(Draft version 2.0)

The blockchain is an undeniably ingenious invention – the brainchild of a person or group of people known by the pseudonym, Satoshi Nakamoto. But since then, it has evolved into something greater. By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. Originally devised for the digital currency, Bitcoin, the tech community is now finding other potential uses for the technology.

Cryptocurrencies are digital asset designed to work as a medium of exchange that uses cryptography to secure its transactions, to control the creation of additional units, and to verify the transfer of assets. As opposed to conventional money transfer and banking systems in which centralized control is owned by a single party, cryptocurrency uses a decentralized structure.

The control of each cryptocurrency works through a blockchain, which is a public transaction database. The blockchain functions as a distributed ledger, making counterfeit cryptocurrency impossible.

Cryptocurrencies have emerged as the latest brave market in the trading world. These trading markets are relatively young and thus full exploitation has not yet been achieved. The fact that some

coins like Bitcoin can rise by 10% in a single day signifies the need for other stable coins to join the market. The tender age cryptocurrency in the trading world has prevented the established trading houses and only left the young companies to invest. Some years back, the market capitalization for cryptocurrency stood at $80 bn and still growing. This further signifies the availability of opportunities for young traders to venture in the market and make profit.

What is Proton?

PROTON is a fully decentralised cryptocurrency built on the premise of providing anonymity, speed, fair mining by being ASIC-resistant and reliability by the usage of Masternodes. By using the PrivateSend feature you can send coins in a safe and private manner. So long as anonymity is not the option you are looking for Proton offer InstantSend, that enables almost-instant transactions in our network.

