DESIGN CENTER NET

Directory

Chapter I DCN Community

Strong and Vibrant DCN is evolving symbiotically with the Zclassic project, with our combined community numbering around 1,000 forum members, developers, miners, traders, long-horizon investors, partner organizations, exchanges, bloggers, etc. As a fully open and inclusive project, all kinds of contributions and support have flowed in to DCN from around the world, and this impromptu yet consistent collective is one of our defining features as a system. Our community already has an enduring history not only of positive relationships and friendly interactions but also of spontaneous support and engagement emerging to prevent or solve disparate problems.

1.1 The Ethics of Open Source

Open source projects can take on an evolving and fluid set of ethics, however the founders of this one hope to keep the community centered on the principles of DCN, hence our name. We are developing a system we hope will be used for peaceful collaboration, permissionless innovation, and maximum inclusion. We hope our legacy will be a massively positive surplus to society, and we personally reject working with anyone intent on harm, either physical or through fraud.

1.2 DCN Support

DCN Support refers to a community of DCN Developers and other distributed IT professionals committed to advancing the technology and offering basic assistance to users. This network will be funded by the DAO, and will serve to make DCN’s technology the most intuitive, easy to engage with in the ecosystem. DCN Support will also consist of a network of contributors from various industries who are committed to serving as ambassadors, mentors, and support for DCN Contributors. See more in subsequent DCN Community sections. DCN Support is a commitment that DCN is structurally designed to foster inclusiveness, collaboration, and collective aid, and that the executive officers, DCN

Ambassadors, Verified DCN Entrepreneurs, or any representative of the DCN Community will be a resource for contributors to depend on and collaborate with.

1.3 DCN Outreach

Our Roadmap includes exciting, unprecedented outreach programs that will serve to strengthen our collective and facilitate engagement with people of all walks of life. In short, DCN does not have a singular “target market”; how could we, when the practical use cases and implementations of our technology are vast and diverse? We do not intend to confine utilization of DCN to the personal visions of our Core Team members, so alternatively we will launch programs upon inception designed to maximize engagement with DCN and allow community members to adapt our mission and initiatives as DCN evolves. Our initial DAO is 18 reserving resources to fund experimental programs and to reward active contributions to our community. Some of these proposed program ideas are explained below. Once again, DCN is inclusive and agnostic, and our global presence will mirror these core values. We will include interest groups such as entrepreneurs, activists, developers, universities, corporations, and uninformed but curious individuals, all boasting varying track-records of engagement with the cryptocurrency space. Through our DCN Ambassador Program, experienced users, thought leaders, and passionate community members will be granted opportunities to represent DCN, propagating our vision to people in corners of the world without access to the resources, capital, and technology necessary to discover and join our community out of individual initiative. Leaders in this program can serve many purposes, from advising DCN startups to mentoring DCN Chapters to representing .

DCN in the press. By participating in our DCN Youth Program, global minors will be offered intensive coding and business development education, and unique opportunities for engagement with the DCN collective. This initiative will be multifaceted, with offerings ranging from global youth competitions for DAO-funded startups built on the DCN platform to lotteries allocating resources to cover education expenses of DCN Youths. These young pioneers will also be mobilized to recruit their peers and engage their communities. Entrepreneurs managing DAO-funded projects will be DCN Verified Entrepreneurs and gain access to relevant startup-accelerator-style perks, such as access to successful business mentors, marketing and user acquisition channels, open sourced developer engagement, direct channels to investors and venture capital firms, and events, partnerships, and seminars designed to collaboratively resolve issues and foster innovation. Individual contributors will gain access to plug and play content fashioned to assist in spawning grassroots movements in the form of DCN Chapters proselytizing DCN technology, ethics, and/or governance and developing projects around the world. These DCN Chapters will be localizable and customizable, with fluid emphasis depending on region and community needs. DCN will offer a foundational online platform of material resources, ranging from:

