SUPERMOON

Peer-to-Peer Crypto-Currency secured via Proof-of-Stake, with APR% rewards based on Phases of the Moon in Real Time

SUPERMOON is a digital crypto-currency with a unique approach to Proof-of-Stake APR% rewards. Each stake return is a variable Annual Percent Reward (APR%) calculated against the occurring four primary Phases of the Moon in REAL TIME. SUPERMOON also has a bonus system for key Stellar Events.

Moon phases and stellar events are calculated and tracked to trigger in real time based on UTC (Coordinated Universal Time). Moon phases and Stellar events rewards stack to award relative value APR% for each wallet competing for Proof-of-Stake block rewards, again calculated in real time.

Author: David Chapman (crypto@supermooncoin.com)

November 4th, 2018

Contents

Abstract 3

Idea 4

Real Time Variable APR% Rewards 6

Current cryptocurrency market problems 7

High transaction costs 7

Proof-of-Stake 8

Coin Age 9

Fairness for Proof of Stake Rewards 10

Proof of Stake Version History 12

PoSv1 12

PoSv2 12

PoSv3 12

SUPERMOON Proof of Stake 3.5 13

Algorithms of consensus 15

Max Coin Supply ... 16
Block Generation under SUPERMOON Proof-of-Stake 3.5 ... 17
Main Chain Protocol ... 18
Security ... 18
Encryption ... 19
Checkpoint: Protection of History ... 20
Block Signatures and Duplicate Stake Protocol ... 20
Energy Efficiency versus classic bitcoin rewards system ... 20
Coinage History and Wallet Locking exploit ... 22
Repository on GitHub ... 22
Areas of Application ... 23
Infrastructure Services ... 23
For Customers ... 23
For Business ... 24
FUTURE API ... 25
Other Considerations ... 25
Conclusion ... 26
The first stage ... 26
The second stage ... 27
Acknowledgement ... 27

Abstract

A peer-to-peer crypto-currency design based on Satoshi Nakamoto's Bitcoin, but the security functions of "Proof-of-Stake" (PoS) replaces the high energy wasteful and extremely high costs associated with using Bitcoin's original "Proof-of-Work" (PoW) functions to provide most of the network security and block generation to keep the coin mechanics and transactions progressing onwards.

SUPERMOON follows, ***in Real Time***, the four primary phases of the moon's monthly cycle to variably switch the APR% return to set the block reward for each approximate seven-day phase.

SUPERMOON links the real world to digital crypto currency, in a way that is unique. With the moon visible worldwide to all residents regardless of location, we all see the same Moon, with the same Moon phase, just be-it seen from different locations across the surface of our Earth.

SUPERMOON was conceptually authored by David Chapman to spark the idea and new concepts for crypto currencies, by using the Proof-of-Stake system principles to make it possible to link the Real World to an untypical digital crypto-currency environment

Under this unique hybrid reward design and original approach using Proof-of-Stake mechanics to facilitate the crypto currency coins functions, although the coin still requires an initial Proof-of-Work phase which mainly provides a basis to produce the initial minting of a number of coins, which is essential for the start for the creation of coin process, but the Proof-of-work phase becomes non-essential and is disabled after the start of the Proof-of-Stake engine phase can keep the transaction block creation engines working full time.

Security level of the network is therefore not dependent on large energy consumption and computing effort once the Proof-Of-Work has provided the initial minimum required base coinstake to guarantee that the Proof-of-Stake can maintain the mining reward mechanics being driven continually thus providing an energy efficient and more cost-competitive peer-to-peer crypto-currency.

The project is named: ***SUPERMOON™ (SUPM ™) Coin.***

Idea

SUPERMOON tracks the four primary phases of the moon's monthly cycle and awards bonuses against Stellar events which all variably switch the APR% return to set the block reward for each approximate seven-day phase in the case of phases of the moon, and timed to the second occurring Stellar events, all in Real Time.

In principle, when wallet's SUPERMOON balance is unlocked to participate in the Proof-of-Stake network, when you personally look at the moon and see the current phase, this acts as a continual reminder of exactly what APR% reward your coin stake has a chance to reward.

Also, outside of the regular phased of the moon reward cycle, a bonus reward system is used for stellar events to add further interest and stimulation to the constant set reward principles. Stellar events are also calculated by SUPERMOON against well-known, regular or one-off Stellar events have also been timed and calculated to be tracked: Meteor shower peaks, Planetary transits, annual periodic key events such the Equinox and Solstices all have variable rewards, with the highest rewards are gained via Solar & Lunar Eclipses, Blue Moons and of course the rare SUPERMOON and New SUPERMOON, again all occurring and tracked in real time.

At the time of publishing, times for the four phases of the moon, and key stellar events occurrences and their timed thresholds versus the APR% reward is calculated into the SUPERMOON's Proof-of-Stake engine up to Jan 2020 (published via the http://SUPERMOONCOIN.com/calendar webpage).

The Phases of the moon are approximately seven-day long cycles across a lunar month: New Moon, Half Moon, Full Moon and then back to half Moon. Each Moon phase is tracked by SUPERMOON over a lunar 'week' and is timed to follow and award a variable block reward rate of APR% return. Each moon phase is calculated starting from the beginning of the first minute of the occurring phase.

The variable % block reward return is based on chance of a wallet stake wining the reward from participation in the network's Proof-of-Stake; Each reward is calculated from actual staked amount versus the phase of the moons assigned APR% reward based on real time calculations. The Proof-of-Stake real time calculation is itself derived and based on the last minted timestamp function of the maximum height of the blockchain. So, with block-time spacing set at about one minute, and the actual blocktime reward averaging at approximately *50* seconds, the comparison in Stellar terms responds in real time.

