Dash Evolution

Dash v13 - Evolution

Design Overview

Rev 1

Evan Duffield - evan@dash.org

NOTE: All Dash Evolution documentation, designs and source are in the research & development phase and subject to change. To access all materials, follow the development, or contribute, visit the Dash Evolution Github (https://github.com/evan82/dash/)

Abstract

Dash[1], an open-source cryptographic currency derived from the Bitcoin[2] protocol, added a 2nd tier to Bitcoin's P2P network architecture (Masternodes[3]) that enabled Dash to improve on the decentralization features of Bitcoin with new capabilities such as trustless transaction mixing within the 2nd-tier network for privacy (DarkSend[4]), instant transaction confirmation without a centralized authority (InstantX[5]) and decentralized governance and funding by blockchain (DGBB[6]). Other features added include multi-phased forks (Sporks[7]), a chained hashing algorithm (X11[8]) and a mining difficulty adjustment algorithm to address flaws in Kimoto's Gravity Well (DarkGravityWave[9]).

In the third major iteration of Dash named Dash Evolution (v13), additional architectural and functional improvements are being developed such as the addition of a 3rd network tier (T3) comprised of a decentralized API (DAPI) that provides users with trustless remote-access via direct HTTP and RPC connections into the Dash network that are serviced by randomly comprised Masternode Quorums, a decentralized wallet protocol that enables users to buy merchandise from the web in a trustless way (DashPay) without the need to host their own full-node or use a centralized payment gateway, a 2nd-tier high-performance shard-based file-storage system that provides improved methods for transaction confirmation and double-spend prevention (DashDrive), Primitives for representing users and accounts as objects to enable users to connect and transact with friends using aliases and rate each other to build trust networks (Social Wallet), decentralized network administration by Masternode operators (DNA), a new dynamic query language for use across Dash Evolution components providing an extensible object-based cross-tier communications standard (DSQL), addition of a historical chain of all signatures used on the Masternode network for use in secure quorum selection (Quorum Chains), improved Privacy architecture, automatic instant transactions (AutoIX) and rated-services provided by network operators such as fiat converters.

---

[1] "Dash: A Privacy Centric Crypto-currency" <https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf>
[2] Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System." <https://bitcoin.org/bitcoin.pdf>
[3] "Masternodes and Proof of Service" <https://www.dash.org/masternodes2/>
[4] "Darksend" <https://www.dash.org/darksend/>
[5] "Transaction Locking and Masternode Consensus" <https://www.dash.org/wp-content/uploads/2014/09/InstantTX.pdf>
[6] "Self-sustainable Decentralized Governance by Blockchain" <https://dashpay.atlassian.net/wiki/pages/viewpage.action?pageId=8585240>
[7] "Multi-Phased Fork ("Spork")" <https://www.dash.org/spork/>
[8] "X11 Chained Hashing Algorithm" <https://www.dash.org/x11/>
[9] "Dark Gravity Wave" <https://www.dash.org/dark-gravity-wave/>

Contents

1 Introduction

1.1 Birth of Dash: a new P2P network architecture

Dash[10], which stands for 'Digital Cash', was originally known as Darkcoin[11] and launched in 2014 as a privacy centric cryptocurrency derived from Bitcoin[12].

Dash implemented the first decentralized privacy system (DarkSend[13]) onto the Bitcoin protocol based on CoinJoin[14], the most widely used anonymization technology for Bitcoin. CoinJoin works by joining different user's transactions together in set denominations to obfuscate the transaction history.

The main problem with CoinJoin is that users need to negotiate transactions they wish to join and there's no known way to do that within the Bitcoin protocol, meaning users have to send their funds outside of the Bitcoin network to centralized CoinJoin services and lose control of their funds during the process.

Dash wanted to create a decentralized implementation of CoinJoin where users can anonymize their transactions without losing control of their funds to a centralized intermediary, and the solution concept was to expand the Bitcoin P2P network architecture to enable fullnodes[15] to provide the transaction mixing service internally between randomly selected groups of fullnodes working together in series.

An issue with this concept was that fullnodes are relatively inexpensive to run. This means the system would be susceptible to Sybil attack[16], because malicious parties could create thousands of fullnodes at low cost and 'game' the system by controlling the large % of fullnodes required that could then act maliciously to gain centralized control of user's transactions during mixing and potentially record enough transaction joins to deanonimize a user's transaction history.

[10] "Dash – Official Website | Private Digital Currency." <https://www.dash.org/>
[11] "Darkcoin - Whitepaper." <http://bravenewcoin.com/assets/Whitepapers/DarkcoinWhitepaper.pdf>
[12] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." <https://bitcoin.org/bitcoin.pdf>
[13] "Darksend | Dash – Official Website." <https://www.dash.org/darksend/>
[14] "CoinJoin - Wikipedia, the free encyclopedia." <https://en.wikipedia.org/wiki/CoinJoin>
[15] "Full node - Bitcoin Wiki." <https://en.bitcoin.it/wiki/Full_node>
[16] "Sybil attack - Wikipedia, the free encyclopedia." <https://en.wikipedia.org/wiki/Sybil_attack>

This led to the solution of requiring users to prove they had a certain level of collateral to be able to provide this fullnode mixing service, meaning gaining a majority of fullnodes would become prohibitively expensive. Dash names these collateralized fullnodes 'Masternodes[17]'.

The second issue with the design was that it is more expensive to run a fullnode that is providing a mixing service so there is no incentive for users to do so other than for altruistic reasons. But to be reliable, network services need to be highly available, with enough nodes to provide an effective service, so Dash's solution was to extend Bitcoin's principle of rewarding miners with blocks of newly created funds autonomously on the blockchain, to also reward Masternodes that provided the mixing service honestly.

This enabled Dash to create the first reliable and decentralized way to anonymize transactions in any Bitcoin based cryptocurrency and at the same time incentivize the infrastructure that provides the service. This has been highly successful for Dash with no DarkSend transactions ever shown to have been deanonimized, positive code review[18] and adoption gained in privacy focused markets along with Bitcoin, and with Dash's 2nd-tier network growing now to over 3300 Masternodes meaning Dash is second only to Bitcoin in terms of transaction throughput capability.

1.2 Phase 2: New Capabilities

With DarkSend in place, the Dash creators realized that the 2nd-network tier of Masternodes could provide a lot of additional benefits over and above the original Bitcoin network architecture and new decentralized functions and services that had not been possible before could now be created.