Chapter II   Core of the DCN Project

2.1 Core of the DCN Project

Introduction The advent of blockchain technologies has enabled the development of an entirely new class of assets backed by cryptographic verification. Bitcoin (BTC) and Ethereum (ETH) are two blockchain-based cryptocurrencies which, as of eclipse the aggregate market capitalization of all other cryptocurrencies. In November 2017, the volumes for BTC and ETH trades exceeded USD $181B (not including over-thecounter and trades executed on private forums). This statistic, coupled with the announcements of Bitcoin futures markets from CME Group and NASDAQ, signals interest from institutional investors looking to gain exposure to digital cryptographic assets. With institutions and HNWIs looking to deploy vast amounts of wealth into cryptocurrencies, we must develop the underlying infrastructure to support such volumes. At a fundamental level, dark pools are private exchanges where financial assets and instruments are traded and matched by an engine running on a hidden order book. These exchanges are primarily created to serve institutional or HNW retail investors who require a system where significant volumes of assets can be block traded with minimal price slippage. Dark pools are estimated to represent approximately 15% of all trading volume of all US stock trades [6]. Extrapolating this statistic for BTC and ETH volumes, a dark pool for such has the potential to execute USD $27.2B of orders monthly. We introduce the Republic Protocol which facilitates the exchange of Ethereum, ERC20 and Bitcoin cryptocurrencies through a decentralized dark pool. This is enabled through research within subfields of cryptography such as secure multi-party computation, which allow us to develop a matching engine to run on the distributed hidden order book. We facilitate cross-chain trades through atomic swaps and implement proper economic incentives to ensure these trades are executed thoroughly. Compared to a centralized dark pool or exchange, the Republic Protocol removes the risk of asset theft, confiscation or possibility of interference from a malicious exchange operator. This leads to greater trust between institutional investors placing block orders and dark pool exchanges leveraging the Republic protocol. Additionally, the Republic Protocol is available universally and is highly transparent with regards to how the underlying protocol operates.

2.2 How the Republic Protocol works

The primary technical goal of the Republic Protocol is to enable a decentralized network of nodes to match orders, without knowing anything about the orders. While it might seem like this is impossible, it can be achieved by applying cryptographic techniques that have been thoroughly researched over that last 30 years; modifying them to be suitable for the world of decentralized computation. The Republic Protocol uses the Shamir Secret Sharing Scheme [1] to break down orders into a large number of order fragments, and distributes them throughout the network. Orders cannot be reconstructed unless a majority of the order fragments are recombined. To prevent this from happening, the Republic Protocol defines an Ethereum smart contract called the Registrar that organizes nodes into a network topology that makes it unreasonably difficult for an adversary to acquire the enough of the order fragments to reconstruct an order. As long as traders respect the network topology defined by the Registrar, their orders will be safe. If they fail to do so, only their own orders are at risk of exposure. Using order fragments from two different orders, a node can cooperate with other nodes that hold other order fragments for the same two orders to perform a decentralized computation that will determine if the two orders match. The decentralized computation does not expose the order fragments, and performs a random scaling of the final output [2][3]. This prevents nodes from reconstructing the original orders, and prevents them from using the output to infer anything about the orders. A Zero knowledge proof is used to verify the integrity of the computation, without revealing any information. These proofs are simple and efficient, allowing them to be performed by an Ethereum smart contract called the Judge [3]. After two orders have been matched, an atomic swap is initiated between the two traders over the Republic Swarm Network, a decentralized peer-to-peer network. Using standard asymmetric encryption primitives, the details of the atomic swap are kept secure. System Properties The Republic Protocol provides the following properties: 1. The identity of the traders is secure within the Republic Dark Pool. The underlying cryptocurrency that is being traded may provide different limitations for privacy. 2. Traders do not have to remain connected to the network while their orders are being matched. Once an order is placed, nodes will run the matching computation until a match is found, or the order is expired (either manually, or by passing a deadline designated by the trader). 3. An order is secure until it is matched. After being matched, some details of the order are revealed to the matching parties. This is the natural limit of security for an order, since both parties know what they submitted, and both parties need to know when a match has occurred. Note that information disclosed in these cases does not provide any informational advantage to either party. 4. The total liquidity of the Republic Dark Pool cannot be reasonably estimated by any participant.

2.3 Clearing of digital assets

Digital asset liquidation business is the most basic application in the DCN ecology. In the DCN ecology, all users, including financial institutions, upstream and downstream enterprises, brokerages, trusts, funds, etc., the behaviors involving transactions will be asset liquidation through the DCN digital asset liquidation application.DCN users first need to register digital assets for digital assets and digital currencies, and buyers and sellers conduct contractual transactions and automated settlement of assets through smart contracts.