- Stellar Events source: NASA.gov : https://eclipse.gsfc.nasa.gov/SKYCAL/SKYCAL.html
- All timed events are calculated against published time calendar, and the common time used is based on Universal Time Calculation (UTC).
- All SUPERMOON events are all published on http://www.supermooncoin.com

SUPERMOON's Proof-of-Stake mechanics are based on a variation of coin age calculations for an ever increasing weight elevating the chance of the winner for each proof of stake block reward, but rewards are based on actual SUPM amounts staked to the network versus variable APR% (annual percent return percentage), rewards calculated based on block time against phases of the moon and stellar events providing bonuses % (which stack on occurrence), again all calculated based in REAL TIME principles.

The APR % rewards and multiplied via the actual amount of SUPM staked, but **without** a return reward accounted for via the coin age history (CoinAge).

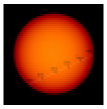
The removal of coinage history from the bonus reward forces participation in the global network by all wallets competing for Proof-of-Stake rewards.

Real Time Variable APR% Rewards

The Moon has four major lunar phases which cycle constantly for 52 lunar weeks annually. Each primary moon phase has the following standard repeating block rewards:

	Full Moon stake reward is calculated against:	**500% APR**
	Half Moon's stake rewards are is calculated against:	**200% APR**
	New Moon stake reward is calculated against:	**100% APR**

SUPERMOON reacts with bonus APR% for various Stellar events for shown periods:

	Meteor Showers (Leonids, etc.)	**+200% APR** (Peak 24-48 Hours of Event)
	Equinox or Solstice	**+200% APR** (24 Hours of Event)
	Planet 'Transits' the sun	**+200% APR** (timed per second of Event)
	Monthly (or Seasonal) Blue Moon	**+300% APR** (24 Hours of Event)
	Solar or Lunar Eclipse (Partial / Full)	**+300% APR** (timed per second of Event)
	SUPERMOON (& NEW SUPERMOON)	**+400% APR** (24 Hours Event)

For dual or triple stellar bonus events occurring simultaneously, SUPERMOON stacks the rewards from each and gives a bonus +100% APR for dual events or +200% APR for triple events, all timed to the second of the overlap.

Current cryptocurrency market problems

One of the main cryptocurrency disadvantages with the older blockchain technologies such as Bitcoin for example, is the low speed of transactions in whatever current algorithm is using. Due to the efforts involved in classic Proof of Work and a block time calculation talking 10 minutes and an obscene amount of computing power to derive a single bitcoin, it is obvious today that those problems associated with scalability are the prime cause of the low speed of transactions.

As the number of cryptocurrency network participants grows; the number of transactions waiting for validation multiplies too. It too has a high-cost occurrence for the highly volatile cryptocurrency market. Proof of Stake (PoS) implementations security addresses the high energy consumption of the classic proof-of-work (PoW) issues that bitcoin for example suffers today.

Traders (full time or even just casual / personal day-traders) working with cryptocurrencies often incur losses because the transaction has been delayed and did not take place in time, sometimes delays run into hours before transactions turn up. Older blockchain technologies, when compared to a service solution that provides high-speed of transactions such as credit cards, mostly cannot hope to compete with traditional ways of payments. Newer technology approaches for crypto currencies now are being developed and geared to cope with the transaction stress of modern financial systems.

The issues listed above are only a small part of the existing cryptocurrency market problems, but they can greatly affect the efficiency and stable growth of the market, as well as trading. Progress is necessary for every cryptocurrency system, and it can be achieved only through a solution sensitive to market tendencies and problems.

High transaction costs

Transaction fees are very high for most established peer-to-peer network crypto currencies. Through the Bitcoin network example, we can find that the price of the fastest transaction is calculated using following formula - 10 Satoshi for 1 byte. Statistically, the average size of the transaction is 225 bytes, therefore average transaction fee is 2250 Satoshi or $0.15 at the current exchange rate (1 Satoshi equals 0.00000001 BTC), while the highest average transaction fee had reached a near un-spendable fee of $32 in early 2018.

The Ethereum network calculates transaction fees amount considering difficulty of the smart contract. Average transaction fee varies from $0.17 to $4.15 according to the statistics for the 2018 year that is much bigger than what traditional payment systems have

Proof-of-Stake

Proof-of-work helped to give birth to Nakamoto's breakthrough, however the nature of proof-of-work means that the crypto-currency is dependent on energy consumption, thus introducing significant cost overhead in the operation of such networks, which is borne by the users via a combination of inflation and transaction fees. As the mint rate slows in Bitcoin network, eventually it could put pressure on raising transaction fees to sustain a preferred level of security, the idea of maintaining a huge energy consumption to have a decentralized crypto-currency surely is not good economics when other options exist that can do the same for a fraction of the energy cost? Thus, it became an important milestone both theoretically and technologically for demonstrative concepts that address the security of peer-to-peer crypto-currencies while not using vital energy resources of the world. This sounds dramatic, but this is a realistic energy consumption reference, when bitcoin production consumption has reached and exceed that of Czechoslovakia's actual energy usage (published consumption versus 108%).

A concept termed Proof-of-Stake was discussed among Bitcoin circles as early as 2011 as a means a form of proof of ownership of the currency, and many crypto currencies now use it.

Proof of Work and Blockchain Consensus Systems

Proof of Work is a proven consensus mechanism that has made Bitcoin secure and trustworthy for 8 years now. However, it is not without its fair share of problems. PoW's major drawbacks are:

- PoW wastes a lot of electricity, harming the environment.
- PoW benefits greatly from economies of scale, so it tends to benefit big players the most, rather than small participants in the network.
- PoW provides no incentive to use or keep the tokens.
- PoW has some centralization risks, because it tends to encourage miners to participate in the biggest mining pool (a group of miners who share the block reward), thus the biggest mining pool operator holds a lot of control over the network.