Now that Dash had a high-performance / high-availability 2nd tier on the network that was growing rapidly as users upgraded and collateralized their fullnodes into Masternodes to get paid for network services by the blockchain in the same way as miners, the creators started innovating new technologies using the new capabilities of the network.

The first innovation on top of the 2-tier network architecture was a method to provide instant transaction confirmations (<4 seconds on average) through transaction locking and Masternode consensus called InstantX[19], enabling to users pay instantly with Dash.

The second major change was to reallocate a percentage of the mining block reward (10%) and allowing Masternode operators to determine to whom it's paid for jobs that people propose to

[17] "Masternodes and Proof of Service | Dash – Official Website." 2015. 5 Dec. 2015 <https://www.dash.org/masternodes2/>
[18] "Darkcoin Code Review Results | The Anonymous Bitcoin ..." <http://blog.anonymousbitcoinbook.com/2014/09/darkcoin-code-review-results/>
[19] "InstantX | Dash – Official Website." <https://www.dash.org/instantx/>

the network, with secure decentralized voting on the second tier by using the collateral public key from each Masternode to sign messages from each masternode, thus creating a decentralized funding mechanism which is permanent and can care for the ecosystem for the very long term.

Dash names the system Decentralized Governance by Blockchain (DGBB[20]) and since DGBB's release[21] in August 2015 all Dash operations have been under the control of the Dash network via the DGBB system, with new proposals made and funded each month autonomously by the network. In fact since the inception of this system, the Dash network has funded the promotion of Dash conferences around the world, acquired high-value property directly from the blockchain (dash.org) and many other projects that were important to the long term success of the ecosystem.

We believe that Bitcoin is in fact the first ever decentralized job network to exist, if we define jobs on the bitcoin network as actions by network participants who are paid directly and autonomously from a purely decentralized source such as the block reward.

Dash unlocked this concept by adding a second job, the masternode operator, which runs infrastructure for the network and is compensated.

These masternode operators exist in a secondary market within the larger primary mining market and have an equilibrium with the amount of capital available to fund the infrastructure.

1.3 Phase 3: Dash Evolution

With a new type of scalable P2P infrastructure and these new decentralized technologies in place, we have identified several new changes to the network architecture that we can make to provide a new level of capabilities to bring cryptocurrencies closer to mainstream users and we are naming this iteration Dash Evolution.

The first major change in Dash Evolution is a Decentralized API (DAPI) that is implemented by using small processing groups of masternodes hardened by proof-of-work randomization. Users can execute simple requests over HTTP, which update or retrieve their information and these small clusters perform the work as a group action, executing the event many times and signing the result.

This opens up a cryptocurrency, for the first time, to decentralized and trustless use directly from the World Wide Web, without reliance on any individual intermediary to handle user's funds.

[20] "Self-sustainable Decentralized Governance by Blockchain ..." <https://dashpay.atlassian.net/wiki/pages/viewpage.action?pageId=8585240>
[21] "V12 Release | DashTalk." 2015. 5 Dec. 2015 <https://dashtalk.org/threads/v12-release.5888/>

Merchants can integrate Dash Evolution into their eCommerce store as easily as they do with centralized services like PayPal or Google Wallet, whilst receiving a faster and cheaper service that lets them transact directly with their customers without having use an intermediary payment gateway or face increased cost and complexity to integrate and maintain their own full-node infrastructure.

Users can check DAPI result signatures against a deterministic quorum-chaining algorithm similar to that of the blockchain, but designed to preserve the historical and current state of the masternode quorum groups on the network. The quorum-chain begins with one masternode (the source masternode) signing a message, which adds the new masternodes to the next quorum-chain entry and so on. As long as the user has the source masternode(s) keys, they can independently check the masternode quorum-chain in a secure and efficient way.

By requiring each second-tier node to have access to a specific amount of storage on the network, we can begin to create a decentralized storage system capable of vast storage capacity. This can allow the storage of metadata and other network-related data to be stored on the network on behalf of the users, which can then be retrieved privately at any time in the future. Writes to this file system are executed in a similar way, requiring all/most of a quorum to agree on what is being changed in the decentralized file-system.

Using DAPI and the decentralized file-system, we create easy to use primitives such as users, groups, accounts and features such as private messaging, group messaging and name-based payments. Users can move from device to device and by querying the data stored privately on the network, automatically syncing all of this data, allowing for a streamless centralized-seeming design, which is infact decentralized start to finish.

Evolution also consists of a lot of other new features to make cryptocurrencies easy to user and access to mainstream users and whilst keeping Dash fully decentralized and scalable which are given an overview in this document and more specific details in separate documents for each major area.

2 Multi-Tier P2P Network Architecture

In most P2P systems, all nodes on the network use the same software and have the same role. We expand on this concept by introducing differentiated roles for the nodes on Dash's P2P network. The different roles allow the network to be increasingly robust and self-sustaining. Nodes can do many things on the Dash Network such as running a collateralized infrastructure and voting on proposals for governance and funding. These proposals in turn determine the direction of the currency and the network in a decentralized way.

Miners form the first tier on the network. Their job is to create and validate a permanent and immutable record of transactions by creating blocks in Dash's public blockchain. For this, they are paid a portion of the block reward. Miners also ensure that approved budget proposals and Masternodes are paid. These Masternodes form the second tier of the Dash Network and provide vital infrastructure, including storage and processing power, for the network. The third tier runs on external hardware (browsers, phones, etc) and connects to the Dash Network via a decentralized API (DAPI).

2.1 First Tier - Mining and Full Nodes

The first tier of the Dash Network consists of miners and full nodes. Miners act normally, as on any proof-of-work based P2P network. In addition, we have the ability to support undifferentiated full-nodes, which can validate transactions and keep up to date with the current state of the blockchain.

Miners share the reward with the rest of the miners according to their contribution to the network itself. In addition, they must honor additional payments out of the blocks they work on via connecting to the daemon and checking the block template. These extra payments service the network by paying for the second tier infrastructure and decentralized funding mechanisms.

2.2 Second Tier - Infrastructure

A stable infrastructure is provided for the network by special nodes we refer to as Masternodes. These are full nodes on the network that are required to meet specific minimum requirements with respect to hardware, configuration (certain ports open, etc.) and participate in regular software updates. By utilizing collateral transactions (unspent inputs signed by the operator for actions), we can organize a secure group of users to provide services for the network, allocate funding, and govern the currency.

The second tier is essentially its own market within the larger mining market. As a market-based solution, a natural equilibrium is maintained between the number of Masternodes running and the payment each Masternode receives from the blockchain.

