Technical Whitepaper

kNET - A user-centered peer-to-peer economic and monetary network

10th August 2019

"Wealth should serve humanity, and not the other way around."**– Dalai Lama**

Version: 0.2b Public Release
Author: A. Kerdemelidis, Kuva Coin Trust
https://kuva.com/whitepaper

DISCLAIMER: This Technical White Paper is for information purposes only, provided on an "as is basis". Kuva Coin Trust does not guarantee the accuracy or the conclusions reached in this white paper, it is provided solely for informational purposes. Kuva Coin Trust does not make and expressly disclaims all representations and warranties, express, implied, statutory or otherwise, whatsoever, including, but not limited to: (i) warranties of merchantability, fitness for a particular purpose, suitability, usage, title or noninfringement; (ii) that the contents of this white paper are free from error; and (iii) that such contents will not infringe third-party rights, including, but not limited to, intellectual property rights, trademarks, licenses. Kuva Coin Trust and its affiliates shall have no liability for damages of any kind arising out of the use, reference to, or reliance on this white paper or any of the content contained herein, even if advised of the possibility of such damages. In no event will Kuva Coin Trust or any of its affiliates be liable to any person or entity for any losses, damages, liabilities, costs, expenses of any kind, whether direct or indirect, incidental, consequential, compensatory, exemplary, actual, punitive or special for any use of, reference to, or reliance on this white paper or any of the content contained herein, including, without limitation, any loss of business, revenues, profits, data, use, goodwill or other losses, including intangible losses. ©Kuva Coin Trust 2019, All Rights Reserved.

Executive Summary

The Kuva Network (kNET) is a blockchain ledger and protocol which incorporates satisfaction and performance measures from verified transactions by end-users to determine its strategic governance.

There are three key participants in the Kuva Network: Strategic Governance, Licensed Service Providers and Infrastructure Providers. Licensed Service Providers provisioning off-network ad-hoc services for end-users of kNET, such as fiat cash-outs, bank payments, payment cards, cryptocurrency asset exchange and the like, are collateralized and participate in determining the strategic governance of the network.

By incorporating collateralized and bonded 'masternodes' along with Proof-of-Work confirmation and transaction finality by collateralized miners, kNET supports counterparty-protected exchanges and swaps of assets across completely independent cryptocurrency networks.

The native currency of kNET, in which all network-related fees are paid, is known as the KUVA 'Util'. This is a mineable cryptocurrency, for which the total unspent circulating/generated amount never exceeds 1.2 Billion (1,200,000,000) KUVA.

This paper describes the key features of kNET as well as our approach to safely launch, by building up a network called the 'Apex' to a critical number of collateralized nodes, prior to enabling full public operation of its infrastructure.

Table of Contents

Executive Summary 3

Table of Contents 4

Table of Figures 7

Kuva 8

kNET 8

Corollary 9

An End to the Means 9

The Means to an End 12

Problem Statements 12

Siloed Cryptocurrency Networks 12

Threefold Aim for the Kuva Network 13

kNET Distributed Autonomous Entity - DAE 13

kNET's Mineable KUVA Util Cryptocurrency 15

kNET Multicoin Transactions 15

kToken – a Standard On-Chain Customizable Token 16

kNET Block Structure and Storage 17

kNET Incentive Model 18

Real-Time Network Layers 19

Collateralization of Service Providers 20

Strategy and Governance 20

Strategic Governance Proposals 21

Governance Blocks and Voting 22

Governance Keys 23

Trias Politica Network Structure 23

Governance Initiation and Transition 25

Strategic Governance Allocation of Treasury Funding and Incentives 25

kNET Licensed Service Provider 26
kREP Persistent Reputations 27
kREP and the Adaptive Governance Model (AGM) 28
kNET Masternodes 30
kNET Hierarchical Masternode Quorums 31
Service and Network Fees 31
Licensed Service Provider Class Deterministic Lists and Rewards 32
Collateralization and Voting 33
KUVA Util Collateralized Mining Sessions (CMS) 34
Generation of KUVA Utils 34
BlockLock - Blockchain Deep Reorganization/51% Attack Resistance 35
Block Time and Difficulty Determination 37
Block Contention 38
Block Reward 38
kNET Apex Masterminers 39
kToken On-chain Atomic Swap Transactions 39
Chainbond Protected Swaps (CPS) for cross-chain exchange 40
Multiple-Cryptocurrency Network Support 40
CPS Superquorum and Subquorum 40
CPS Quorum Sessions 42
Quorum Observations and Determinations 43
Superquorum Counterparty Compensation 44
Subquorum Escrow Processing 44
Consolidated Cross-Chain Trading 44
Postfunded Chainbond Protected Swap Example 45
Swap Request Transaction 46
Swap Pairing Transaction 46
Subquorum Session Vault construction 46

CPS Business Rule Monitoring 47
Native Multisignature Chainbond Protected Swap 48
Notes on Standardness Rules on External Networks/Blockchains 48
Preimage Attacks and Collision Resistance for Native Multisignature Generation 48
Mempool Size and Transaction Delays 49
CPS Business Rules 49
Notes on Prefunded CPS Transactions 49
Post/Pre-funded CPS Transactions 50
The Block Budget 50
kNET Script Modules 50
KUVA Util Supply 51
Launch and Initialization for Public Launch of kNET 52
kSeries – a Founding Stablecoin Series for kNET 53
Foundational Funding 54
Premine 54
Presale 54
Public Collateralization of the Apex Network 55
User-friendly Masternode Activation 55
Notes on Sharding and Pruning 56
Summary and Conclusion 57

Table of Figures

Figure 1 Kuva Network (kNET) overview 14
Figure 2 kNET address examples for all token types. 17
Figure 3 kNET block format overview 18
Figure 4 Strategic Governance Proposal voting 21
Figure 5 Strategic Governance Proposal Template summary 22
Figure 6 kNET Strategic Governance determination by end-user ratings and transaction volumes 25
Figure 14 End User selection and transaction overview with a Licensed Service Provider – the example is of an Atomic service 27
Figure 7 End User transaction and rating of Licensed Service Provider using kREP 29
Figure 8 Collateralized Licensed Service Provider Class deterministic lists 33
Figure 9 Running BlockLock calculation providing deep blockchain reorganization and mining majority (51% attack) resilience 36
Figure 10 Collateralized Mining Session with Masternode Mining Quorum and Masterminers, operating within a Mining Window and incorporating BlockLocks. 38
Figure 11 Hierarchical Masternode Quorums - Superquorum and Subquorum summary 41
Figure 12 Chainbond Protected Swap overview - Bond Vault, Quorum Vault and Observations 43
Figure 13 Chainbond Protected Swap example 45
Figure 15 Kuva Generation Curve and Burnmine Cycle descriptions 52
Figure 16 Post Pre-Sale KUVA Util distribution and minable allocation at Apex network inception 55

Kuva

"A new economic system.

A network that optimizes its governance for user satisfaction,

Creating the world's largest bank in your hands.

Pay, get paid and trade in an instant, anywhere on the planet.

Simply by using the phone in your pocket.

No middle men, just people like you and me."

kNET

The Kuva Network levels the playing field

When you transact using kNET, you get control.

Your satisfaction is built into the center of its design and protocol.

Even 10 cents is a superpower when united with the spending power of others.

Years ago, banks were powered by giant mainframe computers.

What most banks do today operates within these outdated technological limits.

Banks haven't changed for a long time, even though the world they operate in has.

The mobile phone in your hands is a supercomputer, with far more power than they had.

All the software for an entire bank can be wrapped into a phone app and put in your pocket.

Every person on Earth gets their own bank, for free.

Game changed.

Corollary

An End to the Means

Bitcoin and other decentralized trustless systems have demonstrated that it is possible to enforce a strict protocol in a distributed, participatory way and that this enforcement far exceeds the security of centralized systems. No one person or organization can manipulate trustless protocols maintained by a suitably distributed network; these can only change with the majority agreement of those who provide the resources to sustain it. But the question remains: what say do the end-users have in the governance and protocol evolution of these systems? It is end-users and businesses that form the true economic majority[1], not just infrastructure and service providers, as it is their use of the network that ultimately gives it its value.

There was hope that distributed cryptocurrency networks of various models like Bitcoin, Bitcoin Cash, Ethereum, Dash, Litecoin, Tezos, EOS and others could lead to economic and financial innovation that improves the world we live in, by making it more efficient to trade and do business, and by enabling economic access for more people. But there is a problem currently with these networks. Statically decentralized, consensus-driven, trustless networks are a Gordian knot; the same security that enforces their protocol and keeps users safe is also their weakness. All these protocols are designed to rapidly harden and become unchangeable, such that any changes that might make the cryptocurrency more useful to users become increasingly restricted by the network operators as user adoption increases. This in turn stifles innovation and the ongoing development of the network protocol that is critical in order to enable broader adoption and improved user experience and satisfaction.

In order to support emergent user needs, especially in a greenfield sector such as cryptocurrency, an economic network must be able to evolve and improve on its early concepts and protocols. Emergent products or services should become more efficient and scalable over time; their features must adjust and adapt to be in line with user needs, expectations and usage. The complete opposite has been recently demonstrated by the near-complete stratification of Bitcoin. Bitcoin was launched with a vision for a universal "peer-to-peer electronic cash system", but has now settled permanently to be a form of 'digital gold' rather than 'digital cash', and is effectively unusable for making day-to-day small-value purchases. This is the result of mismatched incentives and the power of influence between users and the agents that operate the network (that is, between the miners, the network nodes and the users who use Bitcoin). Bitcoin has become predominantly useful for longer-term value storage, higher-value payments and as the primary intermediate settlement layer for most cryptocurrency trading, the bulk

[1] https://en.bitcoin.it/wiki/Economic_majority

volume of transactions being executed off-chain through trusted exchanges before on-chain settlement. The reason for this outcome is that it became practically impossible to reach an agreement between these agents providing Bitcoin's network services, in particular the very miners who process transactions, and the strategic groups which were actively developing Bitcoin's software in an attempt to scale the network. The original designer(s) of Bitcoin apparently did not anticipate that a system, which by its own design becomes statically distributed and decentralized very rapidly from inception, also inhibits its protocol from evolving in line with user needs for this very reason.

One of the outcomes of this hardening is that the blocksize of Bitcoin, a part of the protocol where transactions are processed and stored, remains stuck at a size of just 1MB, smaller than a typical photograph taken on a modern smartphone. This seems absurd when we consider the fact that Bitcoin's specialised computing power (hashrate) is in measured in 'exahashes', and has reached over 70 Exahashes/sec (70,000,000,000,000,000,000 SHA-256 hashes per second) which exceeds the current hashing capability of every single supercomputer on Earth put together, by multiple orders of magnitude. Bitcoin's incentives are arranged such that the computing power securing the network has developed to an excessive and computationally wasteful level.

It appears that obtaining the necessary consensus to change the bitcoin protocol much further will only become more difficult over time, let alone providing for the ongoing changes needed to address emergent user needs and scalability requirements. The Bitcoin protocol and network is thus as a glue that has set too quickly before its model can take further shaping. As an example, the Bitcoin Segwit proposal, which was politically and economically opposed by the majority of miners[2], managed to achieve consensus through the economic majority via a User Activated Soft Fork[3] (UASF) and the network now supports it fully. But this method was not able to be used for the Segwit2x hard fork, a highly contentious change (between miners, full nodes and the informal strategic heads of Bitcoin – not the users who would transact with it). The implication of this is that although it would have been beneficial to end-users to have a larger blocksize, resulting lower transaction fees and faster confirmation times, the space inside a Bitcoin block as a scarce resource has become valuable. There is therefore a market for it; blocks are mostly full, a growing and large backlog of transactions remain in the mempool[4], and miners demand a premium in fees from those who wish to include their transaction to be processed in a block - where only certain type of user is willing to pay this premium. It appears that solutions to scaling and cost issues will now always be a non-optimal bolt-on to the core network. As an example, take Bitcoin's Lightning Network, which, as a solution for scaling transactions, is

[2] https://en.bitcoin.it/wiki/Segregated_Witness

[3] https://en.bitcoin.it/wiki/Softfork

[4] http://core.jochen-hoenicke.de/queue/#0,24h

inelegant[5] and compromised. Its constraints and compromises as a reliable 'off-chain' solution for scaling Bitcoin far from satisfy the convenience factor that mainstream users demand.

The result is that Bitcoin is no longer the peer-to-peer digital cash network that Satoshi Nakamoto envisaged a decade ago in his seminal whitepaper. No longer can it be practically used to buy a cup of coffee. The cost of a transaction is uncertain and at times exceeds the cost of the coffee itself.

A cryptocurrency network should seek to achieve the maximum satisfaction of the users it serves, since they are its true 'economic majority'. In Bitcoin, end-users have no influence at all in the development and growth of the network and its protocol. The only way to influence it is to stop using Bitcoin for certain use cases where it is currently inefficient, and this further narrows the applications it could be used for.

For long-term viability, a self-governing economic or cryptocurrency network must be designed to meet the changing needs of the users who give it its value. Such a network must be able to securely improve and adapt its underlying platform protocol to balance the needs of all economic stakeholders, including those provisioning the network, but also its end-users, businesses and any organizations using it, in order to maintain its competitiveness as a solution against readily available alternatives in the market.

This paper defines Kuva's approach for building an economic network that addresses these central issues, leveraging the original techniques of peer-to-peer digital cash to create a user-centered, dynamically decentralized peer-to-peer economic and monetary network, whose strategic governance is derived through the goal of objectively maximizing end user satisfaction.

[5] https://diar.co/volume-2-issue-25/

The Means to an End

Problem Statements

The conceptual basis and infrastructure for many topologies of public-infrastructure, blockchain-based cryptocurrency networks already exist and many are currently developed to at least the proof-of-concept stage. Bitcoin has established itself as the most robust demonstration of peer-to-peer coin distribution and trustless transaction processing. Other networks like Dash are built on the Bitcoin codebase and blockchain technology and introduce the concept of masternodes to provide trustless real-time processing and the operation of a DAO with treasury funding. Ethereum demonstrates a form of dynamic fee charges for on-chain trustless computation, smart contracts and value transaction services. However, it appears that the more distributed they are, the more these networks suffer from the 'static decentralization' problem described in the corollary and do not have the effective adaptability required to respond to emerging requirements from end-users. This stasis is driven largely by the control exerted by an oligarchy of stakeholders who operate these networks' infrastructure. The result is that the end-users of the network who ultimately give the network its value by actually using it to transact have no meaningfully enforceable say in its evolution.

Siloed Cryptocurrency Networks

In order to develop a scalable, autonomous economic network, it is necessary to facilitate the secure exchange of assets between isolated networks. The reliable clearing or escrow of such transactions is a difficult problem, which would normally be facilitated by trusted exchanges that must take secure ownership of user funds in order for any form of asset swap and thus control the private keys for those funds. A distributed exchange, or 'DEX', typically can only run across a single blockchain (Ethereum is the primary example) where smart contracts can be built that allow for trustless swaps between custom tokens (i.e., between two custom tokens adhering to ERC20 standards). Trusted exchanges, in which one or more third-party individuals are in control of private keys and must be trusted completely, are the predominant facilitators of cryptocurrency exchange between independent blockchains. Should the private keys of the exchange wallets become compromised, funds can be stolen from the exchange and users may have no recourse to any compensation whatsoever. This has been the result dozens of times over the last decade; users have suffered losses equivalent to hundreds of millions of dollars. To our knowledge, a trustless, secure and automated solution for cryptocurrency exchange/swaps with clearing, that provides adequate protection for trading counterparties, has not yet been developed in the market.