Proof of Stake was invented to solve many of these problems by allowing participants to create and mine new blocks (and thus also get a block reward), simply by holding onto coins in their wallet and allowing their wallet to do automatic "staking". Proof-of-Stake was originally invented by Sunny King and implemented in Peercoin. It has since been improved and adapted by many other people. This includes "Proof of Stake Version 2" by Pavel Vasin, "Proof of Stake Velocity" by Larry Ren, and most recently CASPER by Vlad Zamfir, as well as countless other experiments and lesser known projects.

Independently discovered the concept of Proof-of-Stake and the concept of coin age in October 2011, whereby we realized that Proof-of-Stake an indeed replace most proof-of-work's functions with careful redesign of Bitcoin's minting and security model, allowing Coin age consumed by a transaction can be considered a form of Proof-of-Stake . This is mainly because, like Proof-of-Work, Proof-of-Stake cannot be easily forged. Of course, this is one of the critical requirements of monetary systems - difficulty to counterfeit. Philosophically speaking, money is a form of 'Proof-of-Work' in the past thus should be able to substitute Proof-of-Work all by itself.

SUPERMON uses Proof-of-Stake to secure its network and Blockchain Consensus Systems. Each wallet allows a participant an offer of a block reward just by unlocking their wallet and allowing the wallet balance /stake to participate in the SUPM Blockchain consensus system.

Coin Age

The concept of coin age was known to Nakamoto at least as early as 2010 and used in Bitcoin to help prioritize transactions, for example, although it didn't play much of a critical role in Bitcoin's security model. Coin age is simply defined as currency amount times holding period. In a simple to understand example, if Bob received 10 coins from Alice and held it for 90 days, we say that Bob has accumulated 900 coin-days of coin age.

Additionally, when Bob spent the 10 coins he received from Alice, we say the coin age Bob accumulated with these 10 coins had been *consumed*. In order to facilitate the computation of coin age, PoS engines introduce a timestamp field into each transaction. Block timestamp and transaction timestamp related protocols are strengthened to secure the computation of coin age. For example, the 'PeerCoin' protocol block generation is based on *coin age* which is a factor that increases the weight of unspent coins linearly over time; the proof that must be provided together with a new block and must satisfy the following condition:

The proof hash corresponds to the hash of an obfuscation sum that depends on a stake modifier, the unspent output, and the current time. With this system it is possible for an attacker to save up enough coin age to become the node with the highest weight on the network. If the attack were to be malicious the attacker could then fork the blockchain and perform a double-spend. After this is done however, a second double-spend would require the attacker to save up coin age again, as the stake resets when the block was generated.

It is worth mentioning that this situation is highly improbable and that the incentive is questionable (saving enough coin age to be the highest weight on the network would either take a lot of time or a lot of coins, and thus money, to make this happen. Next to that, performing such an attack would probably devalue the system itself so it wouldn't be profitable to do the attack in the long run.)

Another problem with coin age are greedy honest nodes. These are nodes that have no malicious intent, but they keep their coins off the network and only stake occasionally, to get their stake reward. The current system encourages abusive behaviour of these nodes by keeping their node offline until it accumulates enough coin age to get the reward in a short period of time and then shut down the node again, but SUPERMOON stops this behaviour by removing the coinage history from the calculation of block rewards.

Fairness for Proof of Stake Rewards

As SUPERMOON's mechanics are is calculated in real time, the coinage history is completely removed from the reward system to become irrelevant in the actual coin reward calculation, but the coinage history provides each wallet competing stake with an ever-increasing network weight to gain and win the right to stake a block reward. Any winning stake gaining the applicable block reward from a Proof-of-Stake has the coinage stripped from the winning stake, and the winning stake is then blocked from another turn through a long coin maturity minimal period of about Sixteen and ½ + hours (1190 blocks), over which the coinage calculation starts again. With a block time averaging 50 seconds on testing, after each single Proof-of-Stake return, the next Proof-of-Stake transaction by each network participant is limited to possibility of participation only once in approximately every 991 minutes period.

Long maturity ensures that other competing Proof-of-Stake participants ever increase coinage and therefore increase staked amount weight should allow even low staked amounts, so that everyone will eventually have enough weigh to win the right to a Proof-of-Stake coin block reward over time.   It also means that large volume whale wallets are excluded for longer periods after each stake reward, instead of recurring wins due to a large wallet balance.

The long coin maturity with no coinage calculation to the block reward behavior also addresses classic exploits of the APR% introducing fairness and incentivizes network participants to open their wallets 24 x 7 to gain a continual chance of return via the Proof-of-Stake , and the coin % inflation is also controlled by design to be reasonably low.

The coinage being removed from block reward is to contest against 'wallet-locking' exploits. The coin locking exploit is were wallet owners taking wallets offline and bringing them back online at high interest block rewards, trying to aim for point in time where rewards being at their maximum, and gaining the coinage history award into that calculation, all at the highest possible % APR. This benefit in doing this is completely removed by removing coinage from the calculation, since there is no longer of any significant benefit due to the removal of coinage reward, wallets must stake all the time to gain a max return. If the wallet owner locks the wallet waiting to target a period of high APR% before unlocking due to a high return, the stake coinage is consumed during the single right to stake in the Proof-of-Stake engine, but the coinage history does provide significant benefit to waiting for a single point in time to maximize any benefit stake return.

A maximum of one wallet can gain the Proof of Stake (Block) reward per block, which is set to block timing target of 60 seconds, but when timed in practice, results in approximately 50 seconds. Block timing and difficulty are targeted and controlled by using DGW (DarkGravityWave v3).

