity harder,speech less free, and individual control the province of individual experts only."[8]

Creation and Motivations

Bitcoin Real was created as an answer to the demands of the Community of Bitcoiners which felt betrayed and not represented by the Bitcoin Core Dev Team. But not as a localized answer to a certain demand, but as a universalistic approach to the needs of the users of the platform, which should ALWAYS be able to say their own opinion, and that opinion should be ALWAYS listened to. This principle is written in the code, and Code is Law.
By doing so an authentic democratic approach to the cryptocurrency model was finally made possible, and Bitcoin Real is a truly decentralized alternative to Bitcoin.

Challenges

- Reduce all energy consumption needed as a means of verifying and securing the network to a much lower value, as proposed by the Bitcoin Green (BITG) developers.
- Create a truly ASIC-resistant eco-system in which miners can afford hardware which doesn't come from only one manufacturer, as proposed by Bitcoin Gold (BTG) dev teams.
- Reach high throughput of transactions-per-second (TPS) by implementing bigger blocks (as proposed by the Bitcoin Cash (BCH) developers) and side-chains (as proposed by the Bitcoin Diamond (BCD) devs)

[8] http://code-is-law.org/

Solutions

1) Staking

The implementation of PoS 3.0 coupled with Masternodes would mean cutting energy costs down a significant notch, and PoS 3.0 being the latest and most secure iteration of the Proof of Stake algorithm, as reported by the latest BlackCoin report. As said before, Proof of Stake is not a flawless verifying system for securing the network;
“the whole purpose of holding competitions for coins is to avoid attacks. Confirmation of transactions is an honor given to the winner of a block. However, if this system can be gamed, then it is flawed.

In Proof of Stake, you first prove you have access to coins and from that point you can compete to win blocks randomly. The more people competing the more secure the block. Coin age is the idea that the longer you hold coins the higher the probability you can win a block. It's original intention was to incentive dormant holders of coins. However, this does not encourage a node to stay connected to the network in practice since they can wait for the reward to increase. Also, shareholders can disconnect from the network for long periods of time, then reconnect and win enough blocks to risk a 50% attack on the network. The time calculation will effect payouts discouraging connectivity. Also, the fewer the nodes that are connected, the easier it is to gain a majority of the blocks forging consensus. Also, stakes can be computed in advance to make the attack more effective. Timestamps are used in Proof of Stake to get a general idea of time. Drift calculations are used to prevent forging erroneous timestamps.

In Proof of Work, a difficulty increase or decrease is made depending on how quickly a block was produced.

However, as a precautionary method to prevent any sort of "Timing Attacks" Proof of Stake coins use centralized checkpoints.”

Thus we are left with a few parameters we can configure to our liking, to try and bring a better Proof of Stake to the network.
These are:

A) Coin age

Coin Age is calculated by the weight of unspent coin and the time they have been dormant. The calculation is simply "proofhash < coins · age · target" The proof hash is the hash of an obfuscation sum that depends on a stake modifier, the unspent output, and the current time. The attack of saving up Coinage was previously outlined as improbable. The reasoning behind this is because it is very difficult to perform consecutive double spending since Coin-Age would reset after the first expense. However, this is not entirely clear because an input can be split into 1000s of outputs. This may give the possibility for consecutive double spend attacks. However, this is still a difficult problem because the attacker would need a significant amount of funds to hold weight greater than the network. In theory, this makes sense. However, if we look at the amount of forks of Blackcoin and other popular POS systems, we can see the amount of nodes are fairly low and this gives much greater weight to a smaller handful of nodes. A holder of many coins may not want to perform this attack since they run the potential of losing value of their share if detected. However rational this may seem, it is probably a fallacy because it is still an attack vector and a very real one indeed. More importantly, with so many coins being published daily, keeping as many nodes connected as possible is imperative to security. Solution from Proof of Stake 2.0: Remove Coinage from the equation - "proofhash < coins · target".