Threefold Aim for the Kuva Network

The Kuva network features three unique aspects described below;

1. Develop a publicly operated monetary and economic infrastructure called the Kuva Network ("kNET"). Individual service providers and organizations may connect to kNET in order to provision services to end-users.
2. Incorporate end-user-satisfaction based optimization and strategic governance into the network protocol.
3. Facilitate trustless and bond-protected cross-currency exchange and clearing across isolated cryptocurrency networks.

In the first aspect, a multi-coin cryptocurrency network has been developed. Kuvacash, a non-custodial financial services platform that has developed a digital wallet and global payments infrastructure along with a number of partnerships, is currently live on kNET. When the network has evolved to a size that ensures its security, availability and performance, it will be open sourced for public operation.

In the second aspect, we propose the introduction of verifiable transaction-derived user feedback to intrinsically balance the influence of centralized and decentralized aspects of the network. This will enable kNET to emerge as a 'dynamically decentralized' autonomous entity that includes all stakeholders in its governance operations. Licensed Service Providers obtain ratings from end-users who transact with them and Proof of Service measurements are derived from network operator infrastructure correspondingly. These scores determine the democratic selection of a Strategic Governance as well as the corresponding distribution of incentives and rewards across the network.

The third aspect introduces the concept of Chainbond Protected Swaps, which allow the network to facilitate completely trustless and automated cross-chain/cross-cryptocurrency exchange and clearing.

Furthermore, kNET aims to solve the problem of innovation lock-up and protocol stasis by prioritizing the objective satisfaction of its end-users for optimizing strategic governance and incentive distribution.

kNET Distributed Autonomous Entity - DAE

Kuva Network, or "kNET", is a mineable, multi-coin blockchain with a two-tier network structure and a non-infrastructure service provider layer. The network tiers include collateralized miners (Masterminers) and a hierarchical real-time masternode network (collateralized Superlan and Masterlan masternodes). The collateralized non-infrastructure service provider layer provides ratable third-party services to end-users. A mined cryptocurrency token called a Kuva Util, or "KUVA" forms the monetary and governance basis of the network.

kNET, as the operating distributed network infrastructure, is designed to emerge as a form of self-governance known as a Distributed Autonomous Entity or DAE. Following a launch period, where the network must be developed to a critical size before allowing a non-trusted entity to operate any node infrastructure, a balanced operating structure between three aspects will emerge;

(1) A Strategic Governance aspect, which can be changed through a democratic weighted voting process of collateralized network participants and users who make verifiable transactions on the network,

and;

(2) A peer-to-peer distributed network of collateralized network participants, which includes a plurality of miners and masternodes, who respectively secure the transactions over the network, securing its governance protocols and verifiably proving their service to the network.

and;

(3) Collateralized 'Licensed Service Providers', (or LSP's) who provision external services to end-users, and for which they are rated by those end-users. Services may include cash out, bank payments, payment card activation and use, asset custodian services, and many others.

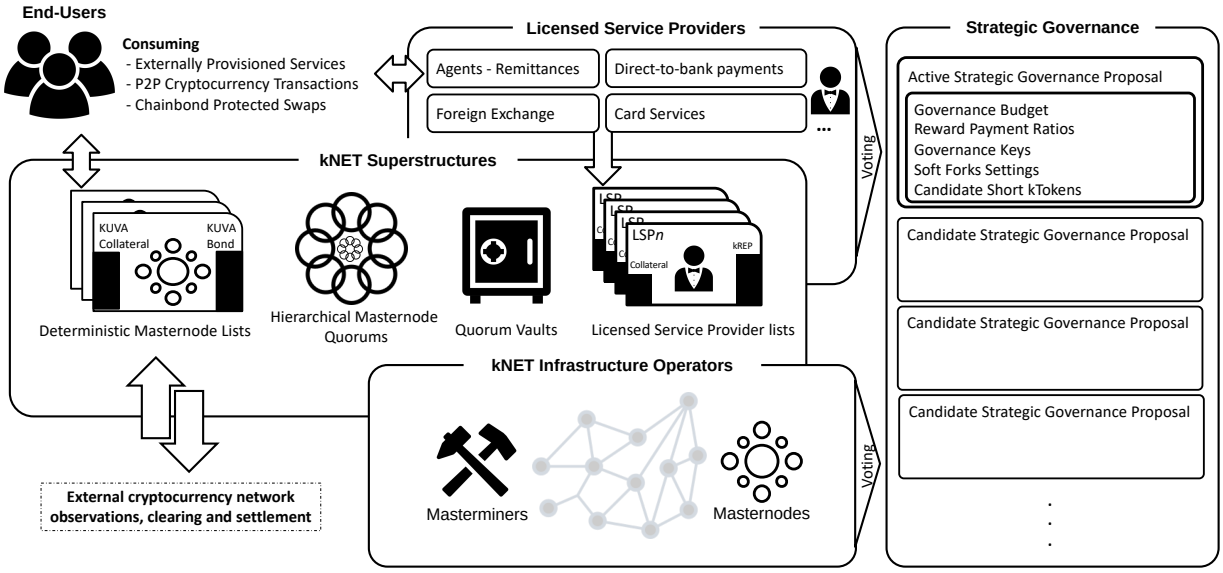

Figure 1 Kuva Network (kNET) overview

In addition to the network infrastructure operators, which are the Masterminers and Masternodes in the network, network-wide 'kNET Superstructures' are automatically formed from these components. These allow for the implementation of higher-level trustless business logic within the network, such as the formation of Hierarchical Masternode Quorums and trustless vaults (Quorum Vaults) for Chainbond Protected Swaps[1] as well as Licensed Service Provider Lists for fairly distributing end-user customer requests and making block reward distributions to collateralized LSPs.

kNET's Mineable KUVA Util Cryptocurrency

Util *n* (plural **utils**)

1. (economics) A hypothetical unit measuring **satisfaction**.
2. (informal, computing) A **utility**.

All on-network participants, including Masterminers, Masternodes and Licensed Service Providers post collateral using the Kuva Network's KUVA token (or cryptocurrency), called a Kuva Util. The Kuva Util, or "KUVA" is the exclusive native minable asset of kNET, used for all economic activities related to incentivizing and governing the network, for example, rewards and fee payments, service collateralization, Chainbonding and voting.

The maximum total supply target is the number of unspent KUVA Utils on kNET at any one time, is set to 1.2 Billion Kuva and is reached through a "Burnmine Cycle" via collateralized mining and distribution to network participants. By providing collateral of the required amount of KUVA for a particular service class, an external service provider becomes a 'Licensed Service Provider' (LSP) and can discover customers and offer services over the network. In addition to fees earned by providing commercial services to the customer using any available currency on the network, LSP's are additionally rewarded with KUVA Utils for provisioning service to end-users. The service provider accrues a verifiable reputation for the transaction with the customer. Accrued reputation from verifiable transactions determines both voting power and subsequent network reward payments.

kNET Multicoin Transactions

kNET supports the ability to transact between multiple custom tokens on its network instantly. It also allows for securing transactions and settlements between completely independent blockchains through a process called the Chainbond Protected Swap[40].

kToken – a Standard On-Chain Customizable Token

kTokens are lightweight, customizable cryptocurrency tokens that may be generated by users and reside on-chain on kNET. They are designed to be used as a simple proxy token on the kNET blockchain representing any asset as its own unique cryptocurrency coin. A permanent transaction ledger in relation to that custom token on kNET's blockchain is maintained and it is possible to transact kToken assets instantly, securely and trustlessly on kNET using the same script opcodes/modules available to all other tokens. By including the ability for custom tokens to be used on the network as proxies for real-world assets, currencies, commodities and the like and providing for atomic transaction and exchange services on kNET between these assets, their economic value is held and traded across the network. It is also possible to allow for useful forms of transactions between multiple assets such as atomic net settlements as well as atomic asset exchanges, development of reserve-backed composite asset indexes and so forth.

There are two forms of kToken – 'Short' which must be introduced to the network through a Strategic Governance Proposal process, and 'Long', which can be issued by any user by paying the required generation fees (in KUVA). Short Tokens are used for representing universally recognized types of commodities and assets which will, necessarily, be managed by external parties (for example, fiat stablecoin series, metals, units of energy). Long Tokens can be generated by any user for any other reason, they are custom tokens with configurable issuance, that can be instantly transacted across the network in a trustless way.

It is possible for any user to generate new types of Long kTokens onto the network through a 'Long kToken Generation Transaction'. The basic parameters to generate a new kToken account include providing its ID, a GUID which is unique on the network for the new token, a 16-byte human-readable tag prepended on a public wallet addresses and a plurality of public keys relating to the issuance. Other parameters required to set up the Long kToken, such as the maximum token transaction amount for any one instant transaction, along with the minimum size of the masternode quorum[6] required to secure it are also provided. Token supply management is also defined in the kToken Generation Transaction - whether there is a fixed supply of the custom tokens and all tokens are generated at once, or whether it is possible for the issuer to generate more of their custom kToken at will.

Transactions addresses and the associated script follows a Bitcoin-like P2SH schema with a UTF-8 coin designator tag appended to the address defining the asset type:

[6] Bonded Subquorum and Superquorum masternode topologies are discussed later in this document.

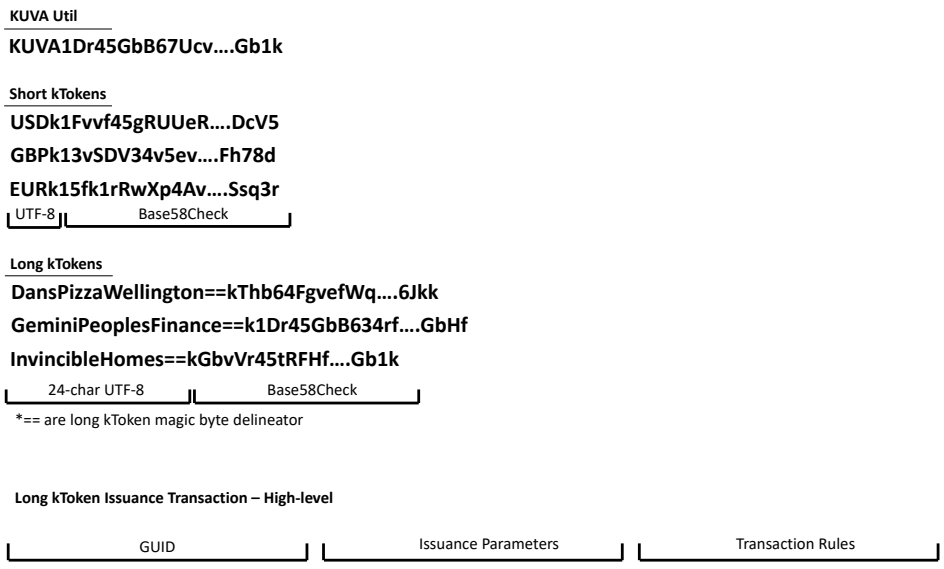

Figure 2 kNET address examples for all token types.

kNET Block Structure and Storage

Blocks within kNET follow a Bitcoin-like schema, with a variable maximum size. At the start of the Apex network, the block size is set to 2MB. A trigger to increase blocksize by up to 20% of the previous blocksize is implemented through the Strategic Governance Proposal process (triggered in the Governance Block) and serves to allow for growth of transactions on the network. This minimizes fee increases due solely to blocksize constraints. The post-Apex network will use a Canonical Transaction Ordering Rule (CTOR) rather than a Topological Transaction Ordering Rule (TTOR), as this allows for more efficient block propagation when using the Graphene protocol[7].

[7] Canonically ordered transactions don't require ordering information to be appended when using a Bloom filter to propagate the next solved authoritative block using mempool transaction entries. This optimization reduces inter-node messaging and bulk block propagation network data.

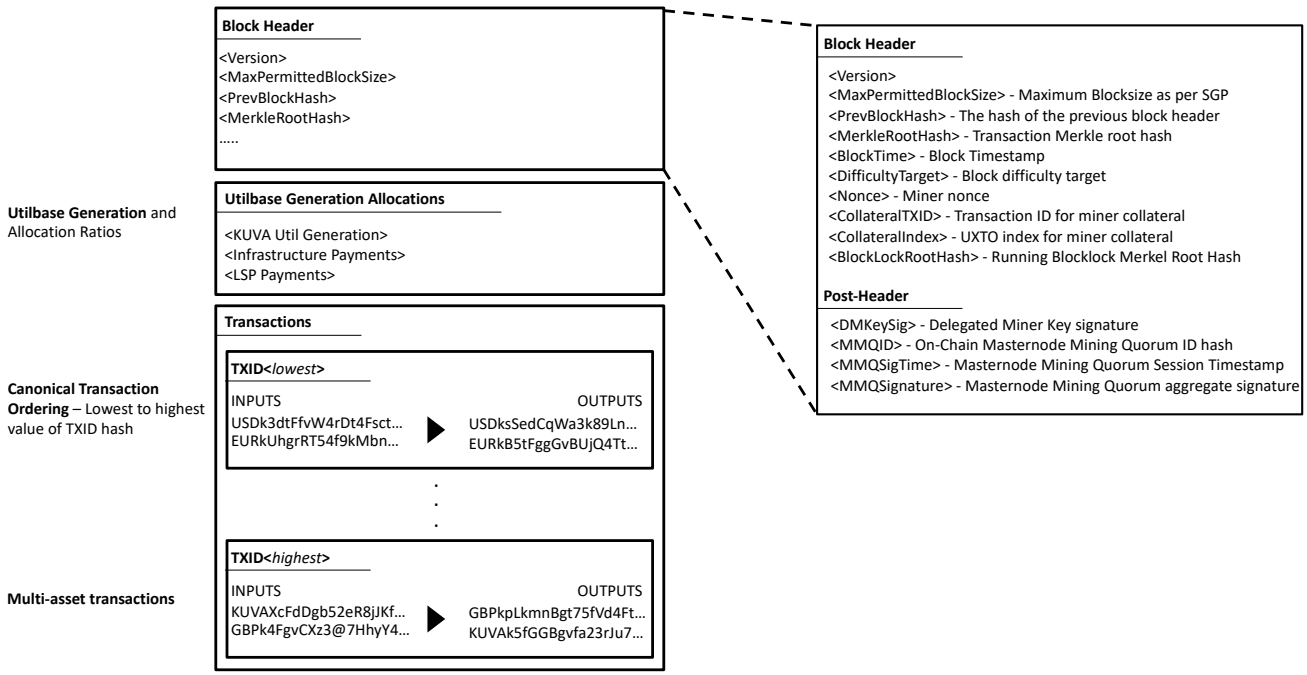

Figure 3 kNET block format overview

kNET Incentive Model

A key feature of kNET is to facilitate incentive alignment between kNET service providers (on and off-network), governance and users over time. This will allow for evolution of the network protocol as its usage grows.

kNET provides for a dynamic incentive model, in which service providers that provision services to the network – whether those services are delivered as network resources (Masternodes) or as externally provisioned services – receive payment in KUVA in return. This is alongside any other payments they may receive for that service - for example, cash-out commission paid in stablecoins. Network Payments to Masternode owners are calculated in line with a proof of service (PoSe) score, ensuring they hold the required collateral and bond and also that they provision adequate network/CPU performance. Collateral holders that are provisioning services on the network and processing high numbers of transactions for which they are rated highly receive a correspondingly higher payment and voting power than those with no/lower reputation.