To provide services for the network, the second tier operators run specific software (the normal Dash daemon configured specifically for Masternode operation) which allows the users to connect to them using a decentralized API (DAPI). When connected to this DAPI, users can do various things on the network like friend others, update their profile, send money, and so forth. These features use the new DashDrive system, which allows secure reading and writing to the decentralized file-system.

2.3 Third Tier - Users

The third tier is comprised of the end-users of Dash. They have no direct access to internal communication happening on the network. Instead, they connect to the network through a decentralized API which allows them to receive secure, fast and lightweight access to the network. By using a REST API, we can allow low resource, friendly access to the network.

To access the features of the network, users will connect to a round robin DNS https://dapi.dash.org/ which points to the entire second tier (Masternode network). A simple open source script that takes the Masternode list and updates DNS entries will be available to anyone who wants to provide this service. T3 developers will then be able to use many known DNS entries in their software for robust decentralized access to the network.

After connecting to the network, users can submit tasks they would like to execute using a simple REST-based interface. As an example:

Accept Friendship

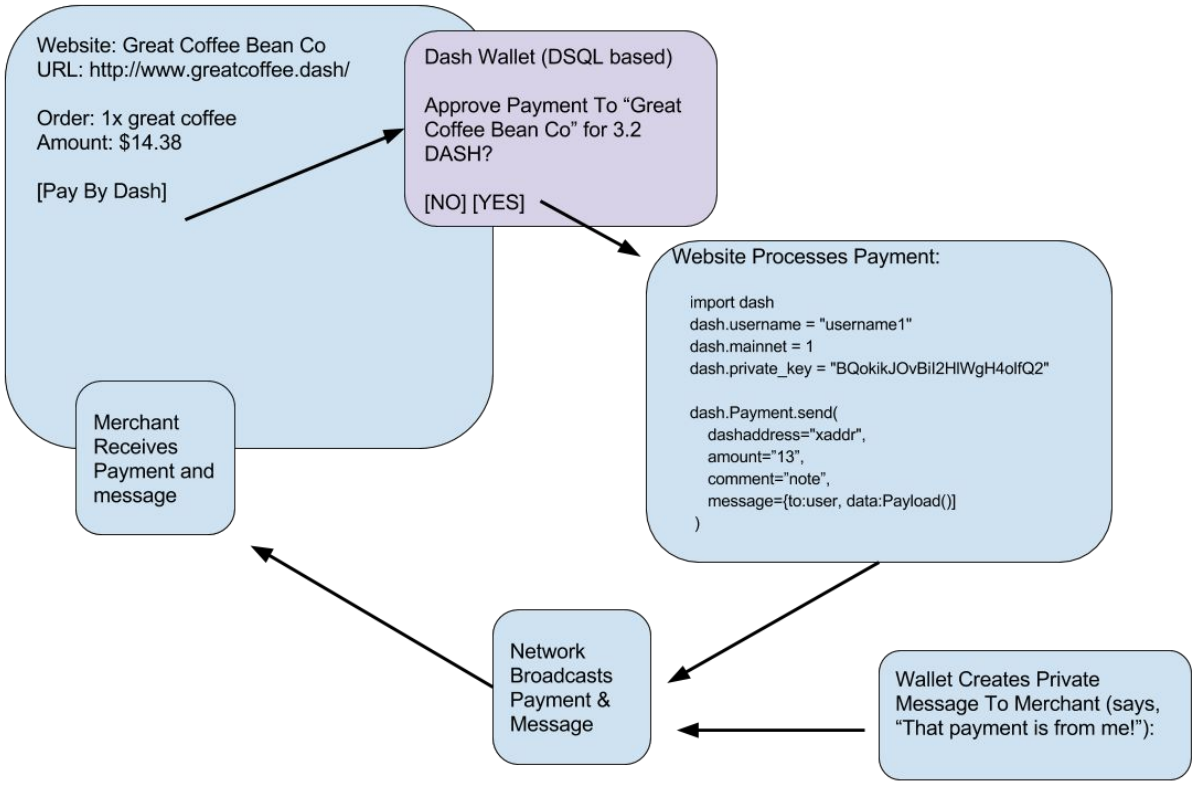
```
import dash
dash.username = "username1"
dash.mainnet = 1
dash.private_key = "XEMpbsG36957nTkrxDZTL..."

dash.Friend.acceptInvitation(
    id="393773938"
 )
```

Random groups of Masternodes are selected by the network to simultaneously perform the work users ask to be done. These groups are known as “quorums.” After doing the work, each member of the quorum will sign and return the results and signatures to the end-user. Users can then be sure the work was performed correctly without tampering..