B) Blockchain pre-computation

The block timestamp is key to the Proof of Stake system. It is possible in theory to fork a coin by changing previous timestamps. The stake modifier does not obfuscate the hash of sufficiently to prevent knowing future proofs. So an attacker can attempt to compute all of the blocks in advance and run a higher probability to forge multiple consecutive blocks. Solution from Proof of Stake 2.0: The stake modifier is changed at every modifier interval to better obfuscate any calculations that would be made to pinpoint the time for the next proof-of-stake. The expected block time was increased from original 60 seconds to match the granularity.

This equates to:

Past limit: Time of last block
Future limit: +15 seconds
Granularity: 16 seconds (effectively increased from 1 second)
Expected block time: 64 seconds

C)Block Reward

The Block Reward in most Proof of Stake systems is unfortunately based on Coin Age. In theory, this is to distribute interest fairly by allowing nodes to receive latent payments due. It is an attempt to keep a common APR. However, this system does not work because nodes can stay disconnected and with many split inputs, reconnect to the network and game the reward system. Also, it does not give nodes any incentive to stay connected. In a decentralized system, the more nodes connected the better the security since it shifts trust from a single entity to the network itself. Solution from Proof of Stake 3.0: The block reward was made a constant 1.5 coins per block. This was based proportional to the supply of coins maintaining interest at %1.

Another key feature in PoS 3.0 is the introduction of MultiSig staking, which permits staking from a multiple number of keys, thus enabling more advanced features for exchanges and users, all for a richer and greener eco-system.[9]

[9] https://bravenewcoin.com/assets/Whitepapers/Blackcoin-POS-3.pdf

2) Mining

A necessary feature of every cryptocurrency which wants to be considered decentralized is ASIC Resistance. This subject has been touched many times, but it appears inevitable that some ASIC will be eventually developed for a certain Algorithm. BTC forks which enabled “ASIC-resistant algorithms” like Bitcoin Gold have had their network compromised and subject to a 51% attack. The algorithm used, Equihash, was once considered resistant, but is now worthless. The same happened for Dagger-Hashimoto Ethash, and the famous CPU intensive Cryptonight.

The latest innovation has been the X16r algorithm, a blend of randomly sequentialized 16 algorithms, including

cubehash
shabal
blake
echo
simd
bmw
hamsi
shavite
luffa
whirlpool
groestl

and more. Taken from the official whitepaper:

“...Another approach is to use a sequence of hashing algorithms where the output of one becomes the input to the next. Dash, formerly DarkCoin, took this approach with their X11 algorithm. X11 uses eleven chained hashing algorithms in an effort to thwart the 1 move to ASIC mining. This approach worked for a while, but several manufacturers now produce ASIC miners for X11. The concept behind X11 can be extended to additional algorithms. For this reason, some coins use X13, some X15, and even X17 which chains seventeen hashing algorithms. The fixed order of hashing algorithms lends itself to the construction of ASICs. While chaining more algorithms together adds difficulty in constructing an ASIC, the X13, X15, and X17 all use the same ordering of hashing algorithms as the X11. This is likely to

lead to faster manufacturing of ASICs for these algorithms as manufacturers only need to extend their existing design to accommodate the additional hashing algorithms.

The X16R algorithm intends to solve this problem by constantly disrupting the ordering of the hashing algorithms. The hashing algorithms are the same proven algorithms used in X15 + SHA512, but the ordering is changed based on the hash of the previous block. This reordering does not make an ASIC impossible to build, but it does require that the ASIC adapts to additional input, which is more easily accomplished by a CPU or GPU. The reordering also prevents a simple extension of the current X11 ASICs or future X15 ASICs.

The X16R hashing algorithm consists of 16 hashing algorithms operating in chain fashion with the ordering dependent on the last 8 bytes (16 nibbles) of the hash of the previous block.