Proof of Stake Version History

Proof of Stake has a long history, and keeps changing, but in principle this section describes what was changed between each version to arrive at PoSv3 for historical purposes:

PoSv1

This version is implemented in ‘Peercoin’. It relied heavily on the notion of "coin age", or how long a UTXO has not been spent on the blockchain and therefore consumed. Its implementation would basically make it so that the higher the coin age, the more the difficulty is reduced.

This had the bad side-effect however of encouraging people to only open their wallet every month or longer for staking, as they would gain a reward for the complete history of the coins via the coinage being used in the coin block-reward calculation. Assuming the coins were all relatively old, they would almost instantaneously have the weight to produce new staking blocks. This however makes double-spend attacks extremely easy to execute. Peercoin itself is not affected by this because it is a hybrid PoW and PoS blockchain, so the PoW blocks mitigated this effect.

PoSv2

This version removes coin age completely from consensus, as well as using a completely different stake modifier mechanism from v1. This was done to remove coin age from consensus and make it a safe consensus mechanism without requiring a PoW/PoS hybrid blockchain to mitigate various attacks.

PoSv3

PoSv3 is more of an incremental improvement over PoSv2. In PoSv2 the stake modifier also included the previous block time. This was removed to prevent a "short-range" attack where it was possible to iteratively mine an alternative blockchain by iterating through previous block times. PoSv2 used block and transaction times to determine the age of a UTXO; this is not the same as coin age, but rather is the "minimum confirmations required" before a UTXO can be used for staking.

This was changed to a much simpler mechanism where the age of a UTXO is determined by its depth in the blockchain. This thus doesn't incentivize inaccurate timestamps to be used on the blockchain and is also more immune to "timewarp" attacks. PoSv3 also added support for OP_RETURN coinstake transactions which allows for a vout to contain the public key for signing the block without requiring a full pay-to-pubkey script.

Furthermore, as mentioned above, Proof-of-Stake based on CoinAge tried to create a common APR% for all users - did not encourage satisfactory level of network support and yearly compounding interest was not big enough pull factor for users to run their nodes continuously.

SUPERMOON Proof of Stake 3.5

SUPERMOON introduces concepts to achieve a variation which is termed Proof of Stake 3.5.

SUPERMOON adopts the basis mechanics from Proof-of-Stake 3.0 which solves many underlying issues of Proof-of-Stake used in older crypto-currency coins. As in all implementations of Proof-of-Stake , simply unlocking a wallet and presenting the network with a balance / stake which only the wallet has the access to, allows the stake to be calculated and actively partake in network competition where the prize is the privilege to sign the transaction on the SUPM blockchain, for which the winner is rewarded with new coins through a block reward against the variable phase of the moon in real time.

The general rule states the higher the network competition there more secure the network becomes. Proof-of-Stake 3.0 dealt with security and stability deficiencies of the previous generation of Proof of Stake including Coin Age, Blockchain Precomputation and Block Rewards. All the above constitute a potential attack vectors. The original implementation of Proof-of-Stake rewarded Coin Age, which would resulted in incentives to holders who do not take part in securing the network very often by making it easier to win the race if the coins were held untouched for a long time. Coin age is calculated by the weight of unspent coin (UTXO) and the time they have been dormant since last winning and signed transaction via the Proof-of-Stake of SUPERMOON.

In Proof-of-Stake 3.5. CoinAge is removed from the reward calculation to stop rewarding reluctant participants and instead calculations are only awarded based on actual stake encouraging network participation and competition to ensuring the dedicated SUPERMOON users partake on a 24/7 basis. Now only active participants can compete for the network reward for the highest return. Probability of a node winning the right to sign a transaction will be proportional to the percentage of its share of allocated coins taking part in that competition with coinage acting as a factor in elevation of staking weight but does not reward the node for a lack of participation in the network consensus. With this change, this measure creates much stronger pull factor encouraging the network to grow and compete and become more secure.

Another attack vector that former Proof-of-Stake protocol was vulnerable to was Blockchain Precomputation. Proof-of-Stake 3.0 introduced stake modifier interval that enhances obfuscation of hash which makes it harder to predict the time of the next proof of stake block. This prevents an attacker from staking multiple blocks in a row.

Proof of Stake 3.5 is a credible alternative that is much more energy efficient and minimizes environmental impact of normally energy intensive tasks. Also, lower hardware requirements make the system more appealing to a wider group of users and investors.

The strength of SUPERMOON's is the self-adjusting Proof of Stake engine as it allows the user to be exempt from tedious micromanagement of coin piles with multiple addresses if they so choose. With that in mind the Proof of Stake 3.5 engine will give the same comfort of use for its users by utilizing adaptable coin pile split and dust merge rulesets with default values that should fit most users out of the box.

The rewards generated by the wallet via Proof-of-Stake principles of a hashing scheme bearing similarity to Bitcoin's but over limited search space, which is not relying on the difficulty and processing power to calculate a block reward.   Block chain history and transaction settlement are further protected by a centrally broadcasted checkpoint mechanism compiled into the clients for regular Blockhash checkpoints with client version updates periodically to ensure that block chain-splitting does not occur through via accident or via malicious long-range attacks attempts.

A block maturity of 1190 also promotes a huge depth of transactions to spoof before a single winning transaction becomes available again for participation in the proof-of-staking network consensus.

Algorithms of consensus

SUPERMOON's Proof of stake 3.5 algorithms of consensus are Proof-of-Work, and Proof-of-Stake.