2.4 Exchange of digital assets

DCN ecology can realize the exchange between digital assets, DCN will support the exchange between digital assets and traditional assets, such as stock, warehouse receipt, bills, inventory, factories and other physical assets can be digital assets in DCN ecology, determine the corresponding value, through the use of DCN to settle the corresponding value, into the corresponding digital assets.Meanwhile, these digital assets can be traded in the secondary market.

2.5 Security Model

Defining a security model allows us to analyze the security guarantees provided by the Republic Protocol. The Republic Protocol makes use of the real vs. ideal paradigm; analyzing the security of a real world decentralized protocol with respect to some non-existent ideal world in which there is a trusted, and incorruptible, third-party that can be used to handle all sensitive information and perform all sensitive computations (this is not the same as Ethereum, since all transactions and data on Ethereum is publicly available). The security of the Republic Protocol can be demonstrated by showing that any possible attack in the real world is also possible in the ideal world. Since the ideal world is trivial to define, the real protocol is secure by implication. This approach to security analysis is typical for decentralized computation protocols in which there are active and passive adversaries. The ideal Republic Protocol contains a trusted, and incorruptible, third-party T. Traders submit their orders to T, and T guarantees to never reveal the details of these orders. T constantly attempts to match orders that have been submitted, and when a match is found T informs the respective traders. The traders each submit their cryptocurrencies to T, and if they both do so, T swaps the cryptocurrencies and gives them back to the traders. This completes the trade. The real Republic Protocol is considered secure if, and only if, all attacks on the real protocol are also possible on the ideal protocol. From the definition of the ideal Republic Protocol it is clear that such an equivalence is sufficient. 4 The Republic Protocol is able to guarantee that, unless the majority of nodes in the network are active adversaries, it is as secure as the ideal world protocol. If 50% of nodes are active adversaries, and they are enjoying the attackers best-case scenario, they are able to reconstruct all orders. However, the Republic Protocol ensures that such a best-case scenario is impossible to achieve in the real world. In the typical case, 50% of nodes becoming active adversaries would only allow the adversaries to reconstruct 50% of the orders. A more detailed explanation is given in “Attacks and Defenses”.

2.6 Circulation incentive scenario

DCN will establish a trust system based on blockchain, so that the core upstream and downstream institutions, trusts, funds, brokerages and related practitioners in the financial industry will form a consensus incentive system, so that DCN ecological participants can spontaneously promote the prosperity and vigorous development of the whole ecology.

In the DCN ecosystem, through the incentive mechanism of Token reward for participants’ effective activities, the subjective initiative and motivation of participants are better stimulated, and through the characteristics of blockchain decentralization and data openness and transparency, to solve the value trust problem and form a reliable closed loop of data flow.The DCN ecosystem builds a new financial environment and business relationship, changes the concept of the market and completely reverses the value flow and distribution model of the traditional financial industry.The DCN serves as the only means of payment in the DCN ecology.For the business exchanges of various participants in the ecology, the circulation of DCN is realized in the form of intelligent contracts. DCN is not only a payment tool, but also an incentive means. The high circulation of DCN is a strong guarantee for the high activity in the DCN ecology.

2.7 Decentralized Order

Matching Order matching is the process through which nodes match orders against each other without being able to observe the details of the order. To achieve this, traders first breakup their order into a set of order fragments. Note that these fragments do not individually represent a fraction of the order ’ s value, they simply represent the separation of sensitive data regarding the underlying order. On its own an order fragment reveals nothing about the underlying order, but when at least half of the order fragments for an order are combined, the order can be reconstructed (see “Attacks and Defenses” for details about protecting against this). Each node performs an order matching computation on order fragments from multiple different orders and combines the results with the results from nodes (who are using different fragments).