The algorithms are as follows:
0=blake 1=bmw 2=groestl 3=jh 4=keccak 5=skein 6=luffa 7=cubehash 8=shavite 9=simd A=echo B=hamsi C=fugue D=shabal E=whirlpool F=sha512

Example:

Previous Block Hash:
00000000000000000007e8a29f052ac2870045ae3970270f97da00919b8e86287 The final 8 bytes:
0x7da00919b8e86287
Each hex digit (nibble) determines which algorithm to use next.

cubehash -> shabal -> echo -> blake -> blake -> simd -> bmw -> simd -> hamsi -> shavite -> whirlpool -> shavite -> luffa -> groestl -> shavite -> cubehash

Some of the hash algorithms take longer than others. This time differential tends to average out across the 16 algorithms while mining each block. The test platform for this mining algorithm is Raven (RVN). Raven was launched on January 3, 2018, the 9th year anniversary of Bitcoin's launch.

Raven changes the issuance schedule, block time, and mining algorithm. Raven is the reference implementation for X16R, which defines the number of algorithms, the specific hashing algorithms used, the order of the algorithms, and the order of and bytes used from the previous block hash. The concepts

behind X16R could be extended to include Scrypt, Equihash, and other ASIC resistant algorithms to continue to allow anyone with an idle computer to participate in mining with off-the-shelf hardware.

The ordering of the algorithms can easily be changed for each coin in order to dissuade hardware manufacturers from building ASICs for an entire class of coins as with X11."[10]

This type of innovation is extremely interesting and advanced, and will be the core idea which drives Bitcoin Real forwards.

3) Scalability

Scalability has often been approached, mainly through two roads; the off-chain and the on-chain method.

The off-chain method involves calling in a secondary chain (a peg-chain or drive-chain) which acts as a payment-gateway for two people. This is how the famous Lighting Network works.

The on-chain approach is slightly different and involves augmenting the Block Size, pruning the Blockchain and lowering the block-time.

The debate on these two different type of approaches still rages on, and a 50/50 ratio of Bitcoiners support one or the other.

Faithful to what we said earlier, Bitcoin Real listens to everyone's opinion and will be scaling the Block Size up to 64MB, while implementing the latest stable release of the Lighting Network.

Vision

[10] https://ravencoin.org/wp-content/uploads/2018/03/X16R-Whitepaper.pdf

Here at Bitcoin Real we live for a cryptocurrency which will uplift people from their current financial slavery and permit them to be the real owners of their own money. The core idea, Code is Law, will always be respected and honoured, and everything which come from it will be respected and honoured, since it’s the only possible way to institute a true democracy based upon true values and real freedom.

Long Term Objectives (LTOs)

Our long term objectives are various and very ambitious, here are a few we particularly want to develop towards.

Transactions-per-second are key for our vision. We are going to integrate advanced data compression tools to achieve ultimate TPS ratio. We have scaled to 100’000 in our lab, but we can certainly do more.

ddAI, or Distributed Decentralized Artificial Intelligence, will be continuously trained to achieve maximum use case and functionality, by training neural networks in big data-centres.

Miscellanea and Concerns

Security

The underlying technology of Bitcoin Real, the blockchain, has been proven to be most secure when paired up with a hybrid network of PoS + PoW, when that network has Masternodes, when the algorithm used for PoS is Quantum Resistant and the algorithm used for PoW is ASIC resistant. Bitcoin Real checks all the boxes.

And adds some others...ddAI will run on top of each node and will double check transactions and eventually control mining difficulty and subsequent block time.

Graphene Protocol

The new experimental protocol for massive tx/s will be included in Bitcoin Real.
Unlike other approaches, Graphene never sends an explicit list of transaction IDs.
Instead it sends a small Bloom filter and a very small IBLT. The intuition behind Graphene is as follows.

The sender creates an IBLT I from the set of transaction (txn) IDs in the block. To help the receiver create the same IBLT (or similar), he also creates a Bloom filter S of the transaction IDs in the block.

The receiver uses S to filter out transaction IDs from her pool of received transaction IDs (which we call the IDpool) and creates her own IBLT I ' .