COIN SPECIFICATIONS

Coin Name PROTON Coin

Coin Abbreviation PROTON

Coin Type PoW

Proton Block Time 120 seconds

Hashing Algorithm X16R

Block Reward 50 coins per block decreasing by ~10% every year

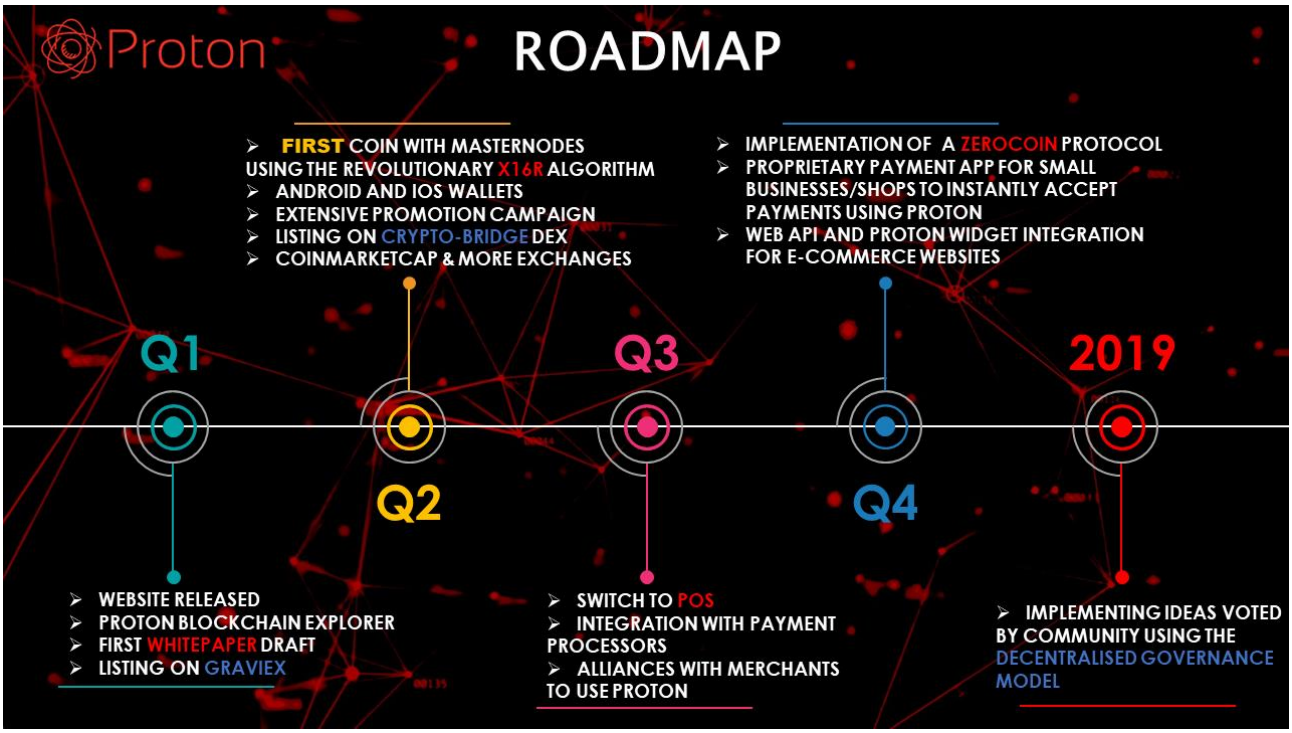
Max Supply 45.000.000

Masternode Reward 85% Block Reward

Masternode Collateral 5000

Premine 1.000.000

PROTON ROADMAP



PROOF OF WORK

“Proof of Work”, as its name implies, requires that the decentralized participants that validate blocks show that they have invested significant computing power in doing so. In bitcoin, validators (known as “miners”) compete to process a block of transactions and add it to the blockchain. They do this by churning enough random guesses on their computer to come up with an answer within the parameters established by the bitcoin program.

The main innovation that Satoshi Nakamoto introduced in his article is using so-called proof of work (POW) to create distributed trustless consensus and solve the double-spend problem. POW is not a new idea, but the way Satoshi combined this and other existing concepts—cryptographic signatures, merkle chains, and P2P networks—into a viable distributed consensus system, of which cryptocurrency is the first and basic application, was quite innovative.

Proof of work is a requirement that expensive computations, also called mining for reasons which later will become clear, be performed in order to facilitate transactions on the blockchain. To understand the link between computational difficulty and trustless consensus within a network implementing a distributed cryptocurrency system is a serious mental feat.

WHY IS ASIC RESISTANCE IMPORTANT?

Bitcoin uses the SHA-256 hashing algorithm, which has now been around for many years and the algorithm hasn’t been changed since its genesis. This means that large hardware companies have created ASICs in order to mine at a very high rate compared to those who mine with their GPUs (graphics cards) and CPUs (processors) at home. As a result of this, the cryptocurrency’s difficulty increases and means that GPU mining isn’t profitable for many people. Therefore, people stop mining and the large companies control a lot of the hash power. A large amount of hashing power

in the control of one entity can mean the network isn't decentralized and therefore create 51% attacks.

DIFFERENCE BETWEEN SHA256 AND X16R ALGORITHMS

The history of hashing for cryptocurrencies began with SHA256 for Bitcoin, then Scrypt for Litecoin, Ethash for Ethereum, X11 for Dash, followed by X13, X15, and X17. X16R is the next step in this evolution to find a better mining algorithm.

The reason for the algorithm changes is to minimize the impact of purpose-built hardware on the mining ecosystem of the coin. Bitcoin was originally intended to be mined by computers everywhere. As the value of bitcoin increased, it became advantageous to mine in parallel on hardware designed for parallel processing, so the mining moved to Graphics Processing Units (GPUs). As the economic value of mining further increased, it became economically viable to use programmable hardware in the form of Field-programmable Gate Arrays (FPGAs), which had an advantage over CPUs and GPUs. The next step was to build custom chips that are purpose-built for mining. These Application Specific Integrated Circuits (ASICs) were able to dominate the competing technologies and made it impractical to mine any other way. The last, and likely final, iteration for Bitcoin mining is the move to faster and more energy efficient ASIC hardware.