The PoW is used for initial SUPM coin distribution and for maintaining the security of the network before it needs to become highly-decentralized by many user's participation. The PoS 3.5 will provide scalability and reliability at the later stages of development without forcing participants of the network to use a large amount of resources like electricity for transaction validation.

PoW is made by a hashing algorithm called Scrypt which is use for transaction validation in such popular networks as Bitcoin, Litecoin, DogeCoin, and more than 500 others. With PoS and PoW methods combined, the target speed of the new block's generation at the early stages of Supermoon ecosystem development will be:

> Targeted for 1 block per minute (1440 blocks per day approximately) – timed calculation over various testing is 56 seconds to 45 seconds, averaging near dead-on 50 seconds per block in several sets of 24 hours timespan in practical testing.

Such combining of consensus algorithms will provide essential advantages compared with many popular crypto coins at the present market whether in fee for the transaction (standard fee is 0.0001 SUPM) or in the speed of transaction.

To participate and attempt to gain Proof-of-Stake a block reward, all wallets need to have a non-zero SUPERMOON coin balance available for transaction validation. The amount of reward for block creation depends not only on SUPERMOON'S stake balance but however it differs to avoid a reward the duration of the period that coins are holding on the account since they were last staked.

Thus, stake weight is calculated as follows:

- Stake Weight = Stake Volume * CoinAge
    - CoinAge = bnCentSecond * CENT / COIN / (24 * 60 * 60);
      bnCentSecond is a sum of Cents multiplied by a transaction age for all incoming transactions for the current staked balance; 1 Cent = 0.01 SUPM

The formula calculates transactions valid for reward under for PoS-mining, wallets gain staking weight, but it does NOT allow CoinAge to be used in any way to gain any benefit from being offline.

The SUPERMOON block height reward is calculated based on the real time value of the last confirmed blocktime from the maximum blockheight of the blockchain. Once this is gained the engine then uses this to calculate the current time of the staking engine, and the SUPERMOON block reward.

- AmountStaked * COIN_YEAR_REWARD * 33 / (365 * 33 + 8)
  * multiplier based from 1 (100%) to 5 (500%) for (Phase of the Moon multiplier) and {bonus Stellar Events} and {event staking bonus} of 100% for two events, and 200% for 3 or more stellar events happening at once actual example: Supermoon, Lunar Eclipse and Bluemoon (Jan 2018) which allows a max reward of three of the Stellar common events to award a max of 1200% APR% by calculations in practice calculations.

So, where the AmountStaked is the amount of coins staked by the wallet, but the PoS 3 calculation of coinage of the staked coins via wallet is only used for the calculation of winning the Proof of Stake block reward, which remains the same as a standard Proof-of-Stake version 3 calculation.

- COIN_YEAR_REWARD = 100%

Max Coin Supply

MAX Supply SUPERMOON has decided to use transaction reward fees instead to control the coin inflation once max coins are reached, the removes and awards a set reward to a mere 1 SAT. It also serves as a deflationary force to counter the inflationary force from the Proof-of-Stake minting keeping the Proof-of-Stake reward to a minimal amount, taking Proof-of-Stake rewards down so low, it takes about 150 years of Proof-of-Stake rewards to generate a single SUPM coin, flatlining any benefit.
The initial Supermoon founders stake issue is 50,000,000 SUPM, and the max supply limit is 500,000,000 SUPM, which means that the creation of extra coins will stop in a certain moment of time; it will allow preventing value decreasing with a network growing slowing down on a long-term outlook.

To ensure the proof of stake process does not stop, an initial seeding of SUPM was needed to be created with enough number addresses to drive the engine through the 1190 confirmations for each Proof-of-Stake confirmation before a proof of stake transaction can participate again.

A coin mechanism also allows the Proof-of-Stake mechanics to continue once the max supply is reached, it merely stops awards variable rewards returns once the max supply is reached. In order to send currency to other wallets in process, you need to unlock the wallet in the process. The process will naturally attempt to stake, as well as drive the block reward mechanics onwards, but stop rewarding any stakes of value due to the Max supply.

Block Generation under SUPERMOON Proof-of-Stake 3.5

The Proof-of-Stake hybrid design, blocks are separated into two different types, proof-of-work blocks and Proof-of-Stake blocks. The Proof-of-Stake type of blocks is a special transaction called *coinstake* (named after Bitcoin's special transaction *coinbase*). In the coinstake transaction block owner pays himself thereby consuming his coin age, while gaining the privilege of Stake reward output is based on:

> Actual staked SUPM amount * the calculated reward return based for the amount staked based from the current phase of the moon multiplier, with the real time calculated from the last blocktime stored and confirmed on the SUPERMOON block blockchain:

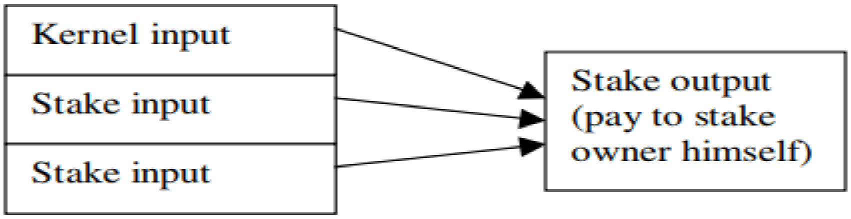


Figure: Structure of Proof-of-Stake (Coinstake) ~ from PPCoin

Transaction generating a block for the network and minting for Proof-of-Stake . The first input of coinstake is called *kernel* and is required to meet certain hash target protocol, thus making the generation of Proof-of-Stake blocks (a stochastic process like proof-of-work blocks). However an important difference is that the hashing operation is done over a limited search space (more specifically one hash per unspent wallet-output per second) instead of an unlimited search space as in proof-of-work, thus no significant consumption of energy is involved.

