6-14-2017

Denarius - Ancient Money for a New World

The Whitescroll

Bitcoin has long been the premium cryptocurrency for the storage of value. Bitcoin is the ‘original’ cryptocurrency; an immutable blockchain with a long history. Bitcoin is for this reason why many still see Bitcoin as a stable currency - not because it has not suffered any issues in the past, but because the blockchain technology originally proposed and brought into code reality by Satoshi stands the test of time and leaves a solid record of all operations in a blockchain including any of those that may be disagreeable. We expect transparency in our public trade markets and often transparency is left lacking, however Bitcoin cannot be argued that it shows every right and every wrong, making Bitcoin a trustable currency medium. Bitcoin is for this reason that it continues to this day to be the ‘trusted’ currency, and it is in these footsteps that Denarius will try to follow.

Even though the Bitcoin network holds a smaller percentage of the transactions taking place in today’s cryptocurrency universe, the number of transactions has steadily risen, especially in times of heavy volatility as many holders of the coin seek to liquidate their holdings. This has lead to some significant troubles and Denarius seeks to provide another store of value which provides the same trusted immutability as Bitcoin. Denarius seeks to solve the issues in Bitcoin’s growth by implementing the same trusted blockchain technology directly from Bitcore code whilst decreasing the block times significantly to provide a much faster and responsive network in order to achieve a much higher transaction volume and speeds that are now expected of mass-adopted modern cryptocurrency networks.

The Bitcoin core code is tried and trusted. Denarius does not intend to attempt to re-write it in any way that it functions. The restriction, we believe, lies not in the blockchain technology itself or any way in which the blocks are constructed, but simply in how often the blocks are created. To answer enquiries of how the blockchain operates in Denarius, the reader only need look to the original Bitcoin whitepaper released by Satoshi (Source).

In Bitcoin, transactions are encoded in the blockchain with a cryptographic hashing algorithm. These hashes are created by miners using a “proof of work” (PoW) algorithm that combines one or more hashing functions. Bitcoin itself uses the SHA256d hashing function, which has been popularly used for a long time. ASICs (application specific integrated circuits) have been built to create SHA256d hashes at alarming rates which in turn has lead to the Bitcoin network hashrate inflating beyond the level that it was ever intended to be. In order to create a single hash for the Bitcoin network and use it to encode a new block in the blockchain, it now requires a significant amount of power and effort. In fact, using a GPU to create hashes for the Bitcoin blockchain is effectively futile against the hashing power provided by SHA256d capable ASICs.

The prevalence of ASICs has lead Bitcoin to a situation where only those significantly invested in hardware are able to gain any kind of reasonable reward from mining it; thereby leaving the transaction processing in the hands of a few actors. Again, this is not an issue of the blockchain itself, but simply a side effect of high block times with an easily solvable hash algorithm.

Hybrid PoW/PoS Phase

In order to discourage ASIC creation which would adversely affect miners of the coin, Denarius seeks to implement a short proof of work phase in hybrid with proof of stake (PoS) where the PoS miners will use low difficulty hashes to create blocks & process a block full of transactions, claiming the transaction fees alone whilst the PoW miners will compete for higher difficulty hashes to create blocks which include a generation payment as well as any transaction fees attached to transactions in the mempool when the hash is solved.

Even if the difficulty of the PoW blocks increases significantly, blocks that are full of transactions can still be processed by PoS miners at a low difficulty to ensure that even at times of very high PoW difficulty, block times can remain at or below 30 seconds.