Real-Time Network Layers

To ensure network operators act in common best interest, core network infrastructure must be collateralized with a corresponding amount of KUVA Utils. Once collateralized, they can participate in mining functions, or can act as one of the two types of masternodes on kNET's topology that form the core network infrastructure;

1. Masterminers: A collateralized blockchain and mining/minting layer responsible for processing the transactions of multiple assets through the mining of blocks, minting of kTokens, as well as regenerating the network utility token of kNET (KUVA).
2. Masternodes: Masterlan (bonded/authoritative and used for enabling and securing all transactions) and Superlan (unbonded/supervisory/audit and used for securing native KUVA Util token transactions) masternodes form a real-time collateralized network layer that is able to form a plurality of hierarchical "quorums", used for authoritative arbitration of mining resources and block generation, enabling instant transaction capability, for Proof of Service (PoSe) determination, Subquorums and Superquorums for Chainbond Protected Swaps and execution of the Strategic Governance protocol.

In addition to the above node types, a non-collateralized 'Full Node' may be run on the network. Masternodes are the reference for network state consensus, but if a complete copy of the blockchain is required for authoritative transaction verification, the Full Node may be used. For lightweight transaction verification operation, it is possible to run a Simplified Payment Verification[8] (SPV) client (as per the Bitcoin network), where only block headers are downloaded by the client rather than the entire blockchain and connectivity to either a plurality of Full Nodes or Masternodes provides information about specific transactions as required.

[8] https://bitcoin.org/en/operating-modes-guide#simplified-payment-verification-spv

Collateralization of Service Providers

Table 1 kNET collateralized service providers (Network Provider - NP, Service Provider - SP).

Service Provider	Description	Collateral Required	Base Vote	Reward Payment – determination by governance
(NP) Masterminer	Collateralized block mining and transaction storage	100000 KUVA Utils	100	At Apex; 250 KUVA per block, settling to 20% of block budget
(NP) Masterlan	Collateralized real-time authority node. A Superlan that is activated with bond becomes a Masterlan	100000+100,000 KUVA Utils Bond	200	At Apex; 200 KUVA per 7 days (post-Apex + quorum fee share) settling to 20% of block budget
(NP) Superlan	Collateralized real-time supervisory and audit node	100000 KUVA Utils without bond	100	At Apex; 50 KUVA per 7 days settling to 10% of block budget
(SP) Master Agent	Providing currency settlement (physical cash delivery, payment card provisioning, bank account payments) to both end-user groups and service providers.	10000 KUVA Utils	10	At Apex; Dependent on trade and set by Strategic Governance Block Budget Ratio
(SP) Independent Agent	Providing end-user settlement on an independent operator basis. Founding services include cash-out and hawala services but will extended to other products delivered over kNET	1000 KUVA Utils	1	At Apex; Dependent on trade and set by Strategic Governance Block Budget Ratio

Strategy and Governance

kNET also includes governance protocols intended to progress the network in the longer term to a 'dynamically decentralized' system. Purely distributed networks without representative forms of strategic governance have been shown to gravitate towards centralization – aggregating leadership, and pooling mining and software consensus, exchange functions, branding, and so forth. At the same time, the establishment of permanent and non-displaceable hegemony is not desirable either. We propose a strategy and governance for the network that is decided between two aspects; collateralized network infrastructure operators (Masterminers and Masternodes), and collateralized Licensed Service Providers (LSP's) providing external services over the network.

Any member of the public or a third-party organization may post a Strategic Governance Proposal (SGP) for voting. An SGP becomes activated on the network through stakeholder voting, the result of which is enabled through a once-monthly generation of a special type of block called the Governance Block. Collateralized stakeholders (both infrastructure providers and LSP's), post a current vote on a

proposed Strategic Governance Proposal. The vote is retained as valid in perpetuity while the voting node remains collateralized and the SGP is active or available to be voted on.

The SGP voting is locked monthly, approximately 3 days before the creation of a Governance Block, and the winning Strategic Governance Proposal then becomes activated at that time. The owner of the SGP, known as the Strategic Governance Proposal Owner (SGPO), formally pre-defines the use of all block rewards within it, these being split in a ratio between the SGPO's payment address, but also Masterminers, Masterlans, Superlans, Licensed Service Providers and User Rewards, for which a plurality of deterministic masternode and service provider lists (and the corresponding payment addresses) are maintained and cycled in a round-robin to participate in the reward payments within every block.

The block reward ratio allocations and service burn fees, defined in a voted-in SGP, form a feedback mechanism that allows for incentives to find a natural market balance, in accordance with the needs of network participants and users. Where participants are objectively delivering a high quality of service to users, they are rewarded through boosted influence over the selection of their chosen SGP, as well as a higher payment reward for their services.

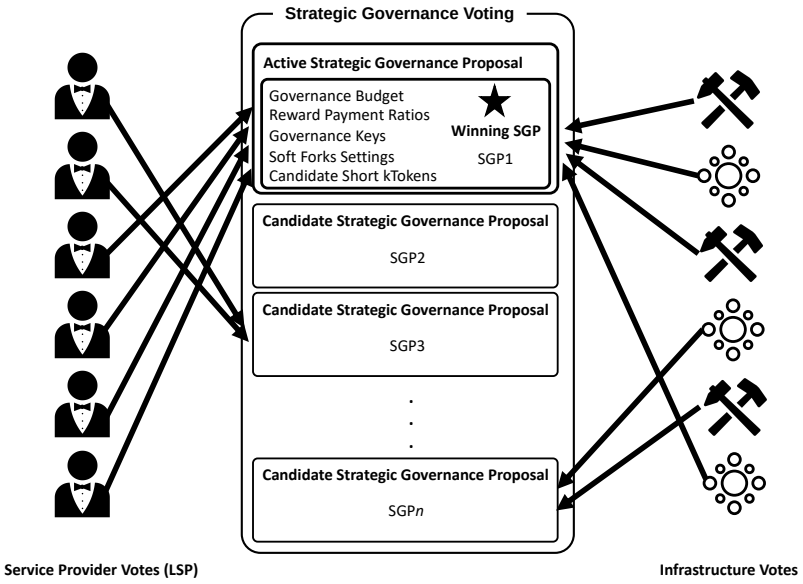

Figure 4 Strategic Governance Proposal voting

Strategic Governance Proposals

In kNET, the active SGP is allocated a monthly Governance Budget of up to 10% of all KUVA that is generated when miners create new blocks. The SGP also pre-defines per-block external service

provider rewards and payment ratios, called the Incentive Ratios (IR). These must be pre-defined prior to the SGP becoming active, since they cannot be changed from within an active SGP. These are the variable key incentives for all collateralized non-network service providers on kNET and serve to provide a multiplier that ranges from halving to doubling the base reward given on the network. The Strategic Governance Proposal Owner of the active SGP also maintains active Governance Keys. These are a set of public/private key pairs that allow active SGPO to securely turn on and off aspects of the network via Switches, for activating any protocol updates and features of the network[9]. The Switches and SwitchBitfield are network-wide parameters for enabling or disabling features of the network, as well as setting feature parameter values, and are automatically applied when the winning SGP becomes active. Depending on the Switch, some are modifiable using the Governance Keys, but others must be defined within the Strategic Governance Proposal and are set by the Governance Block. Any member of the public may post an SGP by burning the required amount of KUVA to allow their proposal to be posted to the network for voting[10]. SGPs that are posted for voting (but are not the active SGP) can be voted on as a candidate SGP for a length of time determined by the amount paid to post the proposal. The cost to post a proposal and keep an SGP as a valid candidate is currently 500 KUVA[11] per month.

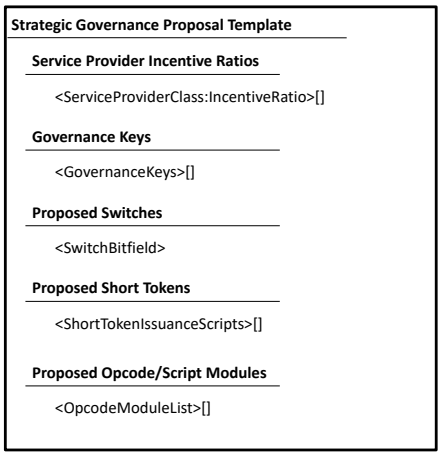

Figure 5 Strategic Governance Proposal Template summary

Governance Blocks and Voting

Any collateralized service providers can post or recall their votes on any SGP. Votes may be cast on an active SGP by masternode owners and Licensed Service Providers in the network, through a

[9] These are an array of bits that are set by the active Governance Keys for the network and define various features and currently active kNET protocol version for each node type.

[10] Public SGP submission will become available after establishment of the kNET Apex and opening of the infrastructure to public operation.

[11] Provisional amount – to be finalized

public/private key pair used for the purposes of proving their vote (and corresponding collateral address ownership). The currently winning SGP becomes the Active Strategic Governance Proposal and is allocated the entirety of a proposed Governance Block budget (up to 10% of block budget). Following this, the SGPO's Governance Keys become valid for the network, and may be used to activate, suppress functions or provide updated parameters for network-wide functions.

Governance Keys

The Governance Keys are included in any Strategic Governance Proposal, allowing for activation or deactivation of critical network functions via the Switches by the winning SGPO, while that particular SGP retains the majority of collateralized stakeholder votes. The Governance Budget is used for direct SGP financing; payments are made directly to the pre-defined wallets of each organization being funded by the Strategy. This distribution of funds can be made on either a per-block basis, (for Masterlans, Superlans and also Licensed Service Providers), or once a month through the process of the Governance Block generation, a treasury accrual and disbursement that is made in that Governance Block, on a monthly basis. At the creation of the Governance Block, the Governance Budget will be distributed across the wallet addresses of each organization pre-defined in the single winning Strategic Governance Proposal, and the creation of the Governance Block also activates the Governance Keys of the SGPO. The new Governance Keys of the winning SGPO become valid at the point the Governance Block is generated; only if there is a change of governance to a new SGP are the current Governance Keys revoked. To pass and become active, an SGP requires both a simple majority of collateralized stakeholder votes and also that a minimum amount of 20% of all active masternodes retain their votes[12] on Strategic Governance Proposals.

Trias Politica Network Structure

A 'separation of powers' within the network structure that forms kNET's polity exists and can be broadly compared to the 'trias politica'[13] model of 'Executive', 'Legislative', and 'Judiciary'. Normally, end-users who transact over the network and are satisfied with the service they are given will provide positive ratings to Service Providers. These ratings give a boost in voting power to those Service Providers (Executive), and for high transaction volumes and user satisfaction, yield a voting power that is higher than the voting power of Network Operators. If end-users are not satisfied with the services they are provisioned, or if they are simply not transacting on the network, then the voting power of the Service Providers is diminished. In that case, the Network Operators (Judiciary) obtain an increased

[12] Votes are persistent, meaning that they remain on SGP's for as long as that SGP is active or the SGP is eligible to be voted on.

[13] https://en.wikipedia.org/wiki/Separation_of_powers

voting influence to displace the Strategic Governance Proposal (Legislature), and/or to put pressure on the active Strategic Governance Proposal to make changes relating to the governance of the network.

In this way, although the active Strategic Governance Proposal functions as the 'legislative branch' for the network, the power to change it shifts between network infrastructure operators and service providers, depending on the satisfaction level of end-users and the corresponding volume of transactions being made on the network itself.

kNET Domain Operator	**Governance Aspect**	**Description**
Active Strategic Governance Proposal	Legislature	**Strategic Governance Owners:** Determination of budget ratios, protocol adjustments, maintenance of Governance Keys
Masternodes Masterminers (Infrastructure)	Judiciary	**Network service providers:** Execution of Observations and Determinations in relation to network transactions, and adherence to protocols
Collateralized Licensed Service Providers (LSP)	Executive	**End-User Service Providers**; as per related service provisioning protocols

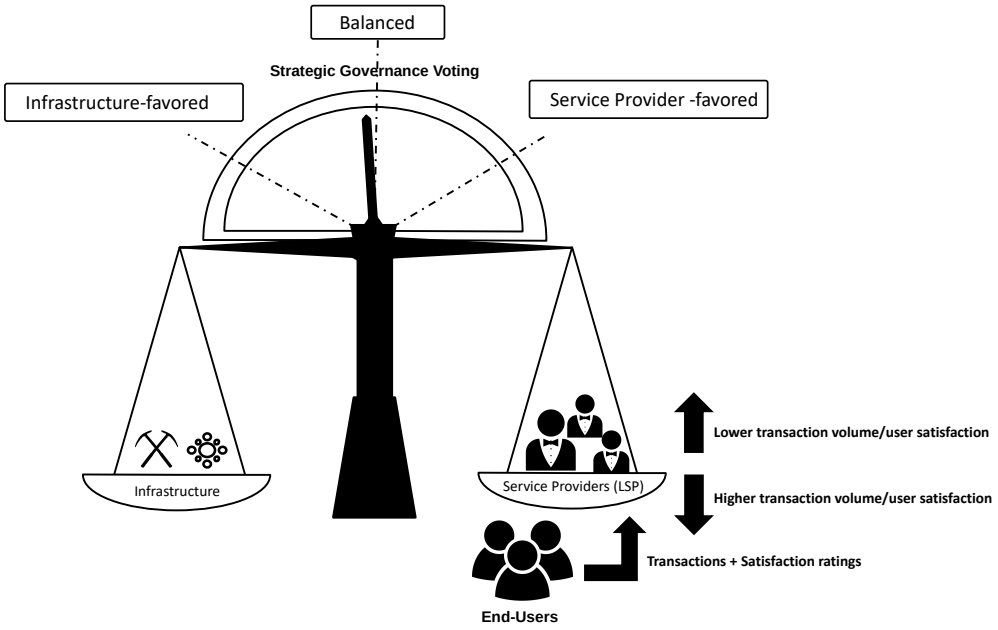

Figure 6 kNET Strategic Governance determination by end-user ratings and transaction volumes

Governance Initiation and Transition

In the same way that the network infrastructure starts privately with the construction of the kNET Apex, Strategic Governance will also be managed by a Kuva Coin Trust delegate[14] before its eventual transition to public and open stakeholder voting enforcement.

Strategic Governance Allocation of Treasury Funding and Incentives

The problem of a flat DAO structure (for example, the structure used by the Dash cryptocurrency for its DAO), is that allocated proposal funds generated in a 'superblock' on a monthly basis are spread across multiple and competing treasury proposals[15]. Rather than stakeholders making broad disparate allocations, kNET's Strategic Governance ensures that kDAO Treasury funds and block rewards are allocated strategically and managed in a focused way.

By allocating Governance Budget funds under the structure of a single SGP (through multiple wallet addresses receiving a proposed allocation of funds), and by defining the distribution ratios for

[14] Kuva Global Trust operations delegate

[15] Dash DAO treasury funds have historically been spread across proposals without a common strategy for allocations. Users play no part in the allocation of funding, only masternodes are able to vote.

collateralized network and external service providers, this structure allows the funding of a singular democratically elected strategy, focusing resources optimally for execution.

In kNET, collateralized Licensed Service Providers with high transaction counts with positive service ratings are allocated the highest voting power. In this way, LSPs providing the most valuable services to users are given the most control of the network's strategy. If users are not happy with the services of a particular type of LSP, they will shift voting power from one LSP to others, either directly, by transacting with other LSPs, or indirectly, by providing lower ratings to LSPs they transact with. In this way, it is the users themselves that are the key deciders of the active SGP of kNET. Ultimately, the winning SGP that emerges from this framework is one that leads the network to a high volume of transactions that are deemed most useful to the network's end-users. This structure helps an operational balance emerge across Strategic Governance, the provisioning of services, and the evolving requirements of kNET's end-users.