The hash target that stake kernel must meet is a target per unit coin age (coin-day) consumed in the kernel (in contrast to Bitcoin's proof-of-work target which is a fixed target value applying to every node). Thus, the more coin age consumed in the kernel, the easier meeting the hash target protocol. For example, if Bob has a wallet-output which accumulated 100 coin-years and expects it to generate a kernel in 2 days, then Alice can roughly expect her 200 coin-year wallet-output to generate a kernel in 1 day.

SUPM Minting based under Proof-of-Stake 3.5

The minting process for proof-of stake blocks, is mined from the actual QT wallet. The trigger for Proof-of-Stake block mints coins based on coin-age in the coinstake transaction. A mint will consume the coinage of the stake in the minting process.

Main Chain Protocol

The Proof-of-Stake mechanism uses the protocol for determining which competing block chain wins as main chain, depends on consumed coin-age, where every transaction in a block contributes it's consumed coin age to the score of the block. The block chain with highest total consumed coin age is chosen as main chain.

This contrasts with the use of Proof-of-Work in Bitcoin's main chain protocol, whereas the total work of the block chain is used to determine main chain.

This design alleviates some of the concerns of Bitcoin's 51% assumption, where the system is only considered secure when good nodes control at least 51% of network mining power. First the cost of controlling significant stake might be higher than the cost of acquiring significant mining power, thus raising the cost of attack for such powerful entities. Also, attacker's coin age is consumed during the attack, which may render it more difficult for the attacker to continue preventing transactions from entering main chain, especially with a block maturity to participate in the Proof-of-Stake process again being set at 1190 confirmations.

Security

Supermoon uses proved cryptography methods with a separation to public and private keys, with the QT wallets aiding simple access control (to your own controlled private keys) via the wallet (account). Many companies (e.g. banks, exchanges and financial organisations) use similar algorithms principles to restrict information access & protection, which provide access for their users within strict control methods to offer external private access to the users own bank provided information e.g. internet banking via https websites, but the keys are provided via signed certificates allowing authoritive access to each users own personal data, and access control (via bank provided and therefore fully bank controlled access) via single factor (username / password) or two factor authentication (password in conjunction with a separate defined additional external electronic devices in the users possession for more secure complex implementation.

The principle of access to each users SUPERMOON (QT) wallet application, where the client logical 'certificates' access is provided and stored locally via the 'wallet.dat' on each users core client. The 'wallet.dat' is secured and protected by a password of the own user's complexity to define.

If a hacker gets access to the device the wallet is installed on, and takes the 'wallet.dat' file, then password complexity is the main method for stopping currency from being taken from that point, but the wallet.dat files are the core method to ease access storing the private keys for each user on the blockchain.

Encryption

SUPERMOON uses several cryptographic algorithms to provide integrity and security of the networks.

First is ECDSA - a cryptographic algorithm with public key, which is connected to each coin in the system by using: public key, private key and signature, so that every node of blockchain can check the belonging of the coin.

Second is reliable one-way encryption algorithm is SHA-256 included in the group of cryptographic hash functions SHA-2. It is considered as a classic one by major crypto programmers in the world.

Hash functions SHA-256 is used for transformations of an input data of any size into 32-byte line for blockchain, which cannot be cancelled or predicted. In case of hacker attack, when some or all input data is changed, hash connected to this data will also be changed, so the generation of another block with the same hash becomes impossible. These 2 cryptographic algorithms provide stable and secure work of SUPERMOON networks, where the belonging of the coin can be easily checked, while distributed consensus is achieved without double expenses.

Checkpoint: Protection of History

One of the disadvantages of using total consumed coin age to determine main chain is that it lowers the cost of attack on the entire block chain of history. Even though Bitcoin has relatively strong protection over the history Nakamoto still introduced checkpoints in 2010 as a mechanism to solidify the block chain history, preventing any possible changes to the part of block chain earlier than the checkpoint. Another concern is that the cost of double-spending attack may have been lowered as well, as attacker may just need to accumulate certain amount of coin age and force reorganization of the block chain. To make commerce practical under such a system a form of checkpoints that are maintained centrally within client version itself at compile, which means that at a regular interval by the SUPERMOON developers, a client release freezes block chain history at key points to finalize transactions.

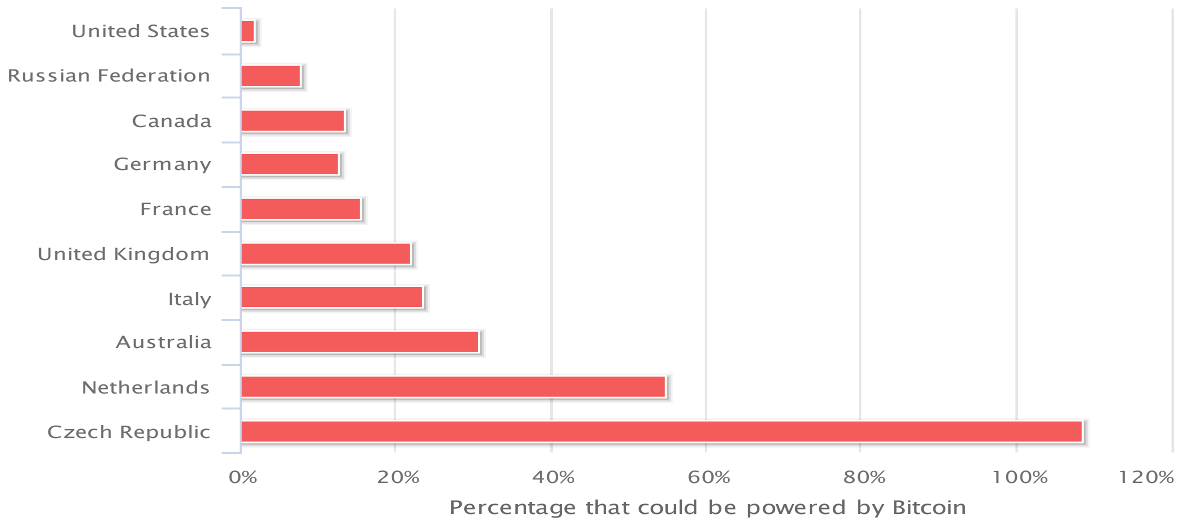
Block Signatures and Duplicate Stake Protocol