The fragments are constructed in such a way that, after the computations are applied, the resulting fragments can be combined to reveal, not the underlying orders, but the result of the order matching computations for the underlying orders. This has several nice properties. For one, only half of the order fragments are needed to reconstruct an order. Nodes are incentivized to avoid collusion (and adversaries have a difficult time subverting this system, see “Attacks and Defenses”). This means that if half of the nodes accidentally die, or leave the network halfway through an order matching computation, the network can still finish the computation. This makes it highly resilient to DDoS attacks, and expected failures. Order fragments are constructed in such a way that the order matching computations can use any function, applied over a polynomial, and can be involve two or more underlying orders. This allows for very flexible order matching computations. Nodes can match orders based on exact price points, partially match orders (when only some of an order can be matched due to the currently available liquidity), match triplets (or more) of orders to increase liquidity (e.g. the triplet BTC-to-ETH and ETH-to-REN and REN-to-BTC, where no match can be found with only pairs). Assuming the existence of a decentralized, consensus-based, data stream for National Best Bid and Offer (NBBO) data, the order matching computations can even involve orders without an explicit price point.

Chapter III Attacks and Defenses

3.1 Order Reconstruction

The security of an order maintained as long as n/2 of its n order fragments are not discovered by an adversary. If an adversary does acquire n/2 (or more) order fragments, the original order can be reconstructed. As such, it is important to understand the defenses in place against such an attack. Nodes in the Republic Dark Pool are partitioned into n disjoint sets, where each order share is randomly distributed to at most two nodes in any one set. To model an attack on this topology, we assume that the adversary has full control over which nodes to corrupt (the Republic Protocol enforces that nodes are actually randomly distributed amongst the disjoint sets, meaning that this assumption provides the adversary with more power than they have in reality). The ideal attack scenario would be where an adversary corrupts all of the nodes in n/2 sets, guaranteeing that n/2 order fragments will be acquired for every single order. Assuming an approximately uniform size of each pool, the adversary must control 50% of the network. Note that it is impossible for an adversary to control in which set their nodes will be registered, making this type of attack impossible. Realistically, when controlling 50% of the network, the adversary is most likely to control 50% of the nodes in all of the n disjoint sets. At this level of control, an adversary has a 0.5 probability of successfully acquiring each order fragment but must successfully acquire n/2 order fragments to know the order. We can model this as a binomial distribution. Let X be the number of successfully acquired order fragments, p be the probability of acquiring any one order fragment, and n be the number of attempts that the adversary has for any one order fragment. Because X is binomially distributed with a 0.5 probability of success. It follows that, This formulation relies on n, the number of disjoint sets, which is directly proportional to the number of nodes in the Republic Dark Pool. As the number of nodes in the Republic Dark Pool grows, the probability that an adversary is able to reconstruct a single order approaches 0.5. This implies that an adversary that somehow manages to corrupt 50% of the network only manages to discover 50% of the orders.

3.2 False Orders

When two orders are matched, both of the matching parties learn that there exists some corresponding order in the Republic Dark Pool (otherwise a match would not have occurred). An adversary can take advantage of this in an attempt to gain insight into the liquidity of the Republic Dark Pool. Assume that there are n legitimate orders in the dark pool when there is no adversary. To simplify the analysis we also assume, in the favor of the adversary, that the adversary knows the maximum price point of orders in the dark pool (realistically, this is impossible and the adversary would have to make several guesses). If we assume that none of the legitimate orders have matches, the adversary needs to submit n false orders (at the maximum price point) to discover all orders. Compared to the fees paid by the rest of the network, the adversary needs to match 100% of the financial commitments to order fees made by the network.

By Assumption (II) this is not realistic, and becomes more and more difficult as the Republic dark pool is used. Now we assume that each of the n legitimate orders has exactly one legitimate match, and an attacker has a way of distributing their order fragments in such a way that their false orders are instead matched with a p=50% probability. Again, this assumption is in favor of the adversary, since they cannot actually know how to perform such a distribution. For a binomial distribution with corresponding probability of success , the probability of exactly successes given trials is given as For example, if n=100 and p=0.5, then the probability is approximately 54%. This shows that only with a substantial commitment to order fees compared to the network as a whole, along with many favorable assumptions, is an adversary able to gain insight into the liquidity of the dark pool. This analysis does not take into account that there is a limited number of orders that can be submitted by any one trader. To submit a large quantity of false orders a trader would also need to stake a large amount of financial power into bond registrations. Future versions will also discuss methods by which traders must forfeit their bond if they do not execute on false orders. Taking these three parts of the analysis into account: the high amount of order fees required to gain insight into the dark pool, the high amount of bond required to submit that many orders, and the high amount of bond sacrificed when false orders are not executed, Adversarial Assumption (II) prevents adversaries from being able to expose the liquidity of the dark pool by submitting false orders.