Thus, kNET allows for establishing a dynamically decentralized economic network between performant participants, with a democratically elected and transferable strategic center, allowing for rapid innovation within and outside of the network.

kNET Licensed Service Provider

By providing Proof of Collateral, a service provider becomes a Licensed Service Provider (LSP) with connectivity to kNET which allows them to deliver services on the kNET network in an assured way. Examples of this are cash-in and cash-out agents, master agents, physical ATM operators, mobile carriers providing data plans, drive-share operators and so forth – any service operator that registers on kNET to discover customers and receive payments. An LSP must collateralize an address that they control the private keys for, with the specific amount of KUVA required for them to register themselves as a service provider on kNET. This gives end-users exposure to services on the network that the service provider can facilitate. The Proof of Collateral is provided by the service provider by demonstrating they have the registered private Service Keys related to the address they have moved collateral into. Along with this movement of collateral, a service provider will also register what the service it is that they are collateralizing. Once successfully registered as an LSP in this way, a service provider will then be able to access customers, deliver that service on kNET, and receive payment.

LSP's can provision two kinds of services; 'Atomic' services, which are a single transaction and a corresponding customer rating; for example, a physical cash-out from an ATM provider, or a ride-share. Alternatively, an LSP can provision 'Stream' services which are provided on a continuous basis. Some examples for Stream services are; an on-demand electric utility providing electricity to a home, or premium video content delivery to a user.

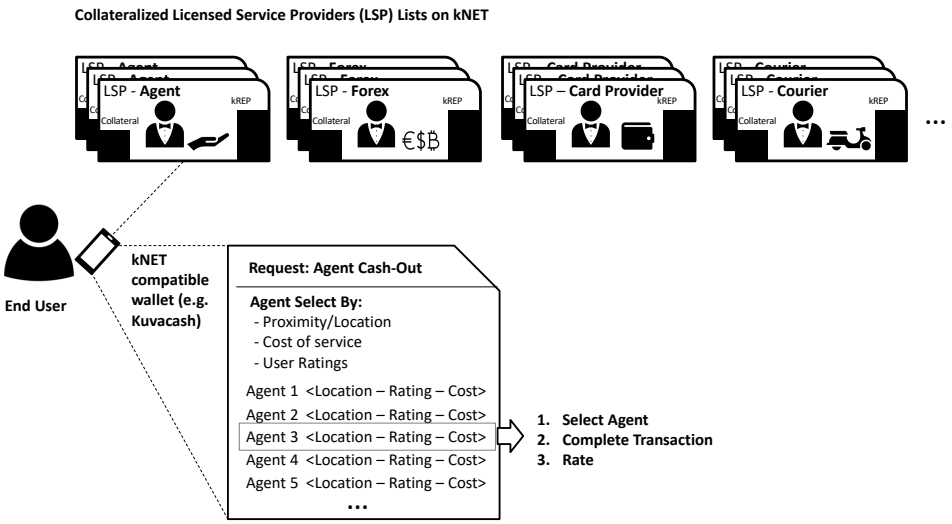

Figure 7 End User selection and transaction overview with a Licensed Service Provider – the example is of an Atomic service

kREP Persistent Reputations

LSP's retain a reputation score at the collateral address of their license. This reputation score is derived through special coins called kREP being sent to that address. A single kREP coin is generated in the context of a 'service transaction', which describes a service provisioned to and paid for by a user. To rate the service provided by the LSP, the user sends a proportion of the kREP back to the service provider (the user may send either the whole or part of the coin to the service provider's collateral address). kREP coins cannot be moved from the address they have been sent to (the actual collateral itself can always be sent to other addresses, but the associated kREP coins cannot).

kREP scores are provided to an LSP on a per-service-transaction basis and are used to boost or inhibit both the rewards and voting power that an LSP has on the network. For example, an LSP with a high kREP for the services they have provided to customers will be preferentially listed when displayed to a customer who is requiring that particular service (other factors will drive placement, of course, such as geo-location of the user, specified service availability). An LSP's reputation score also boosts the LSP's voting rights on the kNET DAO (kDAO) governance. In this way, LSP participants consistently delivering highly rated services at volume over kNET will emerge with more voting power to vote for their Strategy of choice. They are also more likely to retain their collateral at that address and to continue to provide services on kNET if they have collected a high reputation for their services. This exerts a net deflationary effect on the supply of KUVA on the network, since service providers are unlikely to want to sell collateral if they can earn correspondingly higher rewards on their collateralized node with a high reputation they have developed through service.

It is important to allow a Licensed Service Provider to sell their kNET Licensed Service Provider business, because if they choose to exit, they should be able to sell the entire value of what they have created on kNET as a Licensed Service Provider rather than simply sell their KUVA collateral only – their KUVA will be only one part of the business' value. Transactions can either move the entire collateral+kREP to another controlling party in one atomic transaction or can move a part or all of the collateral (in this case the kREP will not be moved). When collateral moves with kREP, it signals to potential users that the business has had a change of ownership or management, which may inform their choice as to whether to purchase services from that provider.

kREP and the Adaptive Governance Model (AGM)

kNET's user-centered Strategic Governance is determined by the Adaptive Governance Model (AGM). This involves the assignment of verifiable "user ratings" by a user per transaction with a Licensed Service Provider. User ratings may be obtained from users in several ways, for example, rating-based (e.g., 5-star system), continuous (sliding scale), or qualitative (text that can be analyzed and responded to). Within service categories, key performance indicators can provide standards to objectively determine the level of service being provided by one LSP in relation to another (e.g., avg. time from booking to complete in the category of fiat cash-out). Ratings can only be made against validated transactions that users have made with service providers within the kNET network.

In kNET, validated user ratings that collateralized service providers accrue boost the voting power of those service providers in the democratic selection of a Strategic Governance Proposal (SGP). An SGP that does not reach high objective user rating scores (the satisfaction of users) or an SGP that does not propose incentive splits that network stakeholders will accept, risks being voted out in favor of an alternate SGP. Thus, the network governance is structured towards the outcome of maximizing objective user satisfaction scoring over time.

This can be pictured as a control system with primary feedback from end-users. This feedback is only possible within the context of a transaction between an end-user and the LSP provisioning a service for that particular transaction. The feedback either inhibits or boosts the votes and rewards of that LSP. Rather than paying incentives to and being controlled by only one or two actors providing the network infrastructure, (for example, miners in Bitcoin or miners/masternodes in Dash), kNET is an active system that utilizes this verifiable user feedback to influence its strategic governance. A successful SGP allows for the right balance of incentives across the network to emerge which achieve the highest level of satisfaction for end-users. The user ratings are stored permanently as a special transaction sent to the service provider's collateral address by the user, called a kREP. A single kREP token is generated at the point a transaction for a service is completed between a user and a service provider. A user,

through a combination of explicit and/or automated methods, can elect to send any fraction of it only to the specific service provider they interacted with for that transaction, in consideration of the service provided, within a timeframe window of *n* blocks from the closure of the transaction, *n* being dependent on the Service Class. The kREP is accompanied by a SHA-256 hash of a text comment submitted to that service provider, which the service provider can retain if they so choose, the hash itself being used to verify feedback the service provider regarding any text related to the rating [16]. The kREP, textual feedback and hash proof are useful for the service provider to gain any insight required to improve their services, to demonstrate their responsiveness to feedback, or to market to other potential customers. Any fraction of kREP that is not sent to the service provider, that is, any kREP 'change' remaining in the service rating transaction from the end-user to the service provider, is deemed burned.

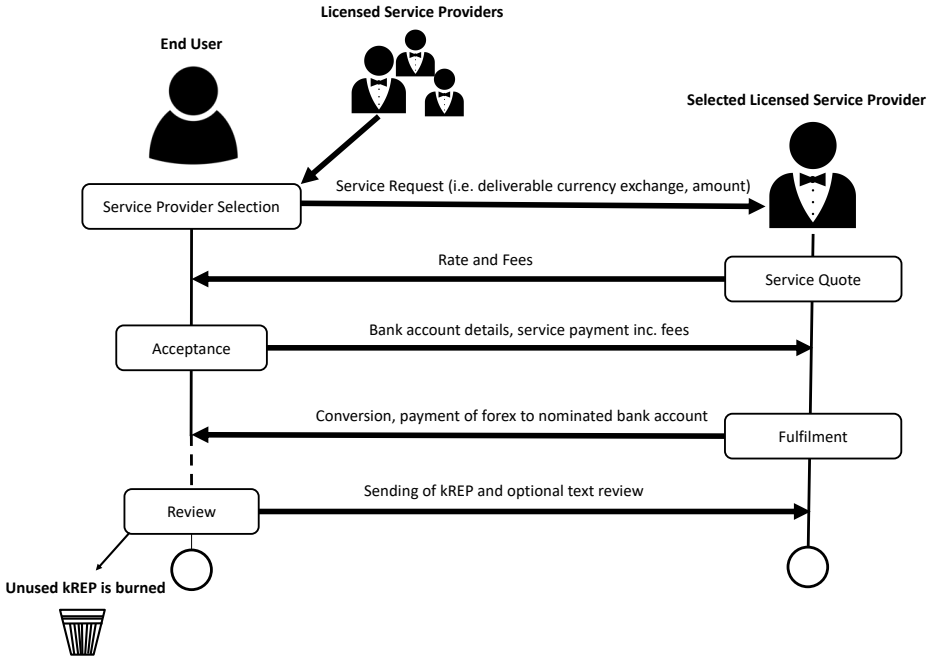

Figure 8 End User transaction and rating of Licensed Service Provider using kREP

Once a kREP transaction is sent to the specific service provider it was intended for, it cannot be moved without moving the entirety of the collateral as well. It is known as a 'sticky transaction' that resides at the address associated with the collateralization of the service provider. This means that if the collateral is sent to another new address in one transaction, the kREP will also move to that new address. However, if the collateral is transacted in increments, then the kREP will not move with it. This

[16] The storage of these ratings may either be retained on the blockchain/distributed storage or stored privately by a service provider.

mechanism allows a service provider to sell their retained value in any kNET business they operate, including the associated SGP voting boost and rewards that come with it from accumulated kREP.

The kREP that a service provider accumulates at an associated collateral address over time, together with other transaction data (size of transaction, any category specific KPIs, etc.), directly affects that service provider's power to vote for an active Governance Strategy.

The quantity and recency of kREP also boosts or inhibits the reward share that the Licensed Service Provider is paid for being an active service provider on the network. This is known as a "kREP Boost" score, which a Licensed Service Provider maintains at their associated collateral address. The kREP Boost score is a multiplier for the Service Provider's Base Vote and will apply on an ongoing basis to any active votes that service provider has cast for a Strategic Governance Proposal. In a generalized form, the effective vote V_e for a collateralized Licensed Service Provider is approximated as;

$$V_e = \sum_{i=0}^{Tcount} \frac{kREP_i * Tsize_i}{\ln\left(B_c(i)+1\right)} * S_{BV}$$

Equation 1 Effective Voting function for Licensed Service Providers

This is the effective Voting function where an amount of $kREP$ is received per transaction of normalized amount T_{size}, and B_c is the block count from the chain tip where the transaction was located. T_{count} is the number of i transactions that the LSP has executed and S_{BV} is the service provider's Base Vote.

With this method of Strategic Governance determination (and following the transition of kNET to public and community operation), the network will direct itself over time towards a balanced mode of operation across both aspects – decentralization and strategic governance.

kNET Masternodes

The concept of Masternodes as participants in an authoritative network tier which provide rapid validation and locking of transactions prior to confirmation into a block, as well as management of governance determination through budget allocation, was introduced by the Dash cryptocurrency network[17] and extended to the 'masternode quorum' concept[18]. A 'masternode quorum' is a subset of masternodes, selected from a list of available masternodes[19], which through a distributed key

[17] https://github.com/dashpay/docs/blob/master/binary: Dash Whitepaper – Transaction Locking and Masternode Consensus.pdf

[18] https://github.com/dashpay/dips/blob/master/dip-0006.md

[19] https://github.com/dashpay/dips/blob/master/dip-0003.md

generation and a threshold signature schemes can be used to rapidly reach an authoritative consensus as to a particular transaction or network action and broadcast the result in a verifiable way to form a network consensus. This concept and approach for locking transactions as well as collecting votes for distributing the funds generated by its treasury is currently in operation on the Dash cryptocurrency network as a 51% attack prevention method and to secure instant transactions between users.

This masternode quorum concept must be adjusted when used on a multi-coin platform such as kNET to enable appropriate levels of transaction security, since the collateral held by a masternode is KUVA Utils, and this may be different from the asset being transacted in real-time with instant finality. The following describes Hierarchical Masternode Quorums as well as the Chainbonding concept used in securing transactions on the network.

kNET Hierarchical Masternode Quorums

kNET uses Hierarchical Masternode Quorums (HMQ); an ordered and deterministic list of variably sized masternode quorums, created under a parent-child structure, that are selected when performing real-time locking of transactions on the network to secure against double-spending, but also for other functions requiring an authoritative determination. HMQs can be considered a form of distributed Delegated Proof of Stake consensus – the validators are not central parties, but instead a quorum group of collateralized masternodes is formed and acts as a 'distributed validator' for a period of time, and for a particular function performed on the network. For example, these quorums are used to implement UXTO locking for instant transactions, for implementing on-chain asset swaps between kTokens, as a part of mining sessions to secure against various attacks and for enabling Chainbond Protected Swaps between independent cryptocurrency networks. The size of the masternode quorum and any bond posted, determines the amount of security which covers a particular validation requirement, since kNET operates with service providers collateralized in Kuva Utils, but moves coins that may not be denominated in that collateral (e.g., USDk or GBPk). As kNET is a multi-coin network with varying values of each coin, the appropriate minimum size of masternode quorum is selected when locking an instant transaction relating to a particular asset (the representative collateral of its members providing the incentive for good behavior among its members). One reason for the initial development of the kNET Apex network, and the pricing behind the KUVA Utils at launch, is to ensure that bond collateral of an adequate value is held by the network at inception.

Service and Network Fees

There are two tiers of fees on kNET; the first are external 'service fees' that LSPs charge end-users for their services. For example, these could be top-up fees, cash withdrawal fees, transportation and

courier service fees, insurance premiums, and the like, which are still settled using the network and using any currency the service provider accepts which is also supported in kNET. Internal service fees are the kNET 'network fees' that relate to a particular service (for example, fees on a simple agent-based physical cash-out transaction). The internal network fees are always charged in KUVA Utils to a service provider and are 'burned' in the transaction.

Licensed Service Provider Class Deterministic Lists and Rewards

Collateralized service providers are maintained in deterministic lists and provide network infrastructure as well as delivering kNET's end-user services across a number of Service Provider Classes. Within kNET, these providers will be rewarded on an ongoing basis for their validated services to the network. All providers that provision valuable services to the network are directly rewarded with KUVA Util cryptocurrency alongside any other profits they would make by provisioning the service to their particular customer.

Each network provider on the network resides in a network superstructure known as a 'Service Provider Class Deterministic List'; this includes Masterminers, Masterlans and Superlans. Non-infrastructure Collateralized service providers who provide services directly to end-users and businesses, such as Master Agents, Independent Agents, payment processors, merchants, exchanges and so on, will reside in their own Service Provider Class Deterministic List. New Service Provider Classes will be added to kNET as its usage grows to meet demand from users, via the Strategic Governance process.

Lists of collateralized LSP's within each service provider class are maintained in a deterministic way, such that it is possible to derive the order for selection of a reward payment.