Each block is signed by its owner to prevent the same Proof-of-Stake from being copied and used by attackers. A duplicate-stake protocol is designed to defend against an attacker using a single Proof-of-Stake to generate a multitude of blocks as a denial-of-service attack. Each node collects the (kernel, timestamp) pair of all coinstake transactions it has seen. If a received block contains a duplicate pair as another previously received block, the coin mechanics engine ignores the duplicate-stake block until a successor block is received as an orphan block.

Energy Efficiency versus classic bitcoin rewards system

With a classic implementation of Proof-Of-Work, when the proof-of-work mint rate approaches zero as max coins are reached, there would be less and less incentive to mint proof-of-work blocks. Under this long-term scenario energy consumption in the network may drop to very low levels as disinterested miners stop mining proof-of-work blocks, which is a real future problem that the Bitcoin network faces. Unless transaction volume / fee rises to high enough levels to sustain its incredible energy consumption, which when compared to current effort rates versus difficulty, does seem unlikely that the future effort required will be addressed, without a variation of the Bitcoin core code to account for it.

Bitcoin Energy Consumption Relative to Several Countries



BitcoinEnergyConsumption.com

The sustainability of this cannot keep going at the same growth without a change in the bitcoin mechanics, apart from the previous comparison, it also possible to compare Bitcoin's energy consumption to some of the world's biggest energy consuming nations shown in this graph as of October 2018 above:

Under SUPERMOON implementation of Proof-of-Stake design, the energy consumption required to run a wallet is effectively drops to a minimal amount, with a Personal Computer running close to idle and simply being switched on i.e. close to zero in comparison to a proof-of-work cost.

The SUPERMOON network uses Proof-of-Stake services for its protection, each node participating in the network providing the next block. This is the principle of crypto-currency running as *long-term energy-efficient* as the energy consumption is very low due to the SUPM Proof-of-Stake engine process to demonstrate ownership presented to the network.

Even if the core distributed network distribution does not enough participating stakes to run the support network, the SUPERMOON network is maintained by dedicate low stake value staking servers with 1800 minimal minted transactions which are open for Proof-of-Stake 24 x 7, which will trigger in the event of no-single wallets being held higher to stake. This will ensure that the Proof-of-Stake engine can still be driven to mint blocks and drive the network onwards, keeping the coin mechanics running in case of a staking ‘stall’ due to ‘nStakeMinimumConfirmations’ being set at 1190, causing a ‘no mature coins’ staking stall.

Coinage History and Wallet Locking exploit

SUPM has modified the Proof-of-Stake engine to leave coinage as a key mechanic for right to stake (mint) rate to be not determined by block height (time) and maintained the existing code to determine by difficulty including coin age to trigger the right of Proof-of-Stake , but the stake reward is completely determined by block height time and each actual stake, which are compared against public published APR % values / rates of return, of which coins take approximately 20+ hours to mature again for each single stake. This means that no history of coinage can be of value, encouraging participation in the Supermoon network in order to gain any rewards, and increasing the overall security through volume of participation.

The basic principle of ‘you gotta be in it, to win it’ applies.

Repository on GitHub

Since the publication of the SUPM cryptocurrency on the GitHub resource it has since stopped to be under the total control of the Supermoon Team founders but may evolve in the future to be a community based leaders as the principle conceptual idea of using block height time as the method defining events i.e. SUPM uses this principle as its basis defining the rewards per block.

All interested participants, freelancers and specialized development teams can support the development and modernization of the SUPERMOON crypto code.

Documentation, new versions, soft-forks of cryptocurrencies are placed as open source on the GitHub in the Supermoon repository:

- https://github.com/chryophase/supermoon

Phases of the Moon and Stellar events are calendared and published on the SUPERMOONCOIN website. This site has other documentation, as well as the latest new client versions of the SUPM cryptocurrency are placed as compiled client releases on the WALLETS page of:

- http://supermooncoin.com

Areas of Application

Infrastructure Services

The authoritive services are spread across a very large geographic area and are Distributed Denial of Service (DDoS) protected by major data Centres running at Tier 3 protection. Standard services offered are redundancy and availability to 99.99% protection, with daily backups of the main nodes.

The infrastructure supporting the services have three main SUPERMOON daemon nodes, and one full time 'staking node' which are based across the world for active distribution and redundancy in:

- Sydney, Australia
- Los Angeles, USA
- Frankfurt, Germany,
- Tokyo, Japan.

For Customers

Private users of SUPERMOON network can use Supermoon in everyday activity, getting all advantages of the new technologies for the cooperation with each other and for mutual payments once an exchange is defined for common use:
All SUPERMOON and crypto-currencies transactions use the classic Internet without any third party support (or help in the event of mistakes which is a drawback for careless use). Therefore, the transaction fee is less to nothing when compared with the same in banks, for example:

- SUPERMOON fits to use for any transactions: big and small ones.

  Supermoon has no connections with any centralized issuing institute in any country, and due to the incredible instant speed of cryptography wallets and balances, it is easy to use for international transactions.