Using this private DCN, the user can sign the transaction into the transaction object and broadcast the object to the network.The public DCN is included in the transaction, and the node receiving the transaction is able to use kp to verify the signature.This provides effective security for users and the network, as ks is only known to the user, and kp can verify that the signature is a valid purpose.

DCN provides an additional layer of security, using specific categories of transactions, users can register a second password associated with the secret DCN, set a certain fee (currently tentatively 5DCN), this relationship requires all subsequent transactions to sign with the second password to be considered valid, set the second password, users can set directly through the wallet.

Multiple Signature:

For users who need higher security, DCN supports multiple signature accounts as another security system.Multiple signed accounts is an account that requires multiple signers to submit a signed transaction.Any user can enable multiple signatures on their account by issuing a special transaction, specifying a set of ksn and the minimum number of signatures required to confirm that the transaction is valid.It is then stipulated in the blockchain that before processing any transactions from the account, any transactions originating from the account must be signed by the minimum legal number of relevant account:

The DCN address or wallet ID is exported from the public DCN, using the SHA-256 hash public DCN, and then reversing the first 8 bytes of the hash.Account ID is the numerical representation of these 8 bytes, starting with the M character.

3.3 The Broadhash Consensus:

The Broadhash consensus plays a crucial role for the DCN network to prevent forks.In the DPoS system, allocate a slot to the agent by the timestamp, and try to fake the block when the system specifies that the proxy slot is ready.The Broadhash consensus ensures that most peers recognize that forgery is acceptable.

Broadcast cohort:

The broadcast queue is the fundamental role of the DCN network.The transaction must be moved from one node to all the other nodes to be included in the block.The broadcast queue takes up to 51 transactions from the trading pool and gathers them

Synizes a package to work.The bundle then broadcasts to the network at intervals specified every 5 seconds.In addition to broadcast objects, the component has a relay limit to prevent overbroadcast data.In the current implementation, the relay limit is set to 2, meaning that each packet is broadcast once from the originating node and twice more from the receiving node.

3.4 Performance extension support

DCN adopts the dual-chain architecture design, and the dual-chain structure is divided into user chain (UBC) and transaction chain (TBC). DCN is optimized in the two chains respectively, which can not only guarantee user privacy, but also save a lot of computing power.The dual-chain architecture is load-balanced, both parallel and serial, with good extension performance, so simply increasing the server can increase blockchain speed.

Concurrent consensus refers to a parallel Byzantine algorithm (PBFT) that ensures that user privacy does not leak.The Byzantine algorithm is divided into three rounds of voting, each based on the two sides of the N, and after three rounds of voting, a consensus can be built.Unlike traditional Byzantine algorithms that consume great computation, DCN's algorithm will parallel transactions with voting without simplifying any round of voting, so even if the complexity of the voting process increases, the overall transaction and voting process do not need to wait for each other, increasing the transaction speed.

3.5 System safety

The DCN system was developed based on JavaScript, with an architecturally built-in blockchain firewall, interface from Mcafee., the world's top security companyAll applications and software after DCN will review the results of Mcafee to maximize security.

Less chances of being attacked successfully.

DCN will officially deploy more than 200 node servers worldwide that will use the mcafee solution for security hardware settings (firewall, router, server, device). Our proven network firewall with the most efficient next-generation Intrusion Defense System (IPS) and Advanced Malware Protection (AMP) will not only exclude most hackers, but also effectively improve the security of the entire ecological environment.

Distributed data storage

DCN provides safely encrypted distributed data storage capabilities, DCN builds a distributed hash table (DHT) of data blocks, the user finds the list of block nodes in which the data is based to the DHT, and then retrieve and validates the data.When other users access the file, they need to be authorized to get the DCN to view the data.