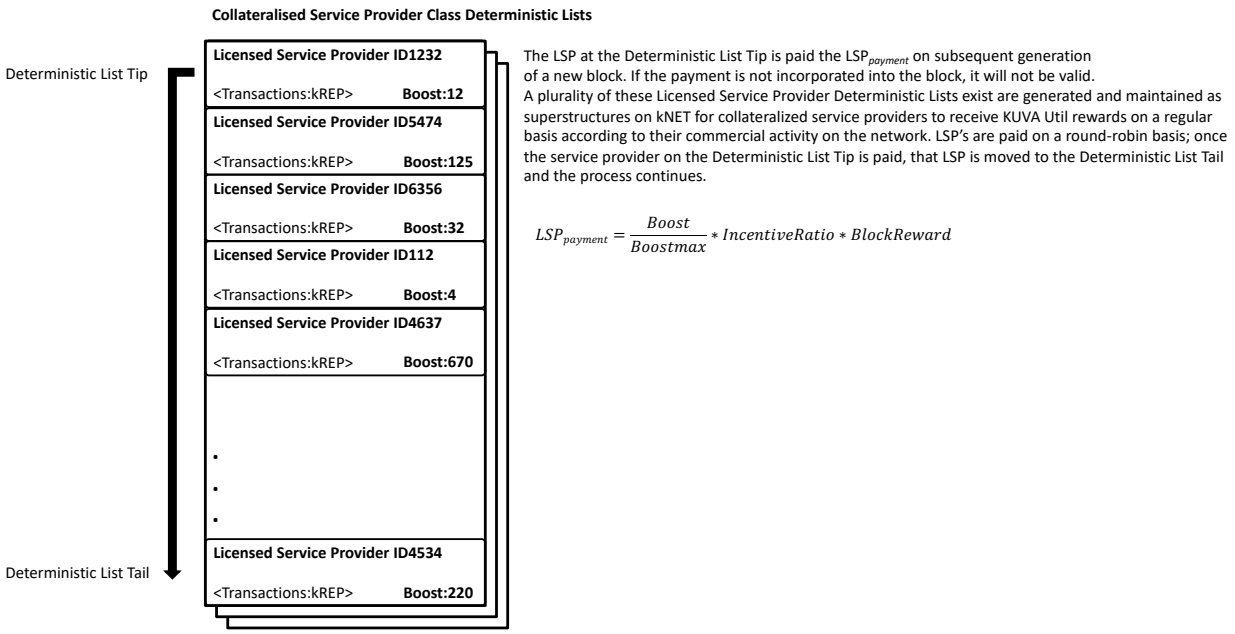

Figure 9 Collateralized Licensed Service Provider Class deterministic lists

kNET extends the use of deterministic lists from infrastructure and service provider payment selection and applies it to several other features of the network;

1. Hierarchical Masternode Quorums
2. Masternode Mining Quorums
3. Fair distribution (and regionalization) of service requests by end-users to service providers

Collateralization and Voting

Registration as a collateralized service provider on kNET (Masterminer, Masterlan, Superlan or external Service Provider) involves the following;

1. Publishing initial proof that the requisite service activation collateral is present and controlled by the registrant (providing collateral transaction hash and address).
2. Registration of Owner and Voting public keys (external provider) and Operator key (for infrastructure operators).
3. Providing the payment addresses for any rewards paid, and payment ratios.
4. Providing KUVA bonding collateral (which activates Masterlan functionality and rewards).

These steps are performed within a kNET Service Provider registration transaction. Each service class has a specific number of block confirmations that they must wait for before their service becomes

active. Once the registration of the Owner, Voting and Operator public keys has been completed and is confirmed on-chain, service providers may begin to offer services to users and receive rewards and service payments. Network provider resources will be registered in the relevant deterministic list and will be activated to provide services to the network and receive subsequent reward payments in line with their Proof of Service scoring.

KUVA Util Collateralized Mining Sessions (CMS)

kNET develops and reaches consensus as to the state of its blockchain through a process involving both Proof of Work and Masternode Mining Quorum consensus as an arbitration system for the selection of the authoritative chain-tip and selection of a winning block in the case of any contention, to provide protection against blockchain reorganization/forking attacks and 51% attacks – known as the 'Running BlockLock' process. Each of these aspects adds a corresponding layer of security to the network, allowing for performant operations of the network while minimizing risk of attack;

1. Masternodes cache and provide a first-pass locking of transactions via a masternode quorum. This enables instant transaction capability across the network (enabled for transactions under a certain size[20]).
2. Collateralized Masterminers confirm transactions into blocks via X11 based Proof of Work[21] and a 150-second Mining Window. A corresponding block reward of 20% of the generated Utils (as per the Generation Curve[51]) is paid to the miner for solving the block.
3. Masternodes use a quorum called a Masternode Mining Quorum, or MMQ within the Mining Window to authoritatively select the next valid block on the chain and broadcast their determination to the network. This minimizes the risk of a blockchain reorganization or '51%' attack (although this risk is already reduced since the network maintains collateralized miners).

Generation of KUVA Utils

KUVA Utils are generated (and regenerated) through the process of CMS. The address of the miners' valid collateral and a valid signature related to a miner's delegated mining key for that collateral is included and hashed in the block header as a part of PoW mining. The delegated mining key is not a private key that can spend the associated collateral, but a public/private key pair used for proving its ownership. This is activated when the miner broadcasts their registration as a service provider on the network. The registration of a delegated mining key is stored/confirmed on the blockchain by way of a special transaction, and 600 confirmations are required before a Masterminer may begin to commence

[20] Masterlans may process native KUVA Util transactions of up to the size of the collateral they hold.

[21] X11 for Apex network, transitioning to an alternative hashing chain post-Apex

mining and submission of valid blocks to the network. Separation of the private/public delegated Mining Keys and the collateral private key allows for delegated mining, in which an owner of the collateral KUVA Utils may purchase hashing power from a mining farm, and where the miner providing the hashing power does not need control of the collateral itself. The delegated Mining Key can be both assigned and revoked by the actual collateral owner.

BlockLock - Blockchain Deep Reorganization/51% Attack Resistance

It is also possible that an attacker will mine a shadow chain with very high mining power in an attempt to overtake the PoW and force a deep blockchain reorganization/fork. This could be constructed to send coins that the attacker has already spent back to the attacker. Prior valid transactions the attacker made that would have been considered final after a number of confirmations on the blockchain would revert back to the mempool[22] and be subsequently rejected by nodes. One method to add security to the mining process is that Masternodes will always reject a block that has the same collateral proof as a block which is less than *n* blocks behind the current chain-tip, where *n* is higher for lower numbers of miners on the network.

Within the mining process, when a valid Block Candidate is found within a Mining Window, the collateral's associated delegate mining key signature is checked by the current Masternode Mining Quorum prior to broadcasting a 'BlockLock' as the current authoritative chain-tip. Three pre-checks are performed;

1. That the delegate mining key signature corresponds to a validly registered miner and that the associated collateral remains unspent.
2. That the current chain-tip referenced by the valid block candidate corresponds to the authoritative chain-tip as per Masternode Mining Quorum determination.
3. That the registered miner does not have another block that it created which has been incorporated into the blockchain for at least *n* blocks from the authoritative chain tip, where at a minimum n>5.

The first check ensures that the Masterminer is registered as a valid service provider on the network. The second check ensures that the previous block references the authoritative chain-tip which has been determined by masternode quorum and for which the header hash been broadcast to all nodes on the network.

[22] https://www.mycryptopedia.com/mempool-explained/

As well as broadcasting the current authoritative chain-tip to the network, the Masternode Mining Quorum will also calculate and broadcast a special 'BlockLock Root' which must be incorporated into block header of the next subsequent block. The BlockLock Root' is a Merkle root[23] of the hashes of the prior 256 block headers from the chain-tip. This provides an additional protection channel as a witness against malicious deep blockchain reorganization attempts to be used by the Masternode Mining Quorum and all collateralized network nodes, thus further securing the latest blocks up to the chain-tip.

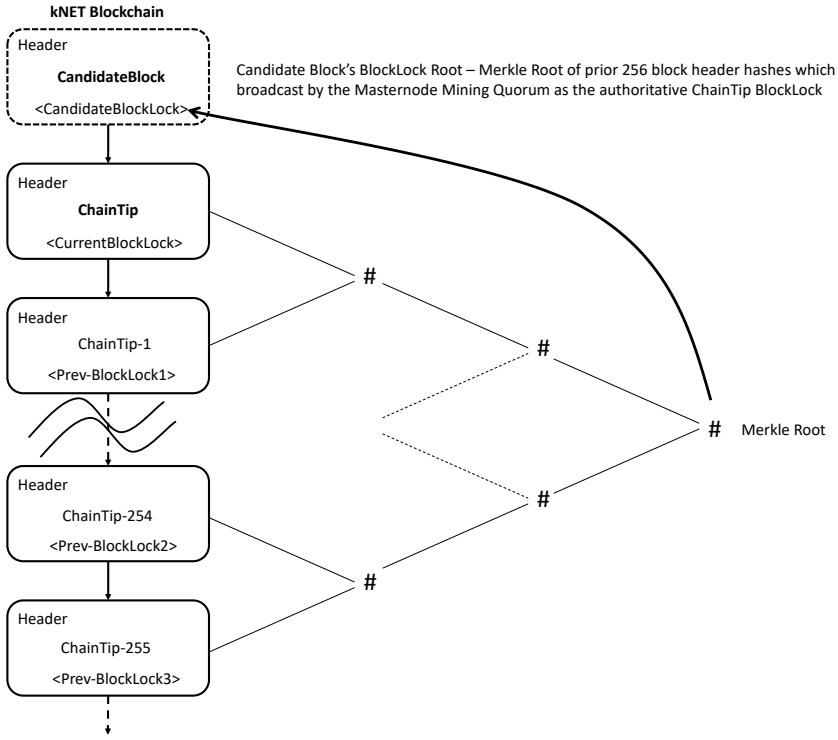

Figure 10 Running BlockLock calculation providing deep blockchain reorganization and mining majority (51% attack) resilience

The third check is to ensure any particular group that is providing mining power also holds collateral commensurate to the hash-rate they would economically provision to the network. This particular check makes it more difficult to attempt a deep blockchain reorganization attack, since attackers would have to maintain considerable collateral associated to each miner to submit the sequential candidate blocks in order to attempt such an attack. At the very least they would need 5x the collateral required to attempt a blockchain reorganization at a depth of 5 blocks. The Masternode Mining Quorum selects the winning candidate block and broadcasts its selection to the network along with the BlockLock. The

[23] Double-SHA256 Merkle Root

BlockLock will then need to be included by miners in the next block candidate's block header, thus a block reorganization attack becomes more difficult to implement.

The design above highlights some of the ways that collateralized mining combined with Masternode Mining Quorums and BlockLocks adds security to the network from external attack. In particular, by requiring all service providers to be collateralized and by limiting the mining power they could usefully provide the network for each registration of miner collateral, Sybil[24] and deep blockchain reorganization attacks become prohibitively expensive and therefore less economically feasible for any attacker to implement.

Block Time and Difficulty Determination

The Block difficulty is targeted through Dark Gravity Wave (DGW) 3.0 such that the block time is approximately every 150 seconds. The difficulty adjustment is also determined by Masternode quorum as a fallback scenario. This is used if a block is not found across multiple anticipated Mining Windows. Because the sale of a miner's collateral deactivates that miner, there may be a need for the network to allow for unexpected and very rapid drops in mining power and a corresponding need to adjust difficulty prior to the generation of the following block. The network should allow for fluctuation of mining power, especially since this requires collateral to be held by the miner. To allow for this, a Masternode Mining Quorum (MMQ) is maintained which observes that block generation is continuing and provides for a difficulty adjustment fallback. In this process, each member observes its view of the current network time, and its own real-time-clock. A quorum determination is triggered if the previous block was generated more than 10 minutes prior, and if the quorum determines that a valid block was not found within the subsequent 5 minutes, a 'difficulty override' message is broadcast to the network, signaling to miners that they may lower difficulty to 90% of the current difficulty, following which the timer is reset. This process is repeated until a block is found. At that point, the masternodes lose the difficulty adjustment priority, which is reset by the DGW difficulty calculation and historic block timings, and mining continues as normal.

[24] https://en.wikipedia.org/wiki/Sybil_attack

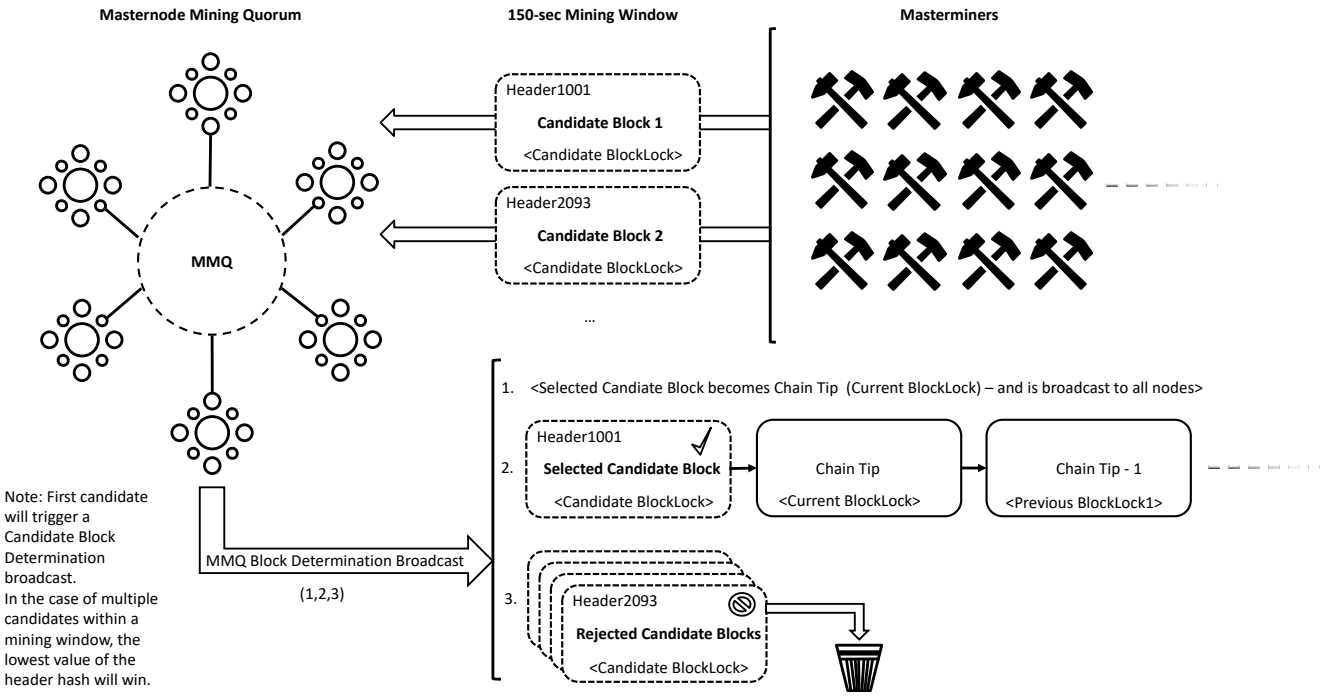

Figure 11 Collateralized Mining Session with Masternode Mining Quorum and Masterminers, operating within a Mining Window and incorporating BlockLocks.