- The SUPERMOON wallet cannot be frozen by any external organisations;
- Cryptocurrency has no controlling organizations;
- No requisites and preconditions are required to execute transactions;

- There are no transaction limits (other than number of different transactions in a single transaction), and it is possible to transfer any size or amount of coins as many times as is required;
- High level of protection against hacking, forgery, and fraud. That's why SUPERMOON is perfect for saving and accumulating value.

For Business

For example, enterprises can use blockchain technology with integrated cryptocurrency: for financial transactions, as a unit of account when making transactions or for encouraging participants in a loyalty program, to use as a unit of account in advertising and other types of platforms, integrate into the marketplace, etc.

Blockchain technology is one of the largest fields of potential applications in the Enterprise.

Applications for use in connecting to system data owned by the authorities so that they can improve business transparency and improve the image of companies has not been fully realized in potential yet.

Consequently, investors and financial institutions working based on environment of the blockchain will play a vital role in daily business activities soon.

Implementation and managing of Supermoon and associated ecosystem by business companies gives next advantages:

- low charge for the circulation,
- strong security, and
- easy scalability.

SUPERMOON is a perfect tool for business development. It can be used as a payment system which easily integrates into network exchange, or into the real economy, starting from online shops, discount providers, delivery services, media, to the banking sector and the real estate industries as applications apply.

1. Due to the low entry level, any business doesn't need to spend many resources for using SUPERMOON to complete transactions;

2. It will be easier to connect SUPERMOON payment system to websites and mobile apps once an API is created via RestAPI.

FUTURE API

For future ease of processing, the development team has the opinion that the technology from Bitcoin should be used in principle for a basis for a SUPERMOON API.

Bitcoin API is easy to upgrade, it has proven the ease of integration and high level of confidentiality of transmitted data. The introduction of crypto technologies into everyday life is the most promising direction. With the help of the API it will be possible to connect:

- online and offline stores marketplace and/ or
- exchange sites
- entertainment applications
- mobile wallets
- charitable and other types of funding applications

The community has no current plans to realize processing between cryptocurrency with payment systems such as PayPal is likely to be easily developed.

After upgrades of modernisation, encapsulation and testing of the required future code, the API SUPERMOON will be placed on the GitHub in time after Q2 2019.

Other Considerations

Babaioff et al. (2011) studied the effect of transaction fee and argued that transaction fee is an incentive to not cooperate between miners. Under the SUPM system this attack is exacerbated so we no longer give any level of significant transaction fees to a block owner.

Conclusion

Upon validation of our design in the Market, we expect Proof-of-Stake designs to become a potentially more competitive form of peer-to-peer crypto-currency to proof-of-work designs due to the elimination of dependency on energy consumption, thereby achieving lower inflation/lower transaction fees at comparable network security levels.

Due to the unique implementation of the real world timing via phases of the moon, the Supermoon developers expect this project to become a success, and to gain some serious interest with its attempts to link the real world stellar events with the digital currency world of crypto-currency.

FUTURE - Cryptocurrency Roadmap

SUPERMOON started as a cryptocurrency that was focused on generating and storing wealth through in-built protocols which will be of benefit to users of personal financial services.

Blockchain technology develops at accelerating pace with every passing year and SUPERMOON is going to be adapting to constantly changing technological and market landscape. To stay compatible and have ongoing access to the wealth of technological advancements SUPERMOON will adopt industry standards necessary to incorporate solutions and components that would be beneficial to the future of SUPERMOON.

Any new feature that has been time tested and would add value to the coin could and would be implemented. In the immediate future after the release, SUPERMOON will be working towards developing a mobile wallet for Android / OSX devices to enable people to access and manage their coins on the go. The development on SUPERMOON Core software will continue throughout the year and will come in several stages. Every new release will add new features to the platform, increase processing power and scalability of the network.

The first stage

- Development of a safe and confidential set of QT wallets with the use of innovations provided via Proof-of-Stake 3.5
- Wallets applications for Mac OS, Windows, Linux and Rasparian.

- Development and Implementation of improvements for the Proof-of-Stake 3.5 algorithms
- Alpha and Beta testing
- Launch of the blockchain in November 2018

The second stage

- Development of SUPM wallets for Android & iOS platforms
- API development
- Access to world trading platforms

Acknowledgement

Many thanks to the Supermoon team and my family for bearing with me and helping out with testing block chain issues, setup of the infrastructure, web and graphics design and other related work through to the issues that faced this coin from idea to reality.

Of course we would like to thank Satoshi Nakamoto and Bitcoin developers whose brilliant pioneering work opened our minds, and previous various altcoins that published their Proof-of-Stake incarnations that made a project like this possible.

References

1. *Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies;*
   Energy Research & Social Science, Volume 44, October 2018, Pages 399-410
   https://www.sciencedirect.com/science/article/pii/S2214629618301750
2. *Babaioff M. et al. (2011): On Bitcoin and red balloons.*
3. *Laurie B. (2011): Decentralised currencies are probably impossible (but let's at least make them efficient).*
   *(*http://www.links.org/files/decentralised-currencies.pdf*)*
4. *Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system.*
   (http://www.bitcoin.org/bitcoin.pdf)
5. *What Happens to Bitcoin After All 21 Million are Mined?*
   a. https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/

6. *Bitcoin Energy Consumption Index*
    a. https://digiconomist.net/bitcoin-energy-consumption
7. *Long Range Attaches*
    a. https://medium.com/@abhisharm/understanding-Proof-of-Stake -through-its-flaws-part-3-long-range-attacks-672a3d413501
8. *Proof of Stake background information*
    a. *PPCoin 'PeerCoin Whitepaper' by Sunny King, Scott Nadal Aug 19, 2012*