When the user stores the data to DCN, DCN slices the data and causes the user DCN to encrypt the data and then chunks on the P2P network, so DCN stores encrypted distributed data blocks to protect user privacy and data security.

Security multi-party calculation

Secure Multiparty Computing (SMC) is a collaborative computing problem of privacy protection among a set of mutual distrust participants. SMC should ensure the independence of input, calculation correctness, decentralization, while not disclose each input value to other members involved in the calculation.It is mainly for the problem of how to safely calculate a convention function without a credible third party, while requiring that each participant cannot get any input information from any other entity other than the calculation results.

The digital signature, tamper-proof, traceability and decentralization of blockchain, and the input privacy, computing correctness and decentralization of security multi-party computing.Blockchain technology and the combination of security multi-party computing, multiple security computing as a part of blockchain data encryption and verification mechanism, and blockchain technology as a component of cloud computing, AI and other infrastructure platform, combined with zero knowledge proof and other cryptography technology, constitute the next generation of general computing service platform, with decentralization, data protection, joint computing, to form a new support for the upper business.

3.6 Sybil Attacks

In the Republic Protocol, defending against order reconstruction attacks (and false order attacks) requires associating an identity with a node (or trader). This opens the possibility for an adversary to forge multiple identities, known as a Sybil attack, in an attempt to subvert the network. p k n n! k!(n − k)! pk (1 − p) n−k 10 To protect against this, all nodes and traders are required to commit a bond in order to register an identity. Under the Adversarial Assumption (2), adversaries have limited financial power, we can be sure that an adversary cannot forge a large number of identities. For malicious nodes, the bond needs to discourage the registration of a large number of nodes and the acquisition of a sufficiently large number of order shares during the distribution of order shares (see “Order Reconstruction”). For this method to be effective, the bond must be high enough that an adversary cannot register a large number of nodes, but small enough that honest nodes are still able to participate. The bond amount should be globally consistent (all nodes must meet the same threshold) but dynamic, to account for fluctuations in the value of the bonded currency. For malicious traders, the bond can be used to further discourage the submission of a large number of false orders (see “False Orders”). This is done by requiring that a trader submit orders that point to their registered bond. There is a linear relationship between the bond amount, and the maximum number of orders. Therefore, a trader that submits a bond of B and is allowed M open orders could instead submit a bond of B/2 and be allowed M/2 open orders. The registration of bonds will be handled by the Ethereum network, and are incorruptible by Assumption (1).

Chapter IV DAO: Infrastructure, Proposals, and Voting

4.1. system of governance

The DCN system will have at least one DAO funded by a portion of the mining rewards, and governed by a voting system that brings stakeholders together.

This system of governance helps ensure that implementation of changes, improvements, and integrations minimizes contention and reduces the chance that a disagreement leads to a fork in the project. As we unroll our broader governance plan derived from rigorous R&D and testing, the goal is to open the governance landscape to full competition; this means that we could see multiple competing DAOs emerge with different teams working on different problems. Each DAO would emerge with its own proposed structure, processes, and goals, which ensures these attributes are evolving through competition and the wrong initial organizational decisions do not perpetuate. Our DAOs will be responsible for building, maintaining, and improving the infrastructure that keeps the system going. It is also responsible for implementing changes to the DCN software applications, and is flexible enough to accommodate other community priorities,such as community outreach, marketing, training, etc. 14 As the DCN system grows in popularity, the support structures for users, miners, Secure Node operators, and ecosystem partners will need to grow and scale as well. The DAO structures will have funds, allocated through projects and proposals, with which to assist in the growth and support. The community is encouraged to participate in contributing to DCN in all different ways. The DAOs are responsible for coordinating the community contributions, and have funds to assist in offsetting expenses incurred by the community. One of the purposes of proposals is to repay community members for their expenses in supporting the system. At launch, DCN will have one DAO staffed with respected professionals that span relevant industries. When the governance plan is ready for implementation, this DAO will be one proposed grouping subject to market competition for others who might wish to stand up their own governance structures; the broad community will make that decision. 7.1 DCN Infrastructure Operated by DAO The DAO system will maintain application servers and services, including:

- Secure Node validation server(s).
- Forum server(s). • Slack moderation.
- Binary repositories.

The DAOs are responsible for the following support: • Help people use DCNCash or other system features.