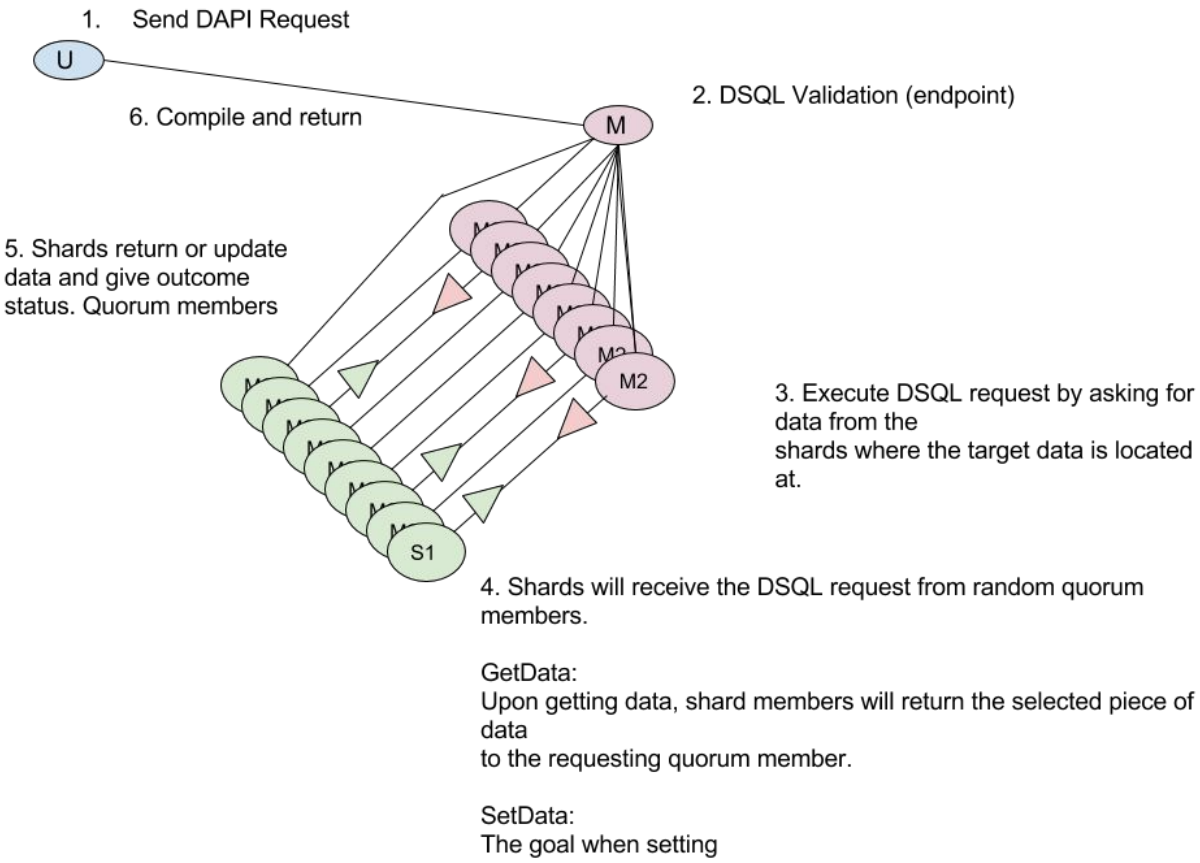
3 Decentralized API

Users will be able to buy goods directly from websites without using any centralized intermediary services. We seek to serve many users in a completely decentralized way using only the second tier, operating similar to a Backend-as-a-service system (BaaS), but fully decentralized. Merchants will use an SDK when accessing the Dash Network from their site. This SDK enables users to click a “Buy with Dash” button, which opens a connection to the Masternode network and makes a payment via DAPI.

3.1 DAPI eCommerce process



3.2 DAPI Internal Resolution



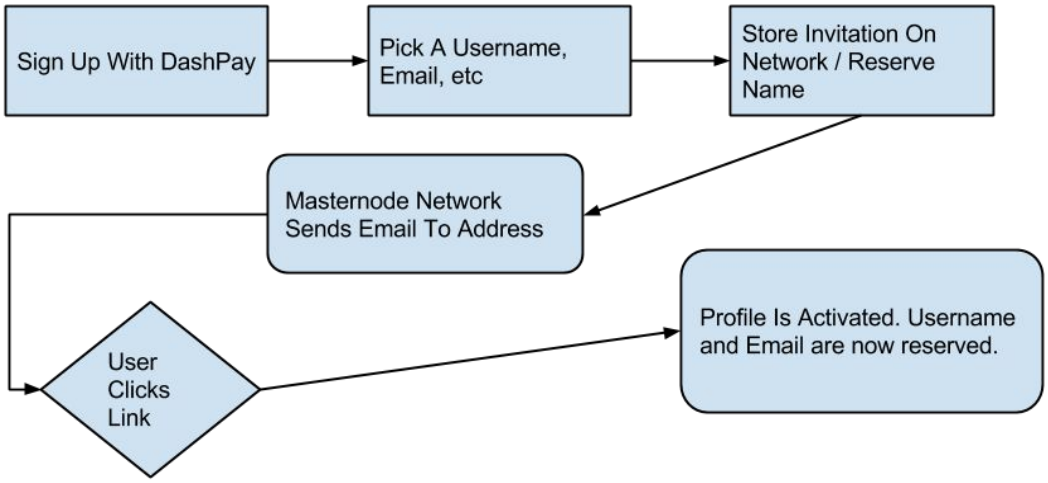
NOTE: For more information on DAPI please refer to the doc ‘DAPI: Decentralized Application Programming Interface

4 DashPay

NOTE: Please refer the document “DashPay Decentralized Wallet”

5 Social Wallet

Users will have a username and password which they use to access the network. The username will be reserved by using features of DashDrive and the password (8-12 words) will be used to create an HD wallet. A primary key will be pulled from this HD wallet, which is used to retrieve information about the user from the network. All communication with the network is protected by using these root communication keys.



To assist in adoption, users will utilize wallets with constructures designed to make working with the network much easier. The goal is to provide an experience similar to a centralized website, but without any centralization.

Users will maintain a friends list on the network, exchange future keys to use privately, create groups for companies and other uses, and create shared accounts so that users and funds can be added and removed. With this combination of features we can achieve a level of user experience that was previously reserved for large-scale centralized systems, with the added benefit of decentralization where users keep control of their funds and don't need to trust any central entity or be exposed to any single point of failure.

Users will also be able to rate others on the network in a nearly-permanent way. Once two users have done business with each other, they may add feedback to each other's profiles. This helps future users make informed decisions based on reputation.

Other notable changes include the ability to send immutable transactions instantly and privately using advanced features of DashDrive. All transactions are instantly confirmed, so that users

don’t have to wait long periods for multiple confirmations on the blockchain. All transactions that are successfully written to DashDrive will be successfully archived in the blockchain.

For more information on Social Wallet, please refer to the doc ‘Dashpay and Social Wallet’.

5.1 Fiat Conversion

Dash Evolution will also give users the ability to convert to and from fiat using using converters. These are special users that provide another service for the network and are paid a percentage of the transaction to process it. Converters will be rated by users who do business with them, and this reputation will be crucial in helping other users decide which converters are most reliable and trustworthy. The result will be a safe and global fiat conversion network.

6 DashDrive

Each member of the second tier will be required to have a specific amount of storage space in order to power the DashDrive filesystem. By sharding the storage via the collateral transaction hash, we can define 1024 different shared storage devices on the network. We use 1024 because, we can identify shards by using the first 10 bits of a unique hash per storage object. For example, with a 40GB allocation requirement, the network can enjoy about 40960GB of storage space. When users interact with the network they will transmit information to be stored on DashDrive via the decentralized API.

For redundancy, each shard will be stored multiple times on the network. For example if the network has 5000 Masternodes, we will store each item ((5000/1024)+seed_count) times.

DashDrive supports a few advanced features such as transactional commits, where users can require multiple files get written to different destinations on the network. If any write fails, the entire commit for all files will be reverted.

In addition, reading or writing files is only possible when a user has access to a given file, such as their own profile page. When trying to read files a user does not have access to, they will be denied access.