Block Contention

It is still possible that in this small group of miners, two or more Masterminers will find valid blocks at approximately the same time, which could lead to a fork contention. All new valid candidate blocks within a Mining Window are submitted to quorum selection by the MMQ. In the case of multiple valid candidate blocks within the Mining Window time, the block with the smallest numerical value for its block header hash will be determined to 'win' a MMQ, and the new Candidate BlockLock hash will be calculated and broadcast, signaling to all nodes what is now the valid block header hash of the authoritative chain tip. This will cause them to reject all other candidate blocks within that Mining Window from that point onwards. Following this, the winning Candidate Block is the new chain tip block and is propagated to all nodes on the network.

Block Reward

The MMQ calculates and sets the maximum amount of KUVA to be generated in the next block within the Collateralized Mining Session, corresponding to the KUVA Generation Curve[51]. When mining a block, Masterminers must not generate more KUVA Utils (as block rewards) than this amount, or their block will be rejected by the MMQ and not included on the blockchain. Block rewards are allocated in line

with the Block Budget ratios set in the current active Strategic Governance Proposal, with Masterminers receiving 20% and Masterlan and Superlan masternodes each receiving 20% and 10% of the Block Budget, respectively.

kNET Apex Masterminers

Collateralized Miners serve to process transactions on kNET, as well as calculate, generate and distribute KUVA payments to Licensed Service Provider Lists, including all forms of Masternodes (Masterlans and Superlans).

For the Apex network, a plurality of reference Masterminers in kNET will be operated across select data centers by the Kuva Global Trust to secure the network and process transactions. The mining algorithm for Masterminer nodes running within the founding Apex network is X-11[25], a concatenated series of hashing algorithms that is used across several cryptocurrencies for providing mining difficulty. Prior to Masterminer operation being open to the public, the hashing algorithm will be transitioned to an alternate concatenated hashing series to restrict mining to GPU and CPU only for the medium term. The exact hashing algorithm and subsequent migration will not be disclosed until after the opening of the public mining launch.

The transition to public participation in mining will occur a short while following the transitioning of the Apex network to public operation, in a staged approach in line with security and network availability/scaling requirements.

kToken On-chain Atomic Swap Transactions

The ability for efficient and secure exchange of assets between market participants forms a key part of any economic system. Because kTokens all reside on kNET, it is possible to implement the functionality of instant kToken swaps through counterparty signature checks in a spend script for an atomic transaction. A transaction would include the swap of both assets within the single transaction context, so there is no need for a bond to be held.

[25] https://en.bitcoinwiki.org/wiki/X11

Chainbond Protected Swaps (CPS) for cross-chain exchange

Through the use of Hierarchical Masternode Quorums[26] on kNET, it is also possible to allow for protected cross-chain swaps[27] between multiple public cryptocurrency networks/blockchains. The solution proposed is largely third-party cryptocurrency protocol agnostic. The process initially supports any cryptocurrency that allows for m-of-n multi-signature ECDSA-based transactions via a Pay-to Script Hash (P2SH) style format for locking and spend scripts. This includes bitcoin-based blockchains, DAG-based networks and masternode enabled networks, so long as it is possible to construct and sign multisignature transactions, broadcast these to the corresponding network and publicly observe the transaction finalization through connection to a plurality of nodes on that network, or by maintaining a copy of that network's ledger/blockchain. This form of cross-chain asset swap is not considered 'atomic' as it is not necessarily performed in the context of a single transaction due to the isolation of each cryptocurrency network domain. Each particular cryptocurrency network in an exchange requires the transaction to be broadcast to it, and the transaction finality verified in order to implement each side of the swap. We demonstrate that it is possible to provide a form of trustless, bond-secured cross-network swap between two completely different cryptocurrencies –a 'Chainbond Protected Swap' or "CPS". CPS is implemented using two key features of kNET; Hierarchical Masternode Quorums[9] and Chainbonding[28], an automated method allowing for forfeitable bonding to provide on-chain protection for all counterparties to an exchange.

Multiple-Cryptocurrency Network Support

A focus for the kNET economic network is initially providing protected swap support for established and high-liquidity cryptocurrencies with a stable public network and high hash-rate, specifically, Bitcoin, Ethereum, Bitcoin Cash, Dash, Litecoin. The reason to restrict protected swaps to the major cryptocurrencies at this time is that less established cryptocurrencies present an unacceptable risk to a masternode's bond when that masternode participates in a Chainbond Protected Swap.

CPS Superquorum and Subquorum

Following the kNET Apex network growing to a sufficient number of Masterlans, Superlans, Masterminers and their corresponding collateral, functionality to allow for the formation of Hierarchical

---

[26] Masterlan Superquorums may form a Subquorum under them which provides audit, bond custody and oracle services such as is needed in cross-chain (off-chain) transaction assurance, for actions performed by those Subquorums

[27] Two-party exchange between cryptocurrency assets across separate cryptocurrency networks – for example, between Bitcoin and Dash, or Ethereum and Litecoin currency pairs.

[28] Chainbonding is the on-chain bond holding by a Superquorum of an amount of collateral that a Masterlan masternode (which forms part of a Subquorum) commits for the purpose of providing protection and assurance to counterparties.

Masternode Quorums[9] will be introduced (described in detail above). These enable the trustless Chainbond Protected Swap exchange features of kNET.

The parent quorum of HMQs is known as a 'Superquorum' and it consists of a relatively large plurality of Masterlan masternodes (>60) used to secure multiple transactions across a timeframe of several days. The Superquorum can be considered a plurality of independent oracles used primarily to make externally observed 'Determinations' that verify that desired off-network actions and outcomes related to a specific exchange of assets on the third-party cryptocurrency network meets a set of expected business rules for the progression and finalization of an exchange or transaction. Within cryptocurrency networks outside of kNET, this means that transactions should appear on their corresponding ledgers and be confirmed to an appropriate level of finality[29]. The Superquorum is able to form, on an as-needed basis, a separate but smaller 'Subquorum' from a plurality of Masterlan masternodes in which its members will be responsible for processing transactions within the context of a protected swap between kNET and any third-party cryptocurrency networks.

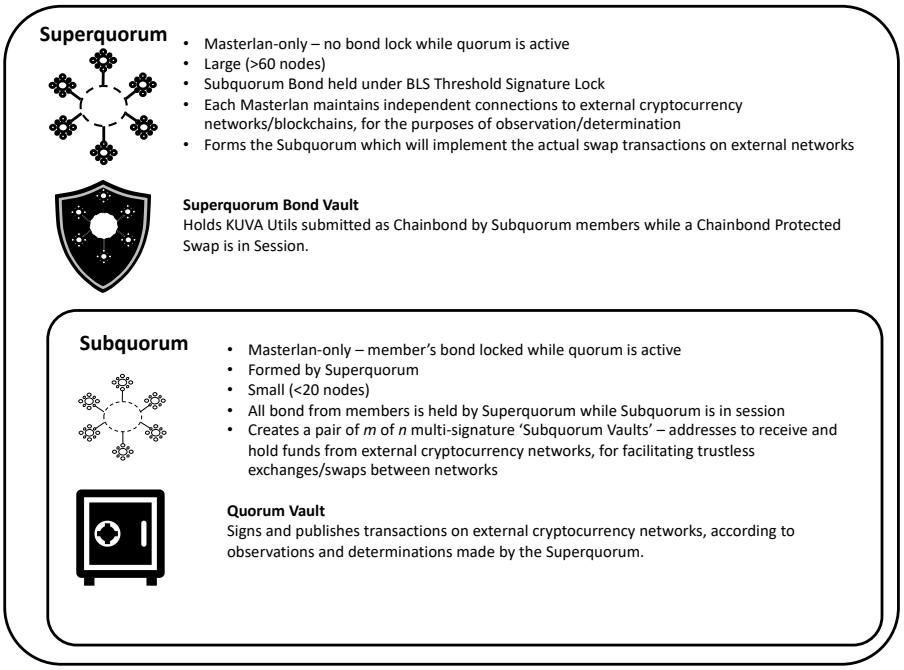

Figure 12 Hierarchical Masternode Quorums - Superquorum and Subquorum summary

[29] For example, the industry standard is 6 confirmations for Bitcoin blockchain, zero-confirmations to 30 confirmations for Dash blockchain with Instantsend, 30 confirmations for Ethereum.

CPS Quorum Sessions

A plurality of long-lasting Superquorums is maintained by the network, which are used to instantiate Subquorums and perform assurance and protection functions (external observation, determination and compensation disbursement) for the smaller-sized Subquorum and the functions it provides for users. A deterministic list of Superquorums is maintained on the kNET network to provide for CPS and other forms of transactions requiring trustless on-chain vaults, audit processes, business rule execution and assurance/protection.

A Subquorum is put in 'Session' by the Superquorum through the locking of the bond collateral of all the Subquorum members' masternodes. This is performed through the Superquorum creating a 'Bond Vault' address using a BLS Threshold Signature scheme; the Superquorum Masterlan members generate a P2SH-style address for receiving payment of the bond by each Subquorum member, called a Chainbond. These Chainbond Transactions are sent by the Subquorum members to their Superquorum's Bond Vault and persisted to the kNET blockchain. The Superquorum may, if the correct determination is made, build and sign a threshold-signature transaction to send the Chainbond it holds in the Bond Vault to the swap counterparties in accordance with any compensation determined by the CPS business rules. This is the 'Protected' aspect of the transaction[30]. Until the counterparty settlement transactions have been completed and the Quorum Session has closed successfully, the Chainbond is held by the Superquorum at the Bond Vault address.

The Subquorum which will be processing and signing external transactions is a group of Masterlan masternodes (these have bonding collateral associated with them). Only Masterlan masternodes can be used as Subquorum Processors, as they must hold the minimum required bond reserve which is associated with their registration as a Masterlan. If unspent bond reserve is not present, the Masterlan is deemed invalid, and is deregistered from its corresponding deterministic list, and therefore it would never be selected to take part in a Subquorum or Superquorum. Each Masterlan in a Subquorum is mutually responsible for processing and signing its corresponding signature for multi-signature transactions off-chain from kNET, and therefore each Masterlan masternode will need to generate and maintain signing keys for the third-party chain individually. A single Masterlan can only participate in as many Subquorums simultaneously as it can commit the required Chainbond balance for.

[30]The bond itself may actually be held in other forms of asset other than KUVA Utils, but the default is to maintain bonding with KUVA Utils as the native cryptocurrency of kNET. If it becomes necessary, multiple bond types can be introduced as an enhancement to CPS functionality.

Quorum Observations and Determinations

Masternodes in their respective Superquorums and Subquorums must maintain a connection to a plurality of nodes on any external blockchains/networks into which they would facilitate the Chainbond Protected Swap (preferentially, to run their own copy of that cryptocurrency's reference software as an equivalent of a synchronized 'full node'). This is because an authoritative view of the state of a relevant external cryptocurrency network is required for each Masterlan in a Quorum Session such that any contentions, attempted double-spends, blockchain reorganizations, forks and the like are observed, and the confirmation status of any transaction is known. Every masternode in a Quorum Session can be considered an oracle that must obtain an 'observation' of the consensus on that external blockchain that is as accurate as possible, enabling the masternodes to act in concert within a quorum and form a 'determination' as to the state of that external blockchain, in relation to the progress and finality of any transactions related to a Chainbond Protected Swap (and any compensatory payment of bond held to each counterparty should either of the corresponding transactions fail).

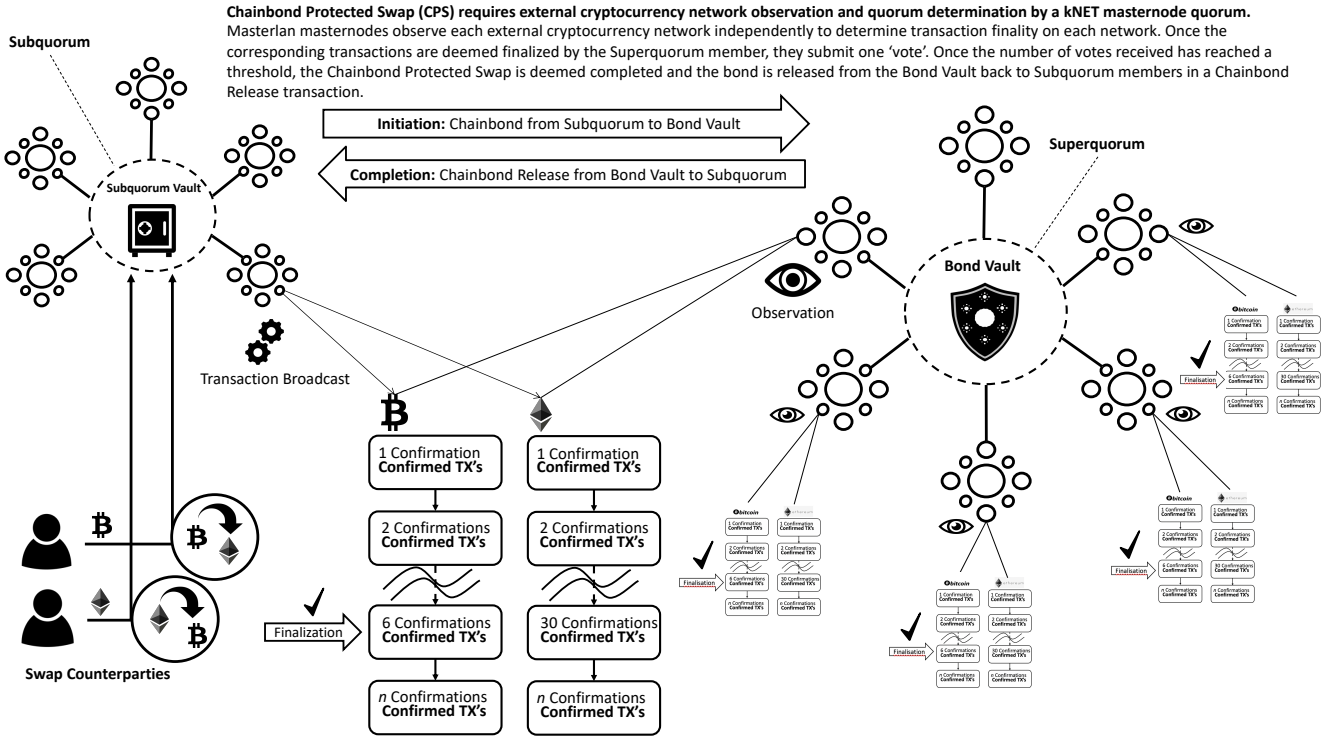

Figure 13 Chainbond Protected Swap overview - Bond Vault, Quorum Vault and Observations

Superquorum Counterparty Compensation

Throughout the process of an exchange of cryptocurrencies or digital assets external to kNET, the Superquorum acts as both bond holder and swap auditor, with the ability to enforce the business rules of a Chainbond Protected Swap transaction and recompense counterparties for transactions that have breached the formal terms of the swap. If the Superquorum, makes a determination of a loss to any counterparty in a Chainbond Protected Swap it can send a compensatory amount of the Chainbonded KUVA Utils to affected parties directly from the Bond Vault. When this happens, the corresponding amount of a Subquorum's Masterlan's bond is considered forfeited. Thus, Subquorum members are disincentivized to collude and defraud the counterparties.