• Troubleshoot voting system problems.

• Provide support escalation.

• Provide rapid and final issue adjudication.

DAO distributes DCNCash to proposal owners after a successful vote and expiration of the veto period. There will initially be 3-5 DAO officers, but this will ultimately be unbounded. Officers can be anonymous, but that is not a requirement. In fact, openly declaring identity comes with the advantage that prior professional achiev There will be disputes and so resolution mechanisms need to be developed to adjudicate these efficiently and fairly. One idea that will be explored in the Governance R&D project will be to establish a judiciary and jury system. 7.2 Proposal Submission and Voting Each DAO will have its own structure, processes, and priorities, but one consistent mechanism will be a system of free and open proposal submissions for work and an evaluation and award process. There is no reason to specify how this happens, only that it should happen. This is an open community to all of humanity, so there should be no barriers to participation. One proposed method for our initial DAO is as follows: 1. Vote every two months. Proposal submission deadline two weeks before voting. Voting dates: Jan 31, Mar 31, May 31, July31, Sept 31, Nov 31. 2. Proposal submission opens day after vote. 3. Veto - core team may veto a proposal within 7 days of a vote with a unanimous core team veto (this should almost never be done). 4. Proposals can be funded in the DCNCash equivalent of the local fiat currency on the date of the vote (prevent Dash issue of rapid rise leading to project rejection). 5. Voting done with tokens. 1440 voting tokens distributed 1 month before vote. 6. Most decisions done by majority vote > 720 token holders voting yes. 7. Some decisions by supermajority vote > 1080 token holders voting yes. 7.3 Voting Process Token Distribution Plan - done for every voting period, 1440 tokens altogether: 1. 360 tokens for sale - allows users and DCNCash holders to buy votes.

1-30: 1 DCNCash

(b) 31-60: 2 DCNCash

(c) 61-90: 3 DCNCash

etc. up to 12 DCNCash per token for last group of 30 2. 240 - DCNCash project developers.

• Awarded by commits, pull requests, or other reasonable measure of contribution. • Goal is to empower software and system developers.

The Core Team initially consists of the three early founders for the project, Joshua Yabut, Rob Viglione, and Rolf Versluis. Each founder is a leader within his respective professional domain and has a strong track record of performance and cryptocurrency expertise. Josh is an experienced red teamer and exploit developer who previously served the aerospace industry. He has a passion for developing adversary-resistant networks and for redefining the status quo. He holds an Offensive Security Certified Expert (OSCE) certification, a Masters degree from DePaul University in IT Project Management, and has extensive knowledge in exploiting government and corporate networks. Josh has extensive cryptocurrency development experience leading the core team for Zclassic, developing the z-nomp mining pool protocol, supporting the ZCash development community, and consistently delivering quality software.

Rob is a former physicist, mercenary mathematician, and military officer with experience in satellite radar, space launch vehicles, and combat support intelligence. Contributions within the crypto space include being part of Zclassic’s core team, support to the Bitshares project, heading up BlockPay’s U.S. & Canada Ambassador program,and consulting for Bitgate. He’s currently a PhD Candidate in finance @UofSC researching cryptofinance and teaching “Bitcoin & Blockchain Applications in Finance.” Rob holds an MBA in Finance & Marketing and the PMP certification. He is a passionate libertarian who advocates peace, freedom, and respect for individual life. Rolf is an experienced business owner in the IT industry and owns a mid-size Bitcoin and Zclassic (DCNCash) mining operation in Alpharetta, Georgia. With prior experience at Cisco systems, the semiconductor industry, and as a nuclear trained officer in the US Submarine force, Rolf brings leadership, management, and technical operational expertise to the DCNCash organization. The motivation for forming a Core Team entity with decision-making authority and an independent budget was to rapidly deploy the system and efficiently execute a wide range of early development tasks that will culminate in a fully operational network outlined in our Roadmap; the ultimate result will be a transition to the broader governance structure resulting from R&D and testing. Our goal is to work ourselves out of our jobs after delivering on the initial Roadmap and standing up our first elected DAO per the governance plan. At that point we’ ll run for office within the existing DAO, or consider launching our own to add to the competitive dynamics of the system.