Writing files can be done only by having enough quorum signatures, and can be used to do maintenance or allow users to update information on the network.

6.1 Masternode objects

Masternode objects are stored on all shards on the network for quick access from any node. There are only a few thousand of these servers (maxing out at 21k), so the file overhead will be

minimal. Masternode keys will constantly be used on the network, so these files will be cached by the software in RAM, creating a Masternode list functionality.

6.2 Quorum Chains

QuorumChain is a historical chain of all signatures that have ever been used on the Masternode network. This historical record allows us to check all signatures that ever been used on the Masternode network and allows the network to decide which Masternodes are qualified to be in a quorum at what time.

How it looks:

```
/quorum/chain/1 => {
    'participants' => [mn1],
    'count' => 1
    'block-start' => 2 (1 + count),
    'block-end' => 3,
    'signatures' => NULL
}

/quorum/chain/2 => {
    'participants' => [mn1,mn2,mn3,mn4],
    'block-start' => 2 (prev.blockstart),
    'block-end' => 6 (2 + count),
    'signatures' => mn1.sig
}

/quorum/chain/3 => {
    'participants' => [mn1,mn2,mn3,mn4],
    'block-start' => 6,
    'block-end' => 10,
    'signatures' => mn1.sig, mn2.sig, mn3.sig, mn4.sig
}
```

Calculation of the QuorumChain uses a random number generator seeded with a historical proof-of-work hash to sort an array of Masternodes. Masternodes are simply added and removed from this list by writing additional files to DashDrive by majority quorum.

6.3 Users / Groups / Accounts

All DashDrive objects are binary files which are written to DashDrive on one of 1024 shards. The files are written as a vector of integers and char vectors, which store fields for user data. This allows users to have many fields such as username, password, friends, etc.

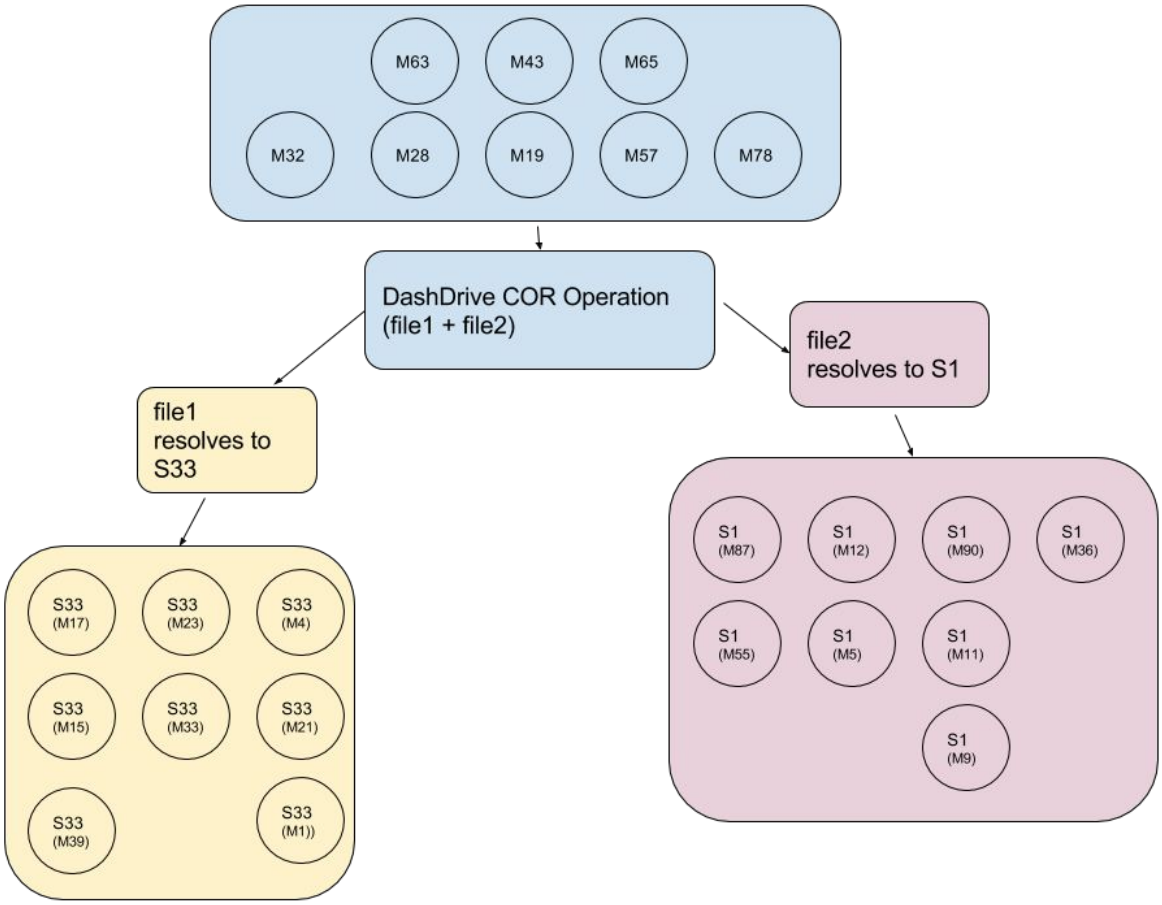
6.4 Double-Spend Prevention - Commit or Rollback

Double spending is not possible on the Dash Network due to the “Commit or Rollback” (COR) feature of DashDrive. After sending a transaction to the network, it will be written to DashDrive and the inputs will be reversed via usage of the filesystem.

```
CTransaction()
(
        Input(1) => /dashdrive/inputs/hash1,
        Input(2) => /dashdrive/inputs/hash2,
        Input(3) => /dashdrive/inputs/hash3,
)
```

If at any point a write to DashDrive fails, the earlier writes will be reverted back to the state before the commit started. This allows two users (or one attacker) can attempt to write a transaction inputs, being that inputs are unique file locators on the network, only one will successfully be able to write the transaction commit. In addition to reserving resources on the network, DashDrive stores the whole transaction history across the shared filesystem, while awaiting archival in the permanent blockchain.

Example COR Operation



6.5 Guaranteed Resources - PoSe

NOTE: This section is currently being written/rewritten

7 Decentralized Network Administration

The Dash Network is run by a decentralized administration workforce, known as the Masternode network. This is a decentralized P2P network comprised of thousands of people that together can administer the network, remove threats, deal with attacks and reduce the load and strain on the network by taking appropriate actions.