Subquorum Escrow Processing

The Subquorum can be seen to act as a bonded escrow agent and transaction processor for users involved in a swap. The Subquorum is able to deploy a multi-signature address on an external cryptocurrency network under the joint control of its members (with one key held per Subquorum member). As a whole, the Subquorum can be considered an autonomous agent which may receive funds securely, and it may also sign to send funds to a corresponding address if a quorum determination to do so is made by the Superquorum. Once the corresponding m of n addresses are signed for by the threshold number of members of the Subquorum for the intended transaction on each network, the transactions are broadcast to each respective cryptocurrency network. Following the Subquorum publishing the transaction to the corresponding networks, each Masterlan member of the Superquorum observes both external cryptocurrency networks involved in the swap and waits for the expected confirmations/finalizations of the transactions on those networks before it releases the Chainbond back to the respective Subquorum members. When the Superquorum has determined that the transactions to the counterparties have been made by the Subquorum and these have confirmed (according to the business rules governing the determination), the Subquorum Session is closed by the Superquorum and a Chainbond Release Transaction (CRT) is published to the network which pays back the bond. Once this CRT transaction has confirmed into a block, the bond may be spent by the Masterlan owners again or be used as bonding for a further CPS transaction.

Consolidated Cross-Chain Trading

Through the use of Hierarchical Masternode Quorums, it is possible to implement an arbitrary level of security and bonding for any cross-network transactions that are able to be independently observed by each Quorum Session member via their own infrastructure. Each observing masternode in a quorum can be thought of as responsible for one logical 'bit' of assurance in the quorum determination related

to a transaction. This process allows for autonomous and trustless cross-network swaps to be realized through kNET.

Postfunded Chainbond Protected Swap Example

The following example describes how such a trustless, escrow-like exchange would be enabled on kNET, including the validation of transactions on each independent blockchain (Ethereum and Bitcoin) prior to the successful closure of the swap. Specifically, we demonstrate a post-funded, two-sided CPS between two counterparties wishing to exchange corresponding amounts of Bitcoin and Ethereum cryptocurrencies[31].

In this specific example, both counterparties will be fully escrowed via kNET CPS. It is also possible to have a one-sided escrow where one counterparty will send funds through kNET CPS, and the second party will observe the confirmation of those funds into the Quorum Vault. In this case, the second party sends the corresponding funds to the swap directly to the external blockchain without committing them through the CPS process. Both processes allow for the protection of each counterparty, but the two-sided process allows for more complete automation and full enforcement of the terms of the swap.

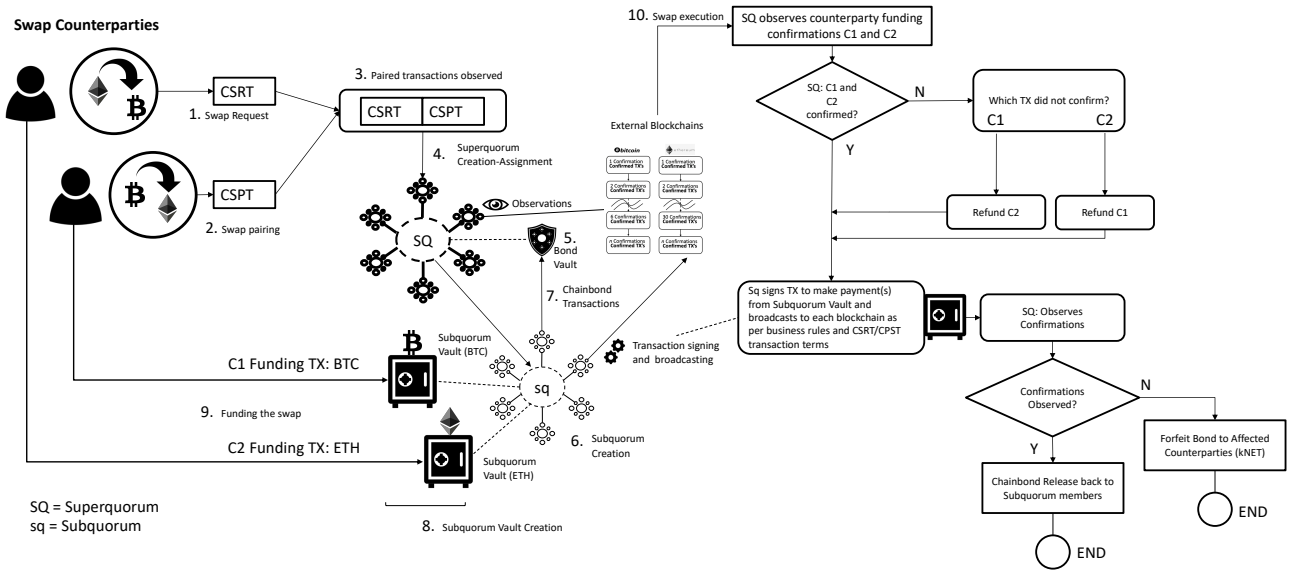

Figure 14 Chainbond Protected Swap example

[31] A Chainbond Protected Swap could also be made between Bitcoin and Litecoin, Bitcoin Cash and KUVA using the same method.

Swap Request Transaction

To initiate an exchange between two supported cryptocurrencies, a special form of transaction called a Chainbonded Swap Request Transaction (CSRT) (1) is generated and published to kNET by an initiating party (Alice). Within this transaction, Alice specifies the two external cryptocurrencies she is looking to respectively buy and sell (in this case, sell ETH and buy BTC), together with the amount (of either one) and the exchange rate is calculated as is a proposed transaction fee for each external network. These transaction fees will need prefunding within the transaction or will be applied from the principal amounts transacted by each party (by the Subquorum). Alice also specifies her receiving BTC address for the exchanged cryptocurrency and, optionally, the receiving ETH address provided by the counterparty to this particular exchange (Bob). Doing this serves to lock the CSRT such that it is useful between Alice and Bob only. If Alice doesn't specify the BTC receiving address of the counterparty, then it would be possible for anyone to observe and accept the exchange (this would describe the extension of this concept into a distributed exchange or 'DEX' using a prefunded swap).

Swap Pairing Transaction

The Chainbonded Swap is initiated when the CSRT is broadcast to kNET, containing the specific receiving address for the counterparty (Bob)- (this includes a small KUVA fee to be burned in the broadcast transaction). Meanwhile, Bob monitors for the transaction and checks to ensure the CSRT is correct and valid for the desired exchange. If he is satisfied with all the parameters of the exchange, Bob then assembles and broadcasts a Chainbonded Swap Pairing Transaction (CSPT) to kNET (2). The CSPT references the transaction ID hash of Alice's CSRT, and it is then signed by Bob's private key corresponding to Bob's receiving address, which Alice included in the CSRT. At this stage, when the corresponding CSRT/CSPT pair are seen in the transaction pool (3), two Masternode Quorums are automatically formed, the Superquorum first (4), which then initiates a Subquorum Session (6) for the purposes of completing the transaction.

Subquorum Session Vault construction

At the initiation of a Subquorum by a Superquorum, a BLS threshold signature wallet address is constructed by the Superquorum for the purpose of holding KUVA Utils in a Chainbond – this is called the Bond Vault (5). All Masterlan members of the Subquorum must send a specific amount of KUVA Utils as bond to the Superquorum's Bond Vault. The bond transactions are broadcast to the network by the Subquorum Masterlans (7) and confirm on the kNET blockchain. The Superquorum holds the Chainbond until such time as the CPS is completed. The Superquorum will then publish a Chainbond Release transaction refunding the bond from the Bond Vault to the Subquorum members. Alternatively,

according to Superquorum determinations which may calculate any compensation owed to counterparties, the Superquorum may also allocate/forfeit an amount of the Chainbond to one or both counterparties.

Once Subquorum members have posted their Chainbonds and the Subquorum is deemed active, a Quorum Vault will be subsequently constructed by the Subquorum. In this process, each Masterlan generates two separate public/private key pairs that they will use to construct the Subquorum's multi-signature Quorum Vault (8) addresses for each of the cryptocurrency networks used in a swap – in this case a BTC address and an Ethereum account. To ensure that a valid Session Vault is constructed, and to restrict the ability of one or more Subquorum members generating a script hash with a single rogue public key, the Superquorum and Subquorum both independently assemble the corresponding spend script from the Subquorum members transmitted public keys. The resulting spend script and associated script hash is transmitted to the Subquorum nodes with multiple redundancy (Superquorum nodes will be transmitting the transaction to multiple Subquorum nodes such that the members of the Subquorum can have additional assurance that they have received the correct spend script and corresponding script hash). Each Subquorum member now checks that they have all received the same corresponding script hash in the communication from the Superquorum, and if so, they broadcast a Subquorum Session Vault Active transaction to the network, including the Quorum Vault payment address. Once the Session Vault Active transaction is confirmed on the blockchain, Both Alice and Bob have a window of time to pay their corresponding contributions for the exchange (for post-funding transactions, the funding transactions should be broadcast immediately, so that they will confirm within an hour). The Superquorum observes the third party blockchains/cryptocurrency networks for Alice and Bob's funding transactions (9), allowing it to make a Determination under their CPS funding confirmation business rules for each of the counterparty networks (10).

CPS Business Rule Monitoring

There is a time window allowed for each of Alice or Bob's valid transactions to be seen in the mempool that fund their respective exchange transactions. If the transactions do not appear in the mempool (as unconfirmed transactions on each corresponding network) within the time period specified in the original CSRT, the transaction is deemed 'Voided.' Subsequently, after a 'safety period', the Chainbond from all Subquorum members will be refunded by the Superquorum, after which the Subquorum session is closed. It is therefore important for Alice and Bob to be ready to transmit funds as soon as the Subquorum Session Quorum Vault is created and its address that is ready to receive counterparty funds is confirmed on the kNET blockchain.

Native Multisignature Chainbond Protected Swap

Native m of n multi-signature[32] is used where single aggregate threshold signatures, for example BLS threshold signatures, cannot be used within the native unlocking script used in an escrow transaction[15]. For example, in Bitcoin's P2SH redeem script it is necessary to use Bitcoin's natively supported ECDSA-based scripted multisignature capability. This checks signatures in a serial manner within the script but has the disadvantage of having a larger transaction size and therefore higher network fees that must be paid on the external chain. For security and key redundancy, it is preferable to require a higher number of signatures for the escrow transaction. Setting the threshold to m=7 for n=15 allows enough redundancy for 8 Masterlans to go offline in the Session and for the transaction to proceed as normal, and this would be valid under current a Bitcoin Core-based node's 'standardness' rules (as the most common node software in use at the time of writing[33]).

Notes on Standardness Rules on External Networks/Blockchains

In the above example of a Postfunded CPS transaction, as the Bitcoin protocol using P2SH only supports m of n multisignatures of up to n=15[34] (because of current popular (i.e. Bitcoin Core) client software restrictions and enforcements known as 'standardness rules'[35]), as well as size restrictions on the length of the script within a transaction intended to be broadcast, m>7 n=15 can safely be used in the Subquorum. For earlier clients (Bitcoin <0.9.2) using more than n=3 signatures in practice for a multisignature address[36] would result in client nodes rejecting and not relaying the transaction. These 'standardness' rules and their development on respective cryptocurrency networks and blockchains would need to be monitored carefully to avoid the Quorum Vault locking funds with a valid, but non-standard and practically unspendable script.

Preimage Attacks and Collision Resistance for Native Multisignature Generation

An important consideration in securing a native multisignature Quorum Vault is the potential for a P2SH Multisignature preimage attack to be used by a malicious Masterlan, when forming the Quorum Vault, using a birthday attack. This lowers the effective overall security on the multisignature address to half of the effective bit-length (the search space for a 50% chance of collision goes from 2^{160} to 2^{80}) in the situation where prior to the submission of their public key, and following their collection/knowledge of

[32] OP_CHECKMULTISIG - https://bitcoin.org/en/developer-reference#opcodes

[33] https://coin.dance/nodes

[34] Supported in IsStandard() Script via P2SH as ECDSA multisig - https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch05.html

[36] For redundancy reasons, it is necessary to have two Masterlan's in a Subquorum per key in an m of n signing session, since it is not desirable to have a single masternode failing; the loss of one of the keys would result in the loss of Subquorum-escrowed funds and corresponding bond reallocation by the Superquorum. Wherever possible Subquorums will be employed with broader key distribution and a lower m of n ratio.

all other public keys submitted by other Subquorum member, a malicious party attempts to construct a script containing their own public key for which the script hash is equivalent to the hash of the fully constructed multisignature script. A 'presubmit and reveal' process between all Subquorum members for all public keys used in the construction is the simplest method that would bring the security back to nominal levels (where the preimage resistance is back to 2^{160}).

Mempool Size and Transaction Delays

Monitoring of the size of the mempool[37] in each blockchain and disallowing swaps to be made in the case of very large transaction backlogs is important, as is ensuring that corresponding minimum required network fees for external transactions are adequate such that the transaction will be picked up by miners for confirmation/inclusion in a block. Delays to confirmation may result in a determination of a counterparty default, even though valid transactions might still reside on the corresponding mempool because of a backlog. Should there be delays in confirmation for any valid transaction, there will be business rules set in place to delay any compensation payment or refund triggers.

CPS Business Rules

Those skilled in the art can observe that further business rules for optimization, various edge-cases and compensation strategies may need to be further developed for other forms of CPS use cases. We note here the need for a voting process to ratify these business rules and that protocol changes or external factors may require adjustment to these rules, including permitted reference node software, authoritative chain, fee sources and fee determination algorithms, mempool levels and per-network 'standardness' rules. To begin with and in order to manage for the production hardening and security of CSP processes, only transactions which are limited in value will be allowed to use CPS functionality. All swaps will be privately monitored by the founding organization (Kuva Global Trust, through the Kuvacash wallet[38]) alongside the Masterlan-based CPS process, until such time as the full set of business rules required to implement fully automated CPS is deemed sufficient for public operation. In the meantime, the Kuva Trust will make any exception determinations and manually execute any outcomes (compensations and refunds).

Notes on Prefunded CPS Transactions

A prefunded CSRT is one where cross-chain funds are committed to and controlled by the Subquorum, the CSRT containing fulfilment and settlement rules as in a Postfunded CPS. The difference is that a

---

[37] https://www.blockchain.com/btc/unconfirmed-transactions

[38] See the Kuva Business Positioning Whitepaper for details on the founding service provider and maintainers of the kNET Apex network.

Prefunded CPS transaction is akin to a placement of an order in an order book of an exchange. A prefunded Swap Pairing Transaction can be created in response to a prefunded CSRT which settles immediately on-chain, and then at a later time when counterparties have completed their trading, balances can be resolved on external chains. This would provide traditional real-time distributed cross-chain exchange functionality. Although this concept would benefit from further exploration, it is clear that at the very least, through pre-funded CPS transactions and the maintenance of an order-book structure and quorum-based order-matching on the kNET network, it is possible to implement a form of pre-funded real-time exchange using Chainbond protection. DEX functionality is out of the current scope of this whitepaper but may be a useful feature development within kNET in the future.

Post/Pre-funded CPS Transactions

The post-funded process described allows two parties who do not have to trust each other, but wish to exchange assets between separate supported blockchains, to do so under an automated and trustless Chainbonded escrow process. Although either party may default in sending their corresponding transactions, the process ensures each party is either refunded on their corresponding blockchain and the refund validated by the Superquorum (ex-fees). Alternatively, if the corresponding transaction cannot be refunded directly to the external blockchain for any reason, either party may be compensated via forfeit of the locked Chainbond amount from the Subquorum Bond Vault.