She then attempts to use I ' to decode I, which, if successful, will yield the transaction IDs comprising the block.

The number of transactions that falsely appear to be in S, and therefore are wrongly added to I ' , is determined by a parameter controlled by the sender.

Using this parameter, he can create I such that it will decode with very high probability.
In sum, the Bloom filter from the sender allows the receiver to determine which transactions from its mempool are in the block. Other approaches require a much larger Bloom filter to keep the false positive rate small; in Graphene, the Bloom Filter FPR is high because the IBLT recovers any mistakes made. Similarly, if only the IBLT was used, it would be much larger than our use of the two mechanisms.

A Bloom filter is an array of x bits representing y items.
Initially, the x bits are cleared. Whenever an item is added to the filter, k bits, selected using k hash functions, in the bit-array

are set. The number of bits required by the filter 1 is x = y - ln(f) ln2 (2) , where f is the intended false positive rate (FPR). For Graphene, we set f = a m-n , where a is the expected difference between I and I ' .

Since the Bloom filter contains n entries, and we need to convert to bytes, its size is - ln(a m-n) ln2 (2) 1 8 . It is also the case that a is the primary parameter of the IBLT size. IBLT I can be decoded by IBLT I ' with very high probability if the number of cells in I is d-times the expected symmetric difference between the list of entries in I and the list of entries in I ' .

In our case, the expected difference is a, and we set d = 1.5. Each cell in an IBLT has a count, a hash value, and a stored value. (It can also have a key, but we have no need for a key).

For us, the count field is 2 bytes, the hash value is 4 bytes, and the value is the last 5 bytes of the transaction ID (which is sufficient to prevent collisions). In sum, the size of the IBLT with a symmetric difference of a entries is 1.5(2 + 4 + 5)a = 16.5a bytes.

Thus the total cost in bytes,T , for the Bloom filter and IBLT are given by
T (a) = n - ln(f) c +aτ = n - ln(a m-μ) c +aτ ,

where all Bloom filter constants are grouped together as c = 8 ln2 (2), and we let the overhead on IBLT entries be the constant τ = 16.5. To set the Bloom filter as small as possible, we must ensure that the FPR of the filter is as high as permitted. If we assume that all inv messages are sent ahead of a block, we know that the receiver already has all of the transactions in the block in her IDpool (they need not be in her mempool).

Thus, μ = n; i.e., we allow for a of m - n transactions to become false positives, since all transactions in the block are already guaranteed to pass through the filter.
It follows that

T (a) = n - ln(a m-n) c + aτ . (1)

Taking the derivative with respect to a, Eq. 1 is minimized when when a = n/(cτ). Actual implementations of Bloom filters and IBLTs involve several (non-continuous) ceiling functions such that we can re-write:

T (a) = * , ⌈ln(m - n a)⌉
n ln(m-n a) ⌈ln(m-n a)⌉
ln2 (2) + - 1 8 + ⌈a⌉τ . (2)

The optimal value of Eq. 2 can be found with a simple brute force loop. In practice, a for-loop brute-force search for the lowest value of a is almost no cost to perform, and we do so in our simulations. Due to the randomized nature of an IBLT, there is a very small but non-zero chance that it will fail to decode.

In that case, the sender resends the IBLT with double the number of cells (which is still very small).

In our simulations, which encoded real IBLTs and Bloom filters, this doubling was sufficient for the incredibly few IBLTs that failed.[11]

This approach has permitted to reach almost 100k tps in lab tests

Proof of Reputation (PoR)

Reputation is everything in every business. Getting a good reputation level in market consumes a lot of years, but a business can lose the same reputation in seconds that had been earned in years. Cryptocurrency like every business also depends on reputations.

Each project or coin gains market traction based on its team, idea, reliability and most importantly profile of its miners.
So, many Crypto coins are adopting proof of reputation, because it is the best way to increase up the reputation level of a coin.