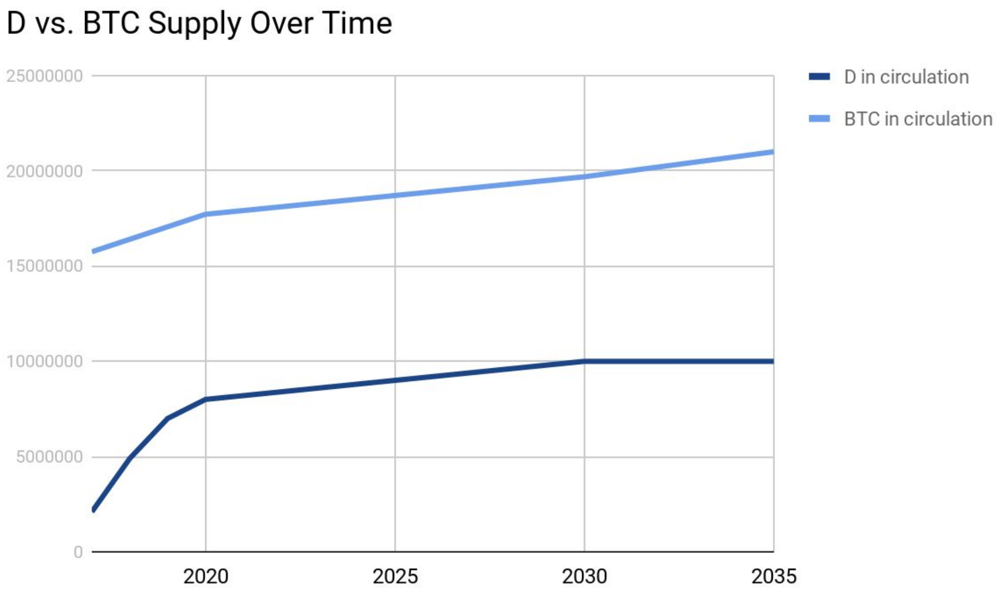
The PoW phase of Denarius is set to run for around 3 years. During this phase, 3 million blocks will be generated between PoW and PoS with up to 30% of the blocks being generated by the PoS portion. The PoS block reward will only contain transaction fees during the PoW period and transition to 6% APR for each staked coin in the full-PoS phase.

Given a 30 second average block time, each PoW phase will last 30 million seconds or 49.5 weeks. For simplification, the block reward structures are divided into one year segments with the exception of the block after the genesis block, which contains 1,000,000 D.

The premine block rewards are 50% dedicated for bounty and marketing costs in the first 6-12 months of the project with the remaining 50% (500,000 D) used for development costs across the lifespan of the project.

The reward structure of the blocks is as follows:

	Blocks	Reward	Total (excl max PoS of 30%)
Year 1	2-1,000,000	3 D	2,100,000
Year 2	1,000,001-2,000,000	4 D	2,800,000
Year 3	2,000,001-3,000,000	3 D	2,100,000
End of PoW Rewards (~May 2020)			8,000,000 D
Maximum D Supply (2030-2035 depending on stakes)			10,000,000 D



This creates a middle-heavy block reward structure that incentivises mining in the second year over other years. In comparison to a “reward halving structure” this encourages a more diverse group of miners to continue mining through the entire phase of the coin’s PoWstage rather than the PoW rewards being continually concentrated towards a small group of the highest rate farms as the PoW phase continues.

The PoW phase ends in May 2020. This will discourage the creation of ASICs for the coin since the possible return on investment would be low given the short PoW phase of the coin.

Pure PoS phase

During the hybrid phase, stake miners only receive the transaction fees that are assigned to transactions that are in the memory pool at the time of the PoS block being generated. During the pure proof of stake phase, the annual percentage rate (APR) awarded to the staking wallets will be set at 6% per coin per year in addition to the transaction fees collected from the memory pool. Given that many coins are held in exchanges, which do not stake (as their supply must be available all the time), it is envisioned that the maximum stake at any time would be 50% of the coin supply.

The total amount of D generated from the pure PoS phase ranges from ~210,000 D in 2020 to ~310,000 D in 2035. The PoS rewards will be discontinued once the D supply reaches 10 million, however stake miners will continue to collect transaction fees from the pool, encouraging a large amount of wallets to remain on the network to process fees.

In comparison to a master-node system where a large portion (sometimes upward of 1% of the supply) is required to qualify and process a block, Denarius rewards even the smallest of wallet holders for remaining on the network. This encourages the flow of D between wallets and keeps the network transaction speeds high due to the availability of stake miners able to encode these transactions in a block.

At the maximum supply of 10 million D, it is estimated a minimum of 2,000 wallets will remain on the network at any time.

The ‘Tribus’ Algorithm

Denarius uses a new PoW algorithm called Tribus - a combination of three of the top five NIST5 algorithms that were created to resist the ability to be calculated by an ASIC. Each of these algorithms is sufficiently different.

The Tribus hash used in a Denarius block is constructed by generating the following amounts of each algorithm and concatenating them together as generated by the original algorithm’s hash function:

1. 80 bytes of JH
2. 64 bytes of Keccak
3. 64 bytes of Echo

Whilst these algorithms concentrate most of the work onto the GPU core, the algorithms are not intensive and do not generate excessive amounts of heat in a GPU core. The listed algorithms are also relatively low-power for calculations.

Whilst there are ASIC devices that exist that can create these algorithms, none are built to create a hash in this manner. The cost and complexity of creating such a device makes it highly unlikely that an ASIC would be created for Tribus, given the relatively short PoW period of Denarius. Any ASIC manufacturer would more than likely have an extensive lead time on creating such an ASIC and may only live to see a few months of mining at a time near the end of PoW when the network hash rate will be at its highest. These combinations make Denarius a non-attractive proposition for an ASIC creator since they could focus on other coins that use other algorithms.

Transaction Speeds and the Memory Pool

Transactions are held in the memory pool until the time when a miner finds a hash capable of creating a new block. At this time, the miner collects transactions from the memory pool and includes them in the new block. Each transaction will have attached a transaction fee (or 'tx fee') that in Denarius is set at 0.00001 D per 226 byte transaction. The memory pool is cleared out by a miner on an average of every 30 seconds. The miner will pick the highest transaction fees to include in their block. If the number of transactions made in a 30 second period exceeds the maximum block size of 4,424 transactions (1MB), then any transactions that cannot fit into the block will be required to wait for the next block to be created.

In the Bitcoin network, during a period of heavy transaction volume, i.e. a "flash crash", thousands of people will flock to the BTC network in attempt to move their Bitcoin, resulting in an overflow of transaction requests. The memory pool is only cleared each 10 minutes, meaning that once the maximum amount of transactions have been requested, transactors are required to pay higher transaction fees per byte in order to incentivise the miners to include them in the next block.

If the transaction is not included in the next block, the transaction fee remains low. It is likely that people will continue to pay a higher transaction fee, in this case the originally requested transaction will remain "low priority" and could take many hours to proceed. Only when overall transaction volumes drop back down below the threshold of the memory pool "low priority" transactions are executed.

Denarius attempts to solve this issue by significantly decreasing the block times to just 30 seconds. The memory pool is collected by a miner every 30 seconds on average, resulting in an effective sustained transaction rate of over 147 transactions per second before transaction fees would require to be increased for transactor efficiency. This is over 20x the rate of Bitcoin. If the transaction volumes do continue above 147 transactions per second for longer than 30 seconds, it will take only another 30 seconds to clear out any transactions that exceed the sustained limit.

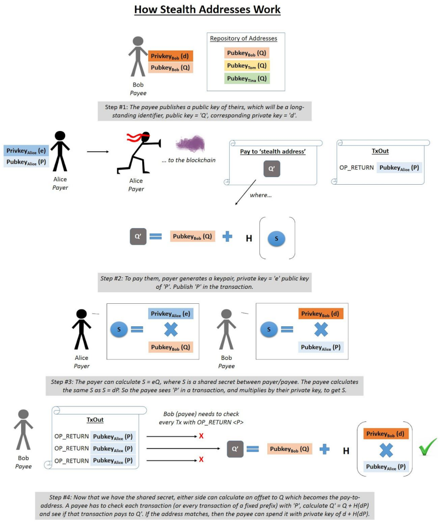
As a store of value, Denarius is not intended to provide lightning-fast transactions in VISA-like volumes, but only to provide a reliable storage of wealth that can be transferred between two owners at a reasonable speed during a significant event. Under heavy VISA-like loads, Denarius transaction times may increase; however, even at 2000 transactions per second, the Denarius network is capable of processing them within 30 minutes using the lowest fee structure.

Confirmations and Block Times

As mentioned previously, block times are the major concern for the speed of transactions in the blockchain technology. Many bitcoin exchanges will trust the Bitcoin blockchain to provide a single confirmation or perhaps 2 confirmations; however, with a 10 minute block time this is still 20 minutes at best before the coins are confirmed. Some exchanges require more than this amount, resulting in a waiting time of an hour, at best. Denarius requires a total of 30 confirmations by default before the coinbase is considered mature. This represents roughly 900 seconds before blocks are 'fully' confirmed and coinbase maturation is assured; however, one can safely assume blocks are confirmed at around 10 confirmations - 300 seconds. Combined with a fast transaction time given by the 30 second blocks, funds appear in the target wallet(s) in under a minute and are fully ready to be transferred further within 5 minutes.

Stealth Addresses

See the image below for on how Stealth Addresses in Denarius function (Source)


How Stealth Addresses Work
Privkey$_{Bob}$ (d)
Pubkey$_{Bob}$ (Q)
Bob
Payee
Repository of Addresses
Pubkey$_{Bob}$ (Q)
Pubkey$_{Tom}$ (Q)
Pubkey$_{Tina}$ (Q)
Privkey$_{Alice}$ (e)
Pubkey$_{Alice}$ (P)
Alice
Payer
Alice
Payer
... to the blockchain
Pay to 'stealth address'
Q'
TxOut
OP_RETURN Pubkey$_{Alice}$ (P)
where...
Q' = Pubkey$_{Bob}$ (Q) + H (S)
S = Privkey$_{Alice}$ (e) × Pubkey$_{Bob}$ (Q)
Alice
Payer
S = Privkey$_{Bob}$ (d) × Pubkey$_{Alice}$ (P)
Bob
Payee
Bob
Payee
TxOut
OP_RETURN Pubkey$_{Alice}$ (P)
OP_RETURN Pubkey$_{Alice}$ (P)
OP_RETURN Pubkey$_{Alice}$ (P)
X
X
Q' = Pubkey$_{Bob}$ (Q) + H (Privkey$_{Bob}$ (d) × Pubkey$_{Alice}$ (P))
✓

Step #1: *The payee publishes a public key of theirs, which will be a long-standing identifier, public key = 'Q', corresponding private key = 'd'.*

Step #2: To pay them, payer generates a keypair, private key = 'e' public key of 'P'. Publish 'P' in the transaction.

Step #3: The payer can calculate S = eQ, where S is a shared secret between payer/payee. The payee calculates the same S as S = dP. So the payee sees 'P' in a transaction, and multiplies by their private key, to get S.

Bob (payee) needs to check every Tx with OP_RETURN <P>

Step #4: Now that we have the shared secret, either side can calculate an offset to Q which becomes the pay-to-address. A payee has to check each transaction (or every transaction of a fixed prefix) with 'P', calculate Q' = Q + H(dP) and see if that transaction pays to Q'. If the address matches, then the payee can spend it with private key of d + H(dP).

(*Enlarged Image*)

Market Info in the Wallet

Denarius contains market information directly inside the wallet UI, providing holders with a real-time overview of the value of their holding. Multiple currency conversions are supported.

Open Source Services

Denarius launched with a complete complement of open source services powered by the RPC services available through the wallet node. Users may run a wallet node on any operating system or machine and point services to it using the RPC port to enable automatic transactions.

These services are only limited by the ability and imagination of the creators; however, to encourage the spreads of Denarius services developers have launched and open sourced the code, that will allow people to easily use Denarius D funds within their various platforms.

Denarius offers several useful services at establishment, such as a paper wallet generator, a vanity address generator and packages available for linux distributions in order to ease implementation of the cryptocurrency on new platforms.

Web Services with your Own Keys

A major concern of many investors of cryptocurrency is keeping their funds secure. It is well known that web services own your private keys and the user must place all their trust (and wealth) in the provider to both stay afloat and to not utilize the private keys themselves. Storing large amounts of cryptocurrency inside an exchange or web wallet is dangerous as the user could easily be disconnected and lose access to all of the funds with no recompense.

Due to slow transfer times in the Bitcoin network, many people keep significant trading funds in exchanges to give them maximal ability to take advantage of market movements. When a significant event occurs in the Bitcoin network, keeping your Bitcoins secure on another machine and moving them into or out of exchanges often cannot be completed before the event is over.

For this reason, Denarius provides an open-sourced web wallet. With a few configuration steps, the user may host their own web wallet using their own private keys on their own server and can be guaranteed the security of their funds whilst still having ease of access. This wallet can be accessed via mobile and utilized to transfer funds to exchanges whenever it is needed. The fast confirmation times of Denarius will allow people to move D from their own private wallet to the exchange within minutes.

The open source NodeJS based ‘Mobile First Web Wallet’ is available on github (which includes 2 factor authentication and social logins). *(Source)*

The New World of Currency

Denarius is a currency which is designed to hold value for a long period and allow that value to be easily moved between wallets without expensive transaction fees or lengthy waiting times. A short PoW period allows the currency to be completely mined within a few years, removing the pressure of ever exceeding mining supply. After the PoW period, the PoS period provides a small amount of supply over a longer period, encouraging holders of the currency to provide node services to the network whilst increasing the supply at a lower rate than PoW (roughly 10% of the rate).

The new proof of work algorithm combined with a low maximum supply and with features such as market and network information directly inside the wallet place Denarius in a unique position in the industry.

In a world where cryptocurrency is expected to gather pace and eventually overtake fiat currency for usability, Denarius provides the feature sets that are needed to accomplish this. This alone places it alongside major currencies and offers stability greater than many coins on the market today, which have value based on features that are not currently available.

Physical Denarius coins may become available in the future, which will be compatible with Denarius private keys, providing real world tangibility.

This paper was written by Dylan (enkayz) and Carsen (kingcarsen) and edited by the Denarius community. It is intended to reflect the technicalities of the Denarius network.

DISCLAIMER: This Denarius Technical White Paper (Whitescroll) is for information purposes only. Denarius and Carsen Klock, does not guarantee the accuracy of or the conclusions reached in this white paper, and this white paper is provided "as is". Denarius and Carsen Klock does not make and expressly disclaims all representations and warranties, express, implied, statutory or otherwise, whatsoever, including, but not limited to: (i) warranties of merchantability, fitness for a particular purpose, suitability, usage, title or noninfringement; (ii) that the contents of this white paper are free from error; and (iii) that such contents will not infringe third-party rights. Denarius and Carsen Klock, and its affiliates shall have no liability for damages of any kind arising out of the use, reference to, or reliance on this white paper or any of the content contained above, even if advised of the possibility of such damages. In no event will Denarius and Carsen Klock or its affiliates be liable to any person or entity for any damages, losses, liabilities, costs or expenses of any kind, whether direct or indirect, consequential, compensatory, incidental, actual, exemplary, punitive or special for the use of, reference to, or reliance on this white paper or any of the content contained above, including, without limitation, any loss of business, revenues, profits, data, use, goodwill or other intangible losses.