In v13 the developers have a whole new toolkit for interacting with the currency as well. All users on the network will act under a single private identifier, or username. This username is able to carry historical transaction ratings for each transaction it completed. This can be thought of as an eBay-like feature, where merchants carry historical ratings and users base their business dealings on those ratings.

Eventually ratings will be able to be analyzed using a graph similar to pagerank[22]; by utilizing an algorithm like this we can build the first trust network on top of a decentralized currency. The network can automatically calculate these trust numbers via Masternode Quorum maintenance and assign them to user profiles. Users will then do business on the network according to these numbers.

Based on the shared infrastructure and quorums, Masternode operators will use a SQL-like language called DSQL. This will allow the Masternode network to vote to ban malicious users or even entire networks of related attackers. After ridding the network of these attacks, we can restore the trust network to its pre-attack state.

In the example of a DashDrive data write attack, the Masternode operators will be able to rewind the DashDrive changes on the network to reverse the damage. They can also prune and undo data-adding attacks on the blockchain. This would be done using majority quorum actions, where a large percentage of the network was required to vote, making it a highly secure operation.

Transactions on the network are free and users will have a certain (limited) amount of network processing time they can use. Larger users will be able to utilize additional processing time on the network by paying a fee that is added to their account.

By definition Network Administrators run Masternodes for the network on the second tier. Each year they prove they own one Masternode, which is recorded in their file. They can then vote on executing various commands on the network to administer it. For example, there might be votes to ban malicious users or nodes from the network.

[22] "Lecture #3: PageRank Algorithm - The Mathematics of ..." <http://www.math.cornell.edu/~mec/Winter2009/RalucaRemus/Lecture3/lecture3.html>

8 Privacy & Fungibility

NOTE: The full details of this new system will be discussed in a separate paper.

9 Automatic Instant Transactions

Since the introduction of InstantX[23], Dash has established itself as the fastest crypto-currency on the market. However, in the current system (v12) this service has to be requested in the wallet. This will no longer be necessary, as this latest implementation of Dash will provide an automatic InstantX service for all transactions on the network. This will also be covered in greater detail in the DashDrive paper.

10 Decentralized Funding And Governance

Decentralized funding and governance of the currency are very important foundational components of a system that is sustainable and can scale without issue. To achieve this we must add a form of decentralized funding for paying for things like the website maintainance, core development, business development and promotion.

Decentralized financing is implemented by adding a proposal and voting mechanism to the Masternode system. By adding such a system we have a democratic, smart, and efficient funding system that will leverage our Masternode operators to pick which budgets to fund and which not to fund. As Masternodes change hands, the control of the currency will move with them, so there will always be a decentralized group of people watching over the currency and network.

As a network, we can choose to finance anything we want, such as large advertising campaigns targeted to specific regions or demographics for attracting users, or new developments. We can develop specific markets in a specific order to have the greatest effect.

Good, decentralized governance of the currency is very important since it gives the user base and investors a clear sense of direction. In the case of Bitcoin, there is no clear system of governance and as a result chasms have formed in the core team and in the community. To avoid that, we give each Masternode operator one single vote on each proposal. We can then use this system and take multiple votes about specific options for advancing and improving the currency. This is all done in a completely transparent and trustless way.

[23] "Transaction Locking and Masternode Consensus" <https://www.dash.org/wp-content/uploads/2014/09/InstantTX.pdf>

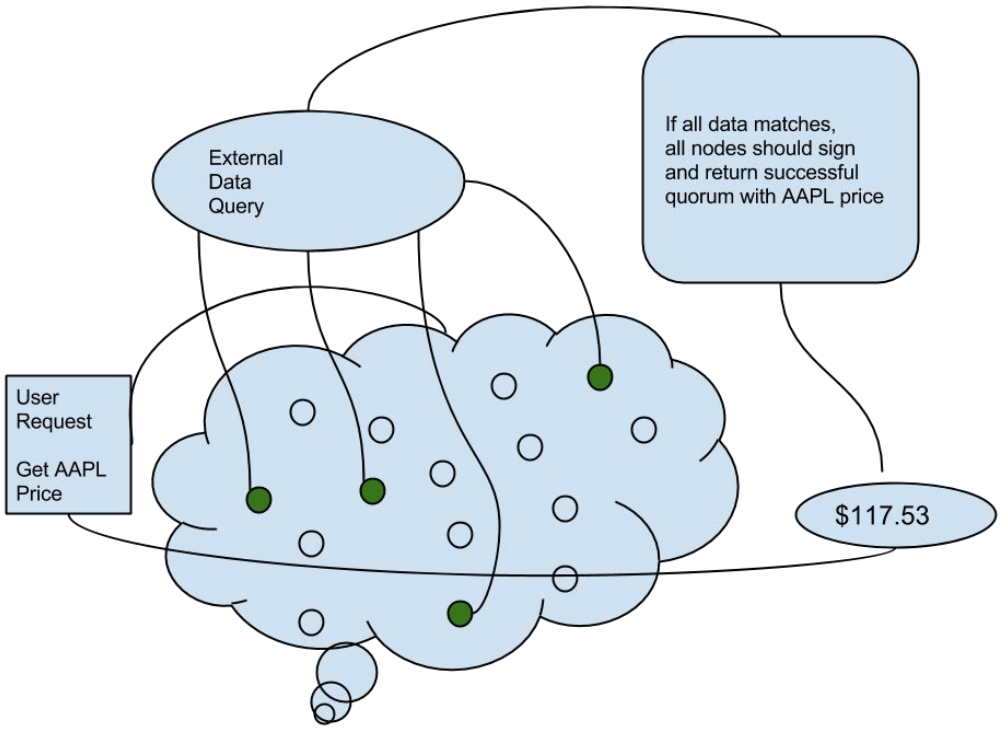
The decentralized budget system will be well funded because the Dash protocol ensures that ten percent of the total currency emission every month is automatically redirected to support the ecosystem without relying on centralized sources of financing or altruism from the community. Funding is very important, because as a project gets more important, it will require better financing to remain competitive and to be properly maintained.

Market Cap	$17M	$50M	$100M	$500M
Budget Funding Per Year	$315,360.00	$927,158.40	$1,854,316.80	$9,274,737.60

As you can see, our financing for the project grows as the value of the Dash currency increases. This results in a virtuous cycle: decentralized funding goes to finance network development which creates price appreciation. This increase in the value of the Dash currency makes more funding dollars available to further enhance and develop the network, which drives more currency appreciation. This will allow us to completely finance development, marketing, legal and infrastructure costs throughout the life of the currency.