Basically, Proof of reputation is linked with miners' reputation; so, in proof of reputation, firms of Cryptocurrency distribute/award coins among the miners with respect to their reputation level. For the best reputation level, a miner must have a clean chit in his professional career; for example, he shouldn't have been involved any hacking case, miner should have a proper updated personal computer (PC), and he must be loyal with the coin.

A miner which is loyal to the coin will be rewarded by a randomly augmenting or decreasing reward at every block, making it difficult

[11] https://people.cs.umass.edu/~gbiss/graphene.pdf

for him to stop mining the coin, because maybe the next block will be worth a lot. This system, which reminds many of gambling, is in place to prevent miners from coin hopping and to avoid hasrate fluctuations.

Advanced technology doesn’t ease only miners in terms of mining, but it also helps miners in producing more new coins or verifying more transactions. With updated versions of PCs, miners will be able to do enough verification of transactions that will also help in uplifting the reputation level of coin.

In, proof of reputation, organizations of Crypto coins award miners as per their profiles’ reputation. Miners must concentrate on their profiles, because these profiles don’t only show up their reputation level, but these are also revealing the exact reputation level of a coin.
Proof of reputation is a secured and an effective way for crypto coins to get high reputation in the market. Proof of reputation is very secured; advanced computers will keep secure the miner’s data as well as mining process. Mining process will be done quickly as miners are using updated versions of personal computers; they are kept concentrated upon their profiles’ reputation, their profiles also have clean chit, and the most important is that chain of algorithm is also being processed without any fluctuation because miners are tirelessly avoiding any kind of errors as they are using updated PCs with heavy anti-virus software.

So, Proof of reputation is clearly helping coins in getting respected reputation level in the market; moreover, it is an effective way of getting enough mining done without any flux. Verification of transactions is also done quickly by the miners, so that users of a coin are satisfied with it.

Miners should do mining or verification with the advanced personal computers, because it will not only give them enough bonuses/rewards, but it will also ease them in terms of doing mining or verification as updated PCs will never get hanged with the chain of algorithm.

Proof of Loyalty (POL)

Loyalty means to be a strong supporter of anything. Every business needs loyal customer/user for its running in the market. You can understand it better with the following example.

Example; Uber gives a kind of referral message to its users through which its loyal users invite other people or ask other people to join Uber. After sending invitations, whoever accepts the invitation, the referral gets some discount in its user ID.
The same is being done in Cryptocurrency with the name of Proof of Loyalty; many Crypto coins gives a referral message to its users by which they invite other users and then these loyal users get some extra coins.

Proof of loyalty plays a vital role in increasing the coin's circulation, usage, supply, and number of investors or traders. A kind of waves address is send to the referral of coin after which he can redeem his free coins.
A referral link may look as below;

3P2UGNo2PRM7NoXE23hJezjEsAPF3P2UGNo2PRM7NoXE23hJezjEsAPFQbHmM2xQbHmM2x

Conclusions

By using a hybrid, ASIC resistant PoW + PoS + PoR + PoL network with the addition of Masternodes, having an extremely high potential TPS of 400'000, and bringing in new features such as ddAI and the experimental Graphene Protocol, with extreme privacy options such as ZK-Snarks, Bitcoin Real is positioned as one of the most innovative cryptocurrencies to be ever developed, and will surely bring some fresh air to the ageing Bitcoin.

References

https://github.com/ethereum/wiki/wiki/White-Paper

https://cyber.stanford.edu/sites/default/files/kadenachainweb-bpase18.pdf

https://bravenewcoin.com/assets/Whitepapers/Blackcoin-POS-3.pdf

http://code-is-law.org/

https://ravencoin.org/wp-content/uploads/2018/03/X16R-Whitepaper.pdf

https://cyber.stanford.edu/sites/default/files/bpase18_master.pdf

https://cyber.stanford.edu/sites/default/files/bpase_porep.pptx

https://cyber.stanford.edu/sites/default/files/hardening_lightning_updated.pdf