The unfortunate side-effect of this transition to ASIC hardware is the centralization of mining. While anyone can order these ASICs, there is an advantage to being near the manufacturing facility as shipping time is reduced. Additionally, access to cheap electricity is a priority, as the electricity used is the variable cost of the mining operation. This has led to some centralization of mining in China because of the proximity to ASIC development and the availability of inexpensive electricity in some provinces.

One solution to minimize the impact of ASIC miners is to use a memory intensive

hashing algorithm. This is the approach of Scrypt, used by Litecoin, and Equihash, used by ZCash. These two algorithms have reduced the impact of ASICs. While there are some ASIC miners for Scrypt, the relative advantage over GPUs is negligible. There are currently no ASIC miners for Equihash.

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

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.

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

MASTERNODES

A Masternode is simply a node that keeps a full copy of the blockchain in-real time. It is active 24/7, and is always interacting with other nodes to make a fully stable and performing decentralized network.

Masternodes can:

- Increase transaction privacy
- Allow instant send
- Participate in governance/voting
- Enable budgeting and treasury system

Running a Masternode helps the network throughout, as there will always be a stable node, with multiple connections around the world, running. As a reward for hosting one of these Masternodes, PROTON will be paid to your wallet on a recurrent basis.

Masternodes are a section of the infrastructure of a certain group of cryptocurrencies. They are computer servers and provide services to cryptocurrency users. Masternode coins were developed so as to give the coin owners more control and more yield. One way that Masternode generates is yield is by offering services to the crypto currency infrastructure.

Proton Coin community is to manage and run the proposals that helps in stabilizing and increasing the value of a currency if the governance system is introduced. In Masternodes, the proposals can be made by any person unlike other coins who charge a proposal fee and this makes Masternode a favorite among investors. After proposals are submitted, a vote is made by master node holders and proposal is voted in. The Masternode system utilizes people’s competitiveness and creativity to get ideas of improving the coin. The best ideas are generated from proposals submitted by coin holders. These ideas improve the currency value which in turn increase the block reward.

Investing in Masternode coins gives you the ability of not only being an investor, but part of the decision makers in shaping the coin advancement. Owning own gives a voice to an investor and makes it more than just money. This is done through submitting proposals. The foundation of Masternodes is stable and has long term values at the core of the infrastructure.

The founding investors have committed their money for a long term making it stable and increases trust among investors. Investors get capital gains by just running the Masternode services. On top of that, investors are paid in that coin as rewards from each block found.

The availability of a stronger community guarantees the long-term sustainability of the crypto project. This in turn ensures that energy is focused on the project's long-term future instead of pump and dump cycles.

WHAT DO YOU NEED TO RUN PROTON MASTERNODE?

- Collateral: 5000 PROTON
- A VPS or a server to host the wallet 24/7
- A dedicated IP address
- Some storage space to keep a copy of the blockchain

In order to ensure that the MN owner doesn't cheat or corrupt the system, a collateral becomes necessary, as the operator needs has something at stake in the environment. We decided to set this collateral as 5000 PROTON, as computed with the total supply and blocks in the code.

CONCLUSIONS

Proton Coin is recently borned yet has made a lot of progress. Tremendous steps have also been made in throughput, network stability and marketing. PROTON will be listed on more exchanges soon. Each day PROTON closes to consensus swap from POW to POS. In a Proof-of-Stake system, the coin holders get paid transaction fees for validating transactions. Therefore, Proof-of-Stake creates a clear and unambiguous economic incentive to hold coins for the long term. The price of the coin can be analyzed based on the expected future cash flows, which are generated in the form of network transaction fees. Essentially, a POS blockchain can be thought of as a decentralized Visa / Mastercard with all the additional distributed ledger functionality supported by the specific implementations. This is important, because a Proof-of-Stake coin value can be supported by traditional value arbitrage investing. A POS coin in a functioning network cannot be valued for too long below the present value of the cash flows generated by the network, similarly to any other cash flow producing asset—thus generating stability and dampening volatility, which in turn means POS coins should be better store of value than their POW competitors.