The budget system is also real-time, so Masternodes can trim the fat to keep the budget as lean as it can be 24/7 and votes can be changed at any time. In the event that a project with a recurring budget fails to deliver the appropriate results, Masternode owners can always change their votes to “no,” and if enough Masternode owners do so, that particular project will stop receiving funding.

11 Masternode Quorums



When we talk about information in the 1st tier of Bitcoin core, we talk about processes that all clients on the network can check and verify. These must be locally verifiable things so that all nodes can do the same verification. If one node rejects something, all nodes should also take the same action when checking the data. This is the basic idea of how Bitcoin operates, however this type of logic is quite limited.

Nodes can only provide information that they directly have their hands on such as: is this signature correct? Is this hash correct? Is this proof of work correct? Does this script check out? If these things are true in one place in the network, they are true in all places.

This type of logic is obviously limited. We propose using a technology called Masternode Quorums, will be used extensively throughout Dash in order to provide a robust system that has never been possible with other types of logic.

Masternode Quorums are powerful because groups of Masternodes can now do tasks that might not be possible to execute over the entire network at once. If the ten Masternodes selected for a quorum are successful at getting the same information, then the entire network

can consider that information true after that point. To stop Masternodes from colluding, we base the deterministic selection algorithm on the proof-of-work hash. This provides an unforgeable base for a secure set of Masternodes to provide quorums.

As an example, Alice issues a command to get the current price of the stock AAPL for an on-blockchain bet. She bets that on Dec 12, 2018 AAPL will be greater than $3000. When this time passes, the network takes a past block hash, then using deterministic math, the whole network selects the same set of Masternodes for this task. Ten Masternodes then become active and hit a public API on the internet.

When these Masternodes are activated, they trigger a python script which has a list of APIs. We can do things like:

- Query stock prices
- Check the news, temperature, RSS feeds, etc
- Broadcast transactions on the Bitcoin network, Litecoin network, etc.
- Download a webpage and search for a piece of data in it. With this you can ask things like “On Google/news/page.html does it have ‘News Item 1’”, the answer will then come from the network.

Another example usage is InstantX[24], where we ask ten Masternodes “Is this transaction valid and can you lock the inputs on the network so double spending is impossible?” The network then either answers Yes or No.

This also allows for the Masternode network to serve as a decentralized oracle about anything and add scripts to transactions that reference their answer and contain their signatures.

11.1 Masternode Quorum Security

The probability of winning the election will be 1 in N Masternodes. Currently the network is supported by over 3300 Masternodes. Each Masternode has a probability of 1 in N of winning the election. Therefore to attack the network, the election process must select all of the attacker’s Masternodes.

We will consider an attack on the transaction locking system by purchasing Masternodes in order to rig the voting system. For simplicity we will use a network consisting of 1000 Masternodes.

[24] "Transaction Locking and Masternode Consensus" <https://www.dash.org/wp-content/uploads/2014/09/InstantTX.pdf>

Probabilities of attack can be calculated by the chance of a Masternode being selected as the winning node for a given block (1/1000). To subvert the system an attacker would have to operate all ten Masternodes that won a given election.

At a cost of 1000 DASH per Masternode, it's prohibitively expensive to attempt to attack the transaction locking system. To gain a probability of 1.72% of being selected for a specific block, one has to control ⅔ of the Masternode network (see Table 1 for more information). To gain control of ⅔ of the network, an attacker would need to purchase 2000 Masternodes (requiring the purchase of two million DASH).

Attacker Controlled Masternodes / Total Masternodes	Probability of success $\prod_{i=1}^{n}((r-(i-1))/(t-(i-1)))$	Dash Required
10/1010	3.44e-24	10,000 DASH
100/1100	2.52e-11	100,000 DASH
1000/2000	9.55e-03	1,000,000 DASH
2000/3000	1.72e-02	2,000,000 DASH

Table 1. The probability of a successful attack given the attacker controls N nodes.

Where:

n is the length of the chain of Masternodes
t is the total number of Masternodes in the network
r is the number of rogue Masternodes controlled by the attacker and it is $\geq n$
The selection of Masternodes is random

Considering the limited supply of DASH (6.03 million at the time of writing) and the low liquidity of the market, it is virtually impossible to obtain a large enough supply to succeed at such an attack.

In the case of an attacker attempting to rig the voting system in favor of the wrong transaction lock (i.e. the lock that isn't propagated across the rest of the network), the network will form an irreversible lock causing the transaction to the merchant to be invalidated. The merchants client in question will permanently show an unconfirmed transaction due to a double spend and will never show the transaction was instantly validated.

11.2 T3 Masternode Quorum Actions

NOTE: This section is currently being written/rewritten

11.3 Decentralized Governance of Block Reward Allocations

On the current Dash Network, there are defined allocations of how the Dash block reward is split between payments to Masternode operators, miners and decentralized budget system. These were defined ahead of time and might not always meet the needs of the currency in the future. Masternodes will be able to form majority quorums using specialized commands to vote on changing these numbers when required on the network. Decisions to change key parameters will require an overwhelming majority, such as 70-90% of the votes actively voting on such a change. This will allow the Masternode network to add more Masternode servers if the load on the network is too high or add more decentralized funding if the network requires that.

12 Scalability and performance

12.1 Incentivized Scaling

Within the Dash ecosystem, we have an incentivized Masternode network that carries the load of the network. These operators are properly incentivized, so we do not have to worry about blocksize limitation or the bloat that would be caused by allowing millions of transactions a day. A larger blockchain simply means that Masternodes will need to be hosted on servers with greater storage capacity. The increased cost of renting these servers will be more than offset by the price appreciation that comes from mass adoption.

When limiting the number of Masternodes by requiring specific amounts of collateral to launch one, the network is therefore limited to an easily calculable maximum number of Masternodes. For example, with 5.5 million DASH in existence and 1000 DASH in collateral required per node, we have an absolute maximum Masternode count of 5500. If we expect that 50% of the coins in existence will be used to collateralize Masternodes, this would give us a soft limit of about 2750 Masternodes.

If each action requires five Masternodes to do the work in parallel and each action takes 10ms, we can determine the amount of work the network as a whole can do before being overloaded. Using these assumptions, we can demonstrate how the Masternode network will allow us to scale indefinitely.

Required DASH per Masternode	DASH Price	Revenue Per Node / Cost Per Month / Dash Per Day	Network Actions Per Second	Network Storage / GB per [2]	Masternode Count [3]
1000 DASH	$10	$160 / $20 / 0.6	275,000 [1]	5.5 TB / 10 GB	2750
500 DASH	$100	$800 / $100 / 0.3	1,000,000 [4]	44 TB / 80 GB	5500
250 DASH	$1000	$4100 / $400 / 0.15	4,000,000 [5]	176 TB / 320 GB	11,000

1. 10ms per action, a quorum size of five and 50% utilization for other tasks
2. Average redundancy of 5x
3. 50% of all coins used for Masternodes
4. 5ms per action, a quorum size of five and 50% utilization for other tasks

5. 2.5ms per action, a quorum size of five and 50% utilization for other tasks

When starting a client that uses the decentralized API, the client will complete a series of 10-25 network actions, depending on what services the client is using. It follows that if the network supports 275,000 actions per second (APS), that should allow between 15M and 45M users to utilize the network's services. As the network scales up, we can achieve an upper cap of nearly one billion simultaneous users.

12.2 Access Speed Over Time

With all user data stored on T3 and accessed via secure API, the accessibility of the service will never begin to suffer from too many users due to blockchain bloat. A larger blockchain does not mean longer sync times for any devices connected to T3. Accessibility to this system will largely be determined by the state of the hardware in T3 and the number of users currently hitting the API.

12.3 Fee Structure / Block Size / Spork Protection

We believe that an incentivized full-node infrastructure, decentralized governance and funding will allow us to have no blocksize limitation for unlimited growth. We don't want to hinder this growth by external limitations that were designed to protect the network from the incomplete incentive models used in the Bitcoin ecosystem.

Fees will be kept near one cent per transaction or less, regardless of the value being transferred. This opens us up to the possibility of spam attacks, so as a precaution, the network will be able to trigger a multi-phase fork (“Spork”[25]) to stop spam attacks on the fly. The network will do this by automatically raising the minimum fee for transactions until the attacker runs out of money. After the attack has been deflected, the network will return to normal operations.

Such a solution is only one option. Masternode operators could also eventually reverse this type of attack by using majority quorum commands to clean up the blockchain by deleting the spam, then ban the users who performed the attack.

[25] "Multi-Phased Fork (“Spork”)" <https://www.dash.org/spork/>

13 Improvements to Decentralization

When designing a cryptocurrency we should strive to have as little centralization as possible. There are many places a cryptocurrency can become centralized and thus prone to being attacked. The most important areas that we've identified are:

1. Centralized database (**Ledger**) - This is the problem Bitcoin solved by decentralizing the ledger in a trustless way.
2. Core Development (**Dev**) - Must be open-source and not centralized to the will of a few powerful individuals. (i.e., Decentralized Governance via voting to make decisions)
3. Infrastructure (**Infrastructure 1**) - If the network hardware is mainly provided by one company or person that leaves the network prone to monitoring and weak to attacks.
4. Lack of Infrastructure (**Infrastructure 2**) - If the level of hardware providing public service is not great enough to support the users, that can leave the currency prone to DOS attack, make syncing slow and creating other similar problems.
5. Lack of decentralized funding (**Funding**) - If a project is receiving its financing only from centralized sources that can leave a project weak to coercion or undue influence from these sources.
6. Centralized mining pools (**Mining**) - One issue that's always plagued cryptographic currencies is the rise of pooled mining which leaves the system weak to attack by a party or small group of parties that has more than 51% of the hash power.
7. Centralized decision making (**Decisions**) - By not having a clear way to resolve disputes, the currency is subject to stagnated development or control of a minority party.
8. Centralized money transfer (**MT**) - If all points of entry into the ecosystem from fiat are controlled by centralized companies, that's a weakness as well.

It is clear that when developing a cryptocurrency, there are many weak areas that must be eliminated in order to make the currency more robust and less prone to attack. We want to design a currency that isn't weak to any of these types of attacks.

	Ledger	Dev	Infrastructure 1/2	Funding	Mining	Decisions	MT
Ripple	✓	x	x/x	x[2]	✓[3]	x[4]	x[5]
Bitcoin	✓	x	✓/x[1]	x[2]	x	x	x[5]
Litecoin	✓	x	✓/x[1]	x[2]	x	x	x[5]
Dash	✓	✓	✓/✓	✓	✓	✓	✓

1. Bitcoin and Litecoin suffer from decreasing full node counts due to a lack of incentive to run a full node and rising costs of supporting a growing network.

2. Centralized funding through one company or organization.
3. 51% attacks are no longer a threat. Look at the DashDrive paper for more information about this.
4. Dash is the only cryptographic currency that has clear guidelines for how the network makes decisions by using the Decentralized Governance within the Decentralized Budgeting System.
5. Dash will provide a selection of third party vendors to convert fiat to Dash, and vice versa, instead of requiring users to go to centralized sources to convert fiat.

Dash is not perfect in all of these areas, but we're trending toward a much higher state of decentralization. In the rest of the documentation we touch on improving these weak areas in the coming years to design something that's almost completely decentralized.

14 Design Improvements

There are some known issues with this design that can possibly be addressed before the launch of Dash Evolution. This section will serve as a starting point for brainstorming additional improvements to the technology.

- When sending money to known aliases on the network, the payments are completely public and transparent. At all other times on the network, addresses are provided to all parties in a transaction via encrypted private messaging. Even public transactions are anonymized in the second phase of blockchain archival, so the transactional mapping would need to be stored permanently and sniffed off the network at the time the transaction was sent and off the specific shards involved.

15 Conclusion

Bitcoin is a revolutionary currency and a brand new way of thinking about money, but we believe there are parts we can improve on. We introduce a series of design changes to the foundational code, which attempts to correct the incentive issues with the Bitcoin network and thus helping scalability, governance capability, funding mechanisms and ease-of-use.

Dash solves these issues by:

a. Allowing scalability by incentivizing the network in various ways
b. Decentralized funding, to finance operational requirements of a currency without risking the decentralized sovereignty of it
c. Decentralizing governance, resulting in a clear, decentralized, and trustless decision-making process
d. Easier, internet-friendly access via the first decentralized API for anyone to access the network without having to run and sync a full node, or rely on centralized services

Since all users will be utilizing the services through the 3rd tier, we simply need to make the interface they use static and our network can change radically on the inside without disturbing world wide commerce outside of the Dash Network. This allows us to try adventurous new ideas and update the network frequently without disrupting the user experience, to keep Dash as a leading innovator in decentralized cryptocurrency technology.