The Block Budget

The total amount of Kuva Utils created as block rewards by Masterminers while kNET operates is known as the 'Block Budget' and is intended to provide payments for collateralized service providers on the kNET network, as well as allow for a component of Strategy financing (the other component being the Governance Treasury). The Block Budget is shared between the Strategy Owner and active stakeholder providers on the network, effectively a split between the Governance, Masternode owners and the Licensed Service Providers. The Strategy is responsible for proposing the split of the ratios which are variable within the Block Budget. The Strategy Owner or group, in their active Strategic Governance Proposal, must therefore carefully consider the balance of rewards paid to all the stakeholders on the network, or risk losing to another Strategy if the voting stakeholders do not consider the split to be fair and vote out the Strategy in favor of an alternate one.

kNET Script Modules

kNET, like Bitcoin, uses a Forth-like stack-based scripting language which is not 'Turing-complete', but extends functionality of its opcodes with extensible 'Script Modules'. It is easier to limit and test a stack-based script and its underlying opcode functions than allowing for Turing-complete scripting.

Script Module extensions which include new opcodes are activated through the kDAO Strategic Governance voting process. If voted in, Script Modules must be supported by all nodes and miners - a Proof of Service penalty will result for non-compliant service providers rejecting transactions with active Script Modules. Script Modules can only be turned on (enforced) and off (inhibited) through the use of the Governance Keys and Switches that are assigned to the current Strategic Governance Owner. These are for the purpose of safely staging Script Modules on the network and having the ability to activate or disable them in case of any issues that may emerge. For example, if an active Strategic Governance Proposal, against the desires of a majority of voters, disables a Script Module (which could cause certain transactions to fail and/or unspent funds with a script which uses the Script Module to become unspendable), then that SGP is likely to be voted out in favor of one where the Proposal Owner enforces the activation of the Script Module.

In the future, Script Modules will allow for further functionality, including off-network threshold signatures, hierarchical signatures, common forms of smart contracts and other schemes which may be needed as the use of the network increases and new use cases arise.

KUVA Util Supply

The total amount of KUVA tokens that can ever be in active circulation, which is the total number of KUVA residing in unspent transaction outputs at any time, is 1.2 Billion KUVA. The circulation is capped to this amount through kNET's 'Burnmine Cycle'. In kNET, network fees are burned when services are used and transactions completed, rather than fully committed to miners as rewards. KUVA is correspondingly regenerated and distributed in the block reward as per the current active Strategic Governance Budget Ratio and the Generation Curve.

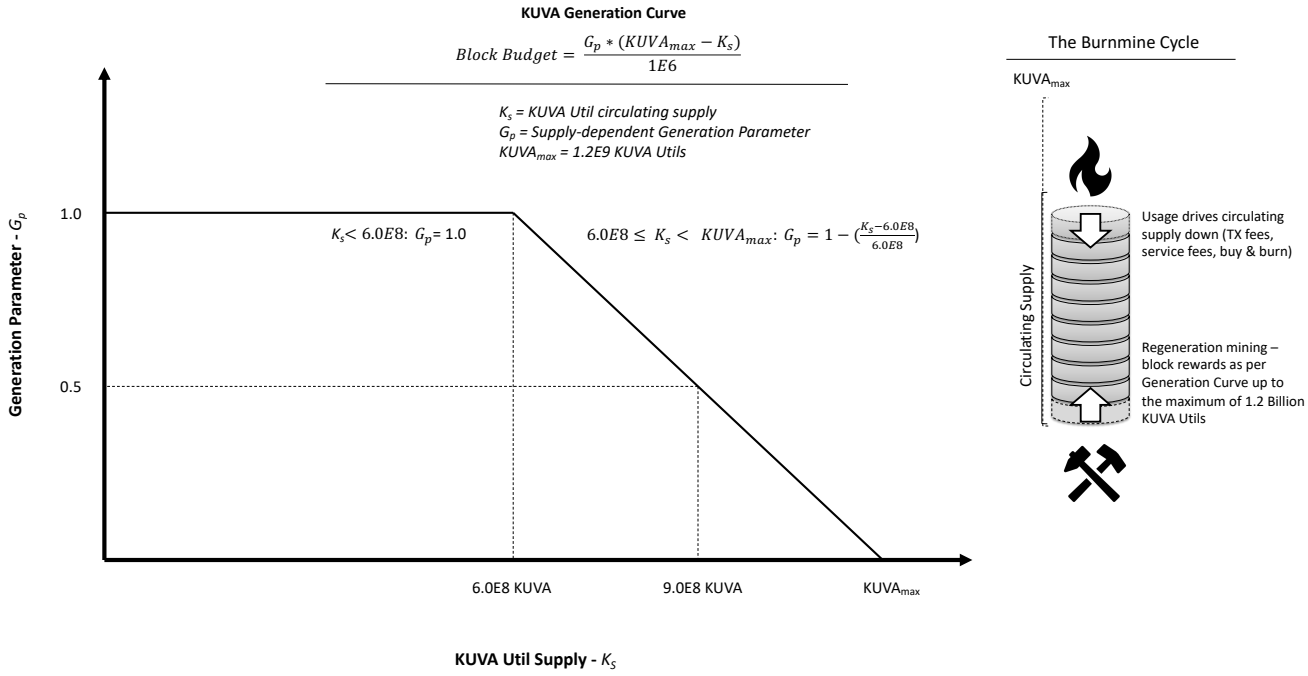

Figure 15 Kuva Generation Curve and Burnmine Cycle descriptions

The block reward payment ratios are set and rewards distributed between all network participants according to the current Budget Ratios within an active Strategic Governance Proposal. This includes the amount set aside for the collateralized miners themselves (Masterminers) Strategic Governance Budget, Masternode lists and the Licensed Service Provider lists.

The issuance at launch of half of kNET's minable supply (600M KUVA Utils) is strictly for the purpose of expanding the financial service offerings and customer base of the founding service provider businesses (Kuvacash Wallet), while collateralizing the Apex network. This, along with the public bootstrapping - 'bottom-up' - deployment of the Apex network following the limited KUVA Util sale is the necessary - 'top-down' - strategic approach to ensure the network is developed in line with viable founding businesses which uses kNET infrastructure. This two-pronged approach to establish the Kuva network is discussed in further detail within the Kuva Business Positioning Whitepaper.

Launch and Initialization for Public Launch of kNET

kNET's initial infrastructure has been developed and is managed by Sky Vault LLC, a Nevis company. kNET's founding Apex network infrastructure will be expanded through a series of sales of KUVA Util tokens by the Kuva Coin Trust, whose mission it is to facilitate further promotion and expansion of

kNET via grants. At the first stage there is a private network which hosts publicly collateralized nodes and forms a launch infrastructure that supports the initial founding 'client' or service provider businesses. At an appropriate time, when the Apex network has reached a critical size allowing for a staged and secure transition to public infrastructure, kNET will become open to public infrastructure operators, allowing the public to collateralize and operate Masterminer and masternode software directly on the network. At or before that stage, this kNET infrastructure software will also be released as open source.

The initial 'client' or commercial proposition using the kNET infrastructure during its private phase is Kuvacash, a fintech platform, wallet application and financial services developed and launched by The Kuva Global Trust. The Kuvacash wallet is operating with connectivity to kNET in pilot stage at the time of this Whitepaper publication. The issuance of the first KUVA Utils (600 million) will enable expansion of the infrastructure network to support this initial client and reach the critical staging and growth marks that will allow the network to go public.

Prior to transition to a public network, during the Apex network's staging and growth phase, purchasers of KUVA may still collateralize, initialize and activate masternodes on the network. A simple-to-use interface to manage Kuva masternodes is available on the Kuvacash wallet and will pay masternode rewards to users who hold KUVA Utils and have activated their masternodes.

kNET's founding Apex network infrastructure is developed through a series of sales of KUVA Util tokens. This is a private network which hosts publicly collateralized nodes and forms a launch infrastructure on which the initial founding service provider businesses may be implemented[2]. At an appropriate time, when the Apex network has reached a critical size allowing for a staged and secure transition to public infrastructure, kNET will become open to public infrastructure operators, allowing the public to collateralize and operate Masterminer and masternode software directly on the network. At or before that stage, this kNET infrastructure software will also be released as open source.

kSeries – a Founding Stablecoin Series for kNET

At the launch of kNET, a stablecoin series called kSeries is established with Short kTokens and managed by the Kuva Global Trust. At launch, USD and GBP are supported fully. The kSeries will grow to include 35+ reserve-backed tokens representing fiat currencies to be used for on and off-ramp fiat to cryptocurrency transactions with fiat fund backing reserves held by the Kuva Global Trust's operational companies. The kSeries stablecoins are used to enable fiat-value transactions and currency exchange across the network. Maintaining a full stablecoin series via kSeries ensures that the backing fiat liquidity reserves can be net settled across the network instantly and efficiently and at low cost to

the end user, providing for immediate payment provisioning and settlement for all licensed service providers.

Foundational Funding

Premine

kNET is the native minable currency, created through a 'Burnmine Cycle[51]'. The network will be initialized with the premine of 600 million KUVA. This sets the initial mineable supply to the midpoint of 50% of total maximum available KUVA (1.2 Billion KUVA). From the premine, a 6% distribution of KUVA for the purpose of bootstrapping the kNET Apex network will be airdropped to the initial financial contributors of Kuva who provided $1 M USD of the total $2.25 M USD raised for funding of the software and business relationships to be built up to the point of launch. This includes private contributors, who will each be allocated air-dropped KUVA from the 6% total, pro-rated to their contributions. In addition to this, 7.25% is provisioned for retaining incentives for key Kuva staff. In total, this is 13.25% of the maximum available cap of KUVA. This amount includes all foundational contribution air-drops up to the point of the presale.

Presale

The Apex presale of 100 million KUVA, or 8.33% of the maximum available cap of KUVA, is offered over a web-based and mobile pre-sale (https://buy.kuva.com and Android mobile application) for purchase by organizations and individuals looking to provision services for profit and/or assisting in the bootstrapping of the kNET Apex network infrastructure through the running of masternodes.

21.58% of total issuance will therefore be pre-allocated at launch, with 28.42% remaining in the Kuva Coin Trust and 50% of the maximum available cap is the minable supply.

The KUVA held by the Kuva Coin Trust is for collateralization of both network and external service providers. The entire premine distribution will gradually be provisioned to the public as kNET grows, with a focus on collateralizing service providers and expanding kNET. The KUVA held in trust will be distributed over the course of the next 5-10 years to promote and support expansion of the network, and the remainder mined continually in the Burnmine cycle. There is a maximum total supply cap, in that there will never be more than 1.2 Billion KUVA at unspent transaction outputs (UXTO's) in total circulation.

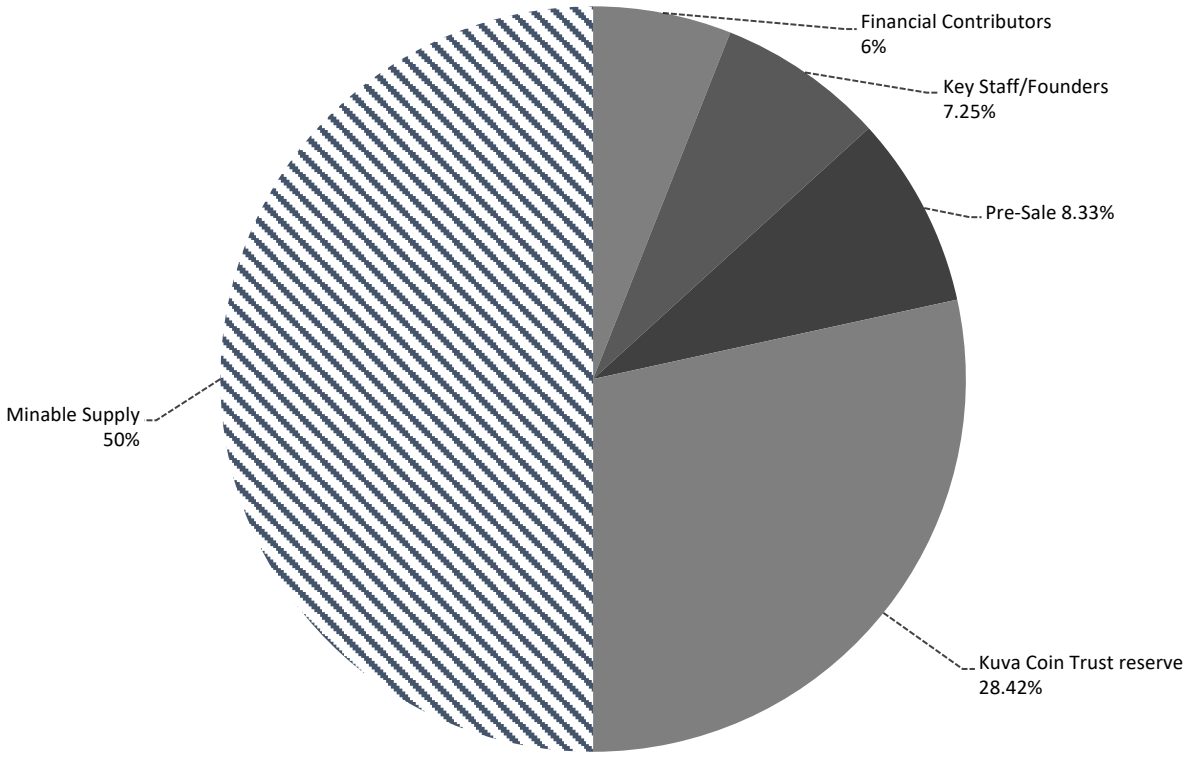

Figure 16 Post Pre-Sale KUVA Util distribution and minable allocation at Apex network inception

Public Collateralization of the Apex Network

At the founding of the Apex network, Sky Vault LLC in Nevis will provision all Masterlan and Superlan masternode infrastructure as well as Masterminers on the network. This network will be collateralized with KUVA Utils sold to and committed by the public. Users will be able to collateralize and activate masternodes on kNET to help build the network to a critical size prior to its opening to public operation.

User-friendly Masternode Activation

For inception and development of the founding Apex network, the Kuva Coin Trust will release enough KUVA Util tokens for sale to enable the public to collateralize and activate a minimum target of 1000 Apex masternodes (Superlan and Masterlan). The functionality for users to participate on the Apex will be available immediately when KUVA tokens are released for sale, via the Kuvacash wallet[39]. Users that hold the required amount of Kuva Utils and wish to run a masternode on kNET's Apex network can use the Kuvacash wallet to generate a collateral transaction (proving that they own or control a specified

[39] https://play.google.com/store/apps/details?id=com.kuvacash.kuva

amount of Kuva Utils) and can directly activate a masternode on kNET Apex, monitor its operation and receive a regular payment for participating in the provisioning and scaling the Apex network prior to public transitioning. More information about this is available on the Kuva Business Positioning Whitepaper.

Notes on Sharding and Pruning

The design and implementation of kNET must ensure longevity of the network, which includes ensuring the most efficient use its network, processing and storage resources. Presently in all major blockchains, storage of the entire blockchain itself is required for each full node or masternode, which the authors believe is over-redundant, inefficient and has a negative impact on network performance. As an example, a network with 10,000 Full Nodes and 5000 Masternodes corresponds to 15,000 copies of the entire blockchain. This may mean that in future public operators may find it prohibitively expensive to contribute infrastructure to the network, since to operate a Full Node or Masternode, they must store all transactions since the inception of the network.

Alternatively, if an effective number of copies of the blockchain is maintained across the entirety of the network in a distributed way – e.g., a maximum of 3000 copies - between the 15,000 Full Nodes and Masternodes using a distributed storage method and protocol such as IPFS[40], the network will be able to store more transactions overall for the available resources while maintaining an adequate level of data redundancy. This approach, also being taken or considered by several other cryptocurrency projects (e.g. Ethereum), will also make it feasible for public operators to provide arbitrary levels of data storage and network resources in order to run the equivalent of a Full Node.

Work is ongoing to select a method for pruning, compressing and sharding the kNET blