DIAMOND

SCARCE VALUABLE SECURE

BIT.DIAMONDS

BE YOUR OWN BANK AND A CREATOR OF WEALTH

Aleksander Mesor
Helmut Siedl
Christian Knoepke

July 13th 2017

Version 1.0

Foreword

Thank you to all the people, both DMD Diamond Foundation members and fantastic Diamond Community, who have contributed with their input to this document and support over the years which inspired us to move forward and continue to develop DMD Diamond with passion.

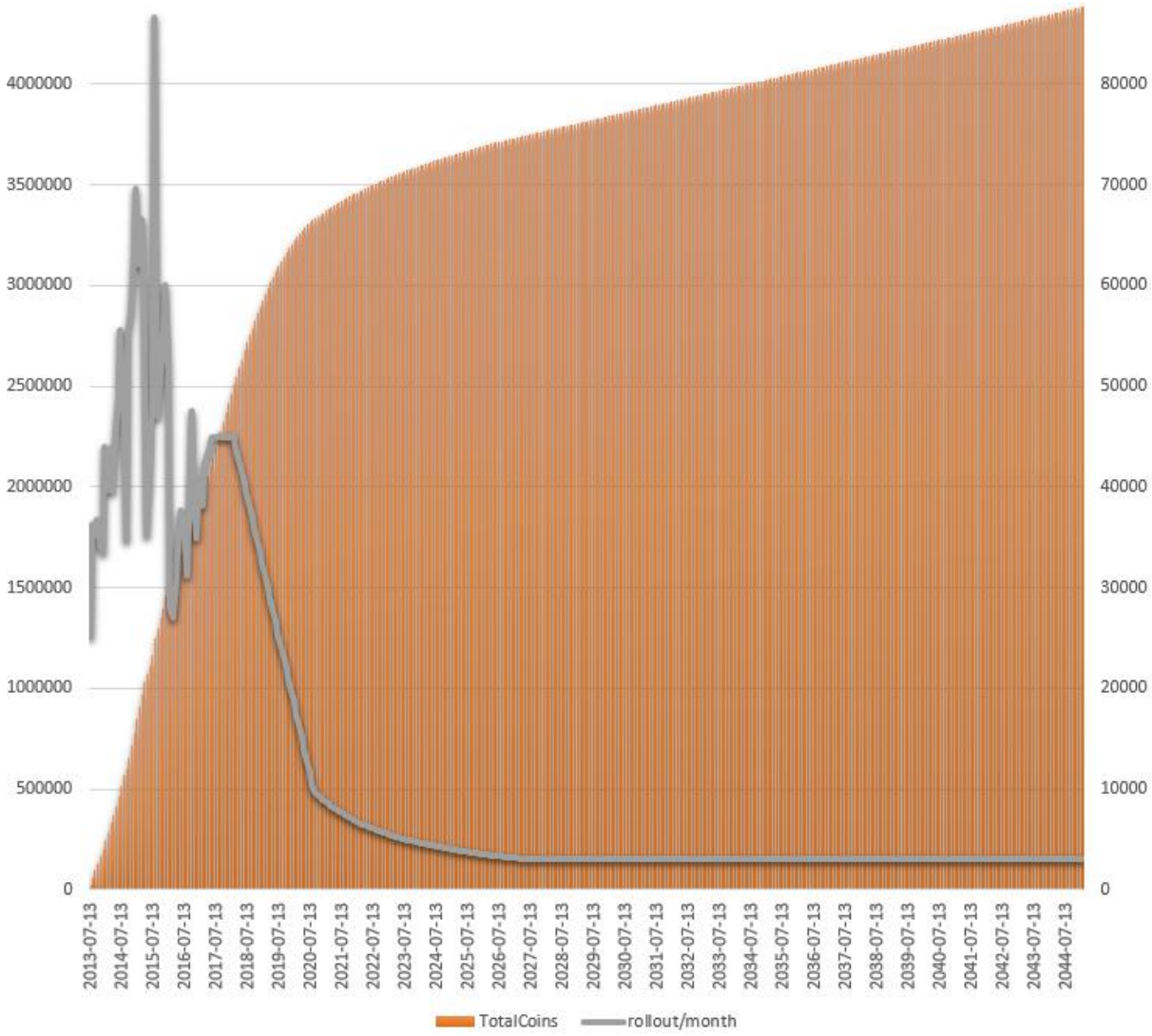
This white paper is the first draft. The final iteration will include detailed description of DMD Diamond 3.0 parameters and adjustment options for the zero micromanagement Diamond Proof of Stake engine (split and merge mechanics).

What is DMD Diamond?

DMD Diamond is a digital currency that that allows people to send money anywhere in the world instantly, securely and at near zero cost. It focuses on creating a multi entry, high rewards monetary system that empowers people to achieve financial freedom through blockchain based technology. DMD Diamond's conceptual goal is to become an ultra-scarce non-government controlled storage of wealth with software facilities that can increase that wealth over time.

Emission Model

DMD Diamond Coin rollout is one of the cornerstones of this monetary system. The emission model stays the same as in DMD Diamond 2.0, however, the introduced changes make the emission of new coins smoother and avoid sudden large reductions in yearly interest.
In the past DMD Diamond relied on both Proof-of-Stake and Proof-of-Work algorithms to govern the network. DMD Diamond 3.0 will be run by state of the art Proof-of-Stake only, while Proof-of-Work is going to be removed completely..



See https://bit.diamonds/images/rollout_graph.png for higher resolution image

Emission model in stages:

Below mentioned stages are just approximation that are to give general overview of how the issuance model is going to roll out; the dates will likely be subject to variation as all the changes are based on block numbers and not specific dates.

Stage 1: from 2017-09-01 till 2018-02-01

From Block 0 till Block 115200 the reward will remain constant at 2.35DMD.

Diamond's yearly monetary inflation will come down from the starting position of 23.7% and drop to 21.6% within 6 months time.

Please note that in the first 1920 blocks the block reward will be 0.0235 instead of 2.35 to prevent instamining with Masternodes and Proof-of-Stake and give everyone time to migrate to the new blockchain.

Stage 2: from 2017-03-01 till 2020-08-01

From Block 134400 till Block 691200 the reward emission will follow a curved line decreasing rewards slightly each month from 2.29DMD per block to 0.55DMD within 29 months. Also, a yearly monetary inflation rate will decrease substantially from 20.6% to 3.8% within that period.

Stage 3: from 2020-09-01 till 2027-07-01

From Block 710400 till block 2284800 the reduction in network rewards will slow down from 0.5 DMD to 0.157 DMD per block, while annual monetary inflation will fall from 3.5% to 0.96% within that period.

Stage 4: from 2027-08-01 - ongoing

From Block 2304000 onward the network rewards will remain at constant level of 0.1563 DMD per block. Yearly inflation will be reducing slowly from 0.95% to 0.87% in the space of 10 years.

Proof-of-Stake algorithm specification:

Layer 1 protocol's block time, without using Diamond Masternodes, is 135 seconds requiring 6 confirmations for fully accepted transaction. This on average produces 640 blocks per day. The block size will be set to 3 MB.

Block rewards are split between Proof of Stake and Masternodes, 35% and 65% respectively. The reason the Masternodes get relatively bigger share is to create

greater incentive to run high performance Masternodes that are capable of powering various additional network services.
With Layer 2 - Diamond Masternode Network - transaction will be fully confirmed and finalized in seconds. However, using Diamond Masternode network to make transactions is an optional feature. Layer 1 protocol, albeit not as fast, with default transaction speed can still process 12x more transactions than bitcoin.

Treasure Digging – striving for deflation

Reduction of money supply is a countermeasure to inflationary devaluation. The scarcer the supply, the suppliers can demand higher prices for the commodity. Conversely, the more abundant the supply, the cheaper the commodity.
After DMD Diamond reaches Stage 4 there will be a long period of slowly decreasing annual interest rate. That is why DMD Diamond Foundation will aim at creating conditions that lead to deflation in the monetary system.
This will be achieved through a new feature of Treasure Digging that involves burning coins. Burning coins is about sending them to an address which is unspendable; an address that has not derived from a private key but was rather generated manually.
Treasure Digging will give ability to search for Unspent Transaction Outputs (UTXO) that was inactive for 10 years and claim part of their balance as a reward while the rest of the coins are burned. An address that has outputs of at least 10 years old qualify to be treated as 'lost coins' where the owner no longer has access to them, could be either through lost passwords, coins sent to wrong address or any other misfortune.
As a transaction is time stamped every time the coins are moved, the counter towards 10 year check automatically resets. Active participants who utilize DMD Diamond or actively support the network by staking coins by definition reset their

clocks proving the coins are not lost. For long term holders there would be self-check safeguards at wallet startup that provide easy one click solution to extend shelf life of coins for another 10 years. Also, a single UTXO of 10 000 DMD will be immune to Treasure Digging as this coin pile size is reserved for Diamond Masternodes and as such can be used as an endless secure cold storage.
This feature will create a situation where more coins are removed from the circulation than are added to it through regular network reward system.
Another positive aspect of this feature would be incentivizing people to pay more attention to their money and encourage in active participation of securing the network.
The technical details of how this feature will work are going to be published closer to the software release date.
If Treasure Digging feature alone is not enough to keep DMD Diamond forever from reaching a total 4,380,000 coins, there will be an array of services and apps which will require burning DMD which will ensure the total number of coins is never reached. What's more, in DMD Diamond 3.0 transaction fees will be burned to create an additional deflationary effect.

Proof of Stake 3.0

DMD Diamond 3.0 adopts Proof-of-Stake 3.0 which solves many underlying issues of Proof of Stake used in DMD Diamond 2.0.
As in all implementations of Proof-of-Stake one must prove it has access to coins which grants the user ability to partake in network competition where the main prize is privilege to sign the transaction for which the winner is rewarded with new coins. 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 used a concept of Coin Age. It was meant to incentives those 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 was calculated by the weight of unspent coin (UTXO) and the time they have been dormant. It was argued the more reluctant participants would be more keen to take part in network competition and work in harmony with those who partake on 24/7 basis. Also, from monetary issuance model it created a static yearly interest rate for all participants.

However, this model has introduced some worrisome behaviours where majority of shareholders were disconnecting from the network for long periods of time, gaining enough coin age to stake and connecting again to claim their rewards. This became a reoccurring pattern. With such system in place there was little incentive to keep nodes running continuously, and the fewer the nodes the easier it was to execute an attack especially as the stakes could be compounded and coin age gathered in advance.

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.

Furthermore, as mentioned above, Proof-of-Stake based on Coin Age - which 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. To prevent this in Proof-of-Stake 3.0 the block reward was made a constant 2.35 DMD per block (initially). This was based proportional to the supply of coins maintaining yearly interest at around

25%. Block reward will be following emission curve line reducing its block value over a period of time to reflect set coin rollout.

Now only active participants can compete for the network reward. 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 this change the fewer participants the bigger the rewards as totality of the paid out reward is split among fewer participants. This measure creates much stronger pull factor encouraging the network to grow and compete.

DMD Diamond's hybrid security scheme mitigated some attack risks by having Proof of Stake and Proof of Work blocks interlacing one another making it harder for a potential attacker to corrupt the system as he/she not only had to gain majority control in staking but also control majority of the mining channel.

With the appearance of FPGA mining, which completely centralized mining, Proof of Work protocol no longer posed a credible solution to the network security and the support for this channel has been dropped. Proof of Stake 3.0 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 DMD Diamond has always been the self-adjusting Proof of Stake engine as it allowed the user to be exempt from tedious micromanagement of coin piles. With that in mind the Proof of Stake 3.0 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. Additionally, it will feature easy and automatic forwarding of Masternode rewards to your primary Proof of Stake address.

Diamond Masternodes

A DMD Diamond network consists of full nodes running as servers facilitating connectivity and transmission of updates. Masternodes is a time tested concept which was originally created to prevent decrease in number of full nodes and incentivize people to keep the network running, decentralised and expanding. Over the years as the technology matured Masternodes became ever more useful and could perform additional network services that go above what a vanilla full node could do.

Diamond Masternode is a computer (a node) that runs Diamond Wallet constantly connected to the Diamond Network and performs certain network duties/services for which it gets network rewards.

To become a Diamond Masternode you are required to send exactly 10 000 DMD towards a Masternode address and leaving it unspent which will be used as a collateral.

These coins never leave your wallet and are only used to prove you have the right to become a Diamond Network service provider. A user can at any time opt out from Diamond Masternode program keeping all the coins. There are numerous benefits to being in the Diamond Masternode program such as providing network stability and efficiency but also it reduces the volatility of the currency by withdrawing large amounts of coins from the open market which in turn aids price appreciation.

When DMD Diamond 3.0 is launched there will be two types of services Diamond Masternodes would do: transactions mixing (MixTX) and quick transactions (QuickTX).

Quick Transactions (QuickTX) - transactions sent with the use of this feature can be received and deemed fully confirmed in a matter of seconds. This is much faster than using traditional way which can take up to 2.25 minutes to achieve

one confirmation. In contrast, Bitcoin takes about 10 minutes to confirm a payment once; this makes DMD Diamond 4x faster.
Transactions Mixing (MixTX) - this service provides enhanced anonymity by allowing properly prepared coin piles, through the build in Diamond Wallet coin-mixer tool, to be sent making it much harder to trace the source address.
In the future, Diamond Masternodes are planned to enable many more services and its first instalment can be considered a foundation upon which the future network services will be built.

How much can I earn with a Masternode?

Diamond Masternodes cost money and effort to host so they are paid a share of the block reward to incentivize them.
Diamond Masternodes are paid 65% of every Proof-of-Stake block rewards, which is distributed to Diamond Master Nodes one at a time on a random basis.
Diamond Network is projected to have just a couple of hundred of such nodes running. Because of that, each Masternode will take part in many pay-out rounds each day (frequency depends on Masternode competition) making sure that investment, upkeep and servicing of Masternodes stays rewarding. This is in stark contrast to what other projects propose where one has to wait for days to get a chance of earning the reward.
There are three types of limits on the number of active Masternodes. The first limit is set by the number of coins available in the system. There will be 4 380 000 coins ever produced / 10 000 coins needed for collateral which gives us 438 Masternodes in total.
The second limit comes in a form of a psychological and financial barrier where it becomes increasingly expensive to acquire a Masternode due to limited market liquidity and coins being used or burned and not traded on the cryptocurrency exchanges.

The third limiting factor is the number of active Masternodes. When a number of Masternodes increases above certain threshold, running a Masternode might not be as profitable as having the same coins in the Proof of Stake mode only. Users then would switch back to more profitable way of earning with Diamond via Proof of Stake.

The expected point where running a Masternode is more rewarding than Proof of Stake is when approximately 25% of total coins participate in Proof of Stake, 50% of total coins participate in Masternode program and 25% of coins are inactive on exchanges or offline wallets. When the competition in Proof of Stake falls below that level block rewards are split among fewer participants, which gives them better revenue and they find blocks more often; which would be more profitable than keeping coins in a Masternode. This is self-adjusting system, profit driven, that makes sure Diamond Network will never be without Proof of Stake securing it and never be without enough Masternodes to guarantee smooth working of Diamond Network services.

Due to many variables and dynamic nature of the system such as the number of competing Masternodes per day, the block reward at any given time or number of times a Diamond Masternode is selected to perform network duties (done on a round the robin basis) it is not possible to exactly calculate the rate of Return On Investment (ROI), however, payments for a standard day for running a Diamond Masternode can be calculated by using the following formula:

$$(n/t)*r*b*a$$

n- is the number of Diamond Masternodes an operator controls

t - is the total number of Diamond Masternodes

r - is the current block reward (presently averaging about 2.35 DMD)

b - is blocks in an average day. For the DMD network this usually is 640.

a - is the average Diamond Masternode payment (65% or 0.65 of the average block amount)

In a scenario where a person owns one Masternode while there are 100 Masternodes in the network in total, an average earning for each would be around 10 DMD per day which is 3650 DMD a year or 36.5% Return On Investment annually.

What is required to run a Masternode?

There are a few prerequisites to run a Masternode.
Firstly, one needs to be in possession of 10 000 DMD Diamond coins. Diamond can be obtained from cryptocurrency exchanges. Alternatively, one can proxy-mine via Diamond Multipool, Diamond Cloud Mining or stake Diamond coins up to the necessary level.
Another requirement is to have a static IP address. Dedicated IP addresses are important so that other computers can easily and reliably connect to nodes. If a Diamond Masternode changes the address frequently it would be penalized by the network for being unreliable and would not get its fair share of network rewards.
Most people do not have static IP addresses with their home broadband service that is why the easiest way is to host a remote (virtual) server that can provide you with one. Of course one can run a Diamond Masternode from home as long as the IP address is static.
However, there is an advanced option to run a Diamond Masternode behind an Onion Hidden Service which allows for a reliable connection with the use of a dynamic IP address.
The detailed guide on how to install and run a Diamond Masternode will be published closer to the date of the official release of DMD Diamond 3.0.

The initial requirements of how powerful these computers should be will change with time as DMD Diamond ecosystem expands to host additional features and

services. However, at the beginning a simple low-end, low-powered microcomputer such as RaspberryPi will be enough to run a Diamond Masternode.

It is important to note, Diamond Masternode that acts as a 24/7 node is not required to have access to the private key of the amount held as a collateral. Only the control wallet which start the Masternode and delegates the work towards it must have access to the private key of the address with the coins.

DMD Diamond Legendary 10 and Foundation Diamond Masternodes

Since the introduction of DMD Diamond 2.0 in Q2 2014 a small percentage of mining rewards had been allocated to be used for promotion and software development of DMD Diamond. Gathered funds helped to move the project forward and continuously support project's main objectives.

With DMD Diamond 3.0 Proof of Work (mining) is no longer supported that is why the structure of continuous funding changes. It is common in other projects to tax Masternodes with 5-10% of their earnings; however, DMD Diamond will have no such mandatory fee. The protocol will pay out 100% of the Masternode rewards to the active Diamond Masternode operators. Instead, DMD Foundation will hold 5 Diamond Masternodes that will not only be used as high performance backbone nodes but also generate necessary funding to further development of the Diamond Network.

It is important to note, that the funds that had been gathered over the years had never ever been spent on paying DMD Diamond Foundation members. All the work for the DMD Diamond Foundation is voluntary. Things that have to be outsourced will be covered with coins from DMD Diamond Foundation.

All DMD Diamond Foundation Diamond Masternodes' addresses (as well as the previous Proof of Work funded network support addresses) are publicly available and open to scrutiny.

Legendary 10 addresses are unique crypto assets that had been auctioned in January 2016. Proceeds from the auction had been used to support development of the Diamond Wallet software. Instead of receiving a staking bonus, Legendary 10 holders will be given one Masternode each that is filled with *ghost coins*. These coins cannot be moved or spent, they are there as a collateral to activate a Masternode. The same *ghost coins* will power the 5 Diamond Foundation Masternodes.

Migration from Diamond 2.0 to Diamond 3.0:

Migration process starts with public release of Diamond Wallet 3.0 software. The exact block number at which the balance snapshot will be taken will be announced in advance, giving time to users and exchanges to prepare.
From then on, every user can claim their Diamond 2.0 balance in Diamond 3.0 with their private keys. It will be as easy as either exporting and importing private keys in the console or just copying over Diamond 2.0 *wallet.dat* file to the new Diamond 3.0 folder. The new wallet includes a repair option '*salvage wallet*' which will recover all private keys from the old *wallet.dat* file and at the same time will keep the encryption so it is fully secured with the old password.
Also, at the very start there will be a period of 3 days (1920 blocks) with reduced rewards to give everyone enough time to prepare their Masternode setup, transfer balances and familiarize with the new software. This is to prevent a small group of people reaping most of the Masternode or staking rewards during the transition period which would be unfair to the rest of the investors.
There is no coin swap or any hard deadline before which time everyone must perform exporting and importing of their private keys to a new DMD Diamond 3.0, however, a 10 year time frame before Treasure Digging feature can be used should be enough time to do so.

DMD Diamond Foundation will abandon any future support, side services and development for DMD Diamond 2.0 blockchain once the new one is active. After the upgrade, DMD Diamond will retain its ticker symbol (DMD) and all the exchanges trading Diamond will convert Diamond 2.0 balances into the new Diamond 3.0 ones; this will effectively delist any Diamond 2.0 coins.

The future

DMD Diamond started as a humble cryptocurrency that was focused on generating and storing wealth through in built protocols. Even though it excelled at these DMD Diamond Foundation has developed Diamond Cloud Mining and Diamond Multipool services to further strengthen DMD Diamond ecosystem and provide more entry points to this new financial system.

On the other hand, blockchain technology develops at accelerating pace with every passing year and DMD Diamond is adapting to constantly changing technological and market landscape. To stay compatible and have ongoing access to the wealth of technological advancements DMD Diamond will adopt industry standards necessary to incorporate solutions and components that would be beneficial to the future of DMD Diamond. 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, DMD Diamond (which will feature a new slimmed down blockchain with much faster loading time), will get a Light Wallet that does not require setting up a full node with the up to date blockchain to be able to use Diamond Network. At the same time, a mobile wallet for Android devices will be released so that one can access and manage their coins on the go.

The development on DMD Diamond 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. Most of

the development will be done on Masternode technology and implementation of additional features.

As the entry level of setting up a Diamond Masternode will increase over time, due to likely price appreciation, one of our main goals is to deliver shared Masternodes technology where more smaller investors could pool their coins (in a trustless and secure way) and reap benefits of providing network services.

All these new Diamond Masternode technologies will expand the capabilities of the backbone infrastructure supporting the network and will ensure that it is capable of handling the transaction loads and data storage requirements of a mass-market user base.

For DMD Diamond security is paramount that is why further development of the software will lead to significant improvements in that area. Quantum computing is real and it could soon become the biggest threat to security and integrity of all cryptocurrencies. For coins that are based on Proof of Stake algorithm this is a particularly important issue as the addresses there are reused a lot which weakens overall security of a private key. To mitigate this risk and increase protection of private keys, DMD Diamond will research the best suitable defense against quantum computer attacks and implement it as soon as it is available. In the near future DMD Diamond will feature a second more complex and more secure address schema (far beyond what Bitcoin protocol offers) which will make it much harder for brute force quantum computer attack to be successful.

What is more, DMD Diamond Foundation has outlined in the past its eagerness to pursue bespoke software solutions that target niche markets. Diamond's brand fits perfectly with the idea of rare, valuable and unique items and this will be a sector the project will see the most development in.

Apart from development work on DMD Diamond Core software, project members embark on creating services powered by DMD Diamond that will give significant boost to Diamond's usability. The project will be self-funded and the first demo will be available in Q2 2018. The software in mind will feature a multi-coin

support platform that will be a gateway to services created on top of it and directly linked to DMD Diamond.

To improve governance, DMD Diamond will utilize a Masternode voting system to decide about forwarding community proposals to the DMD Diamond Foundation. All proposals with above 50% positive voting result will be taken into consideration and feature on the DMD Diamond roadmap.

To further strengthen the position of DMD Diamond, DMD Diamond Foundation is collaborating with teams across the cryptocurrency industry to deliver next generation financial instruments. Work that our partners do will become more apparent and reinforce DMD Diamond's strong position as part of a wider cryptocurrency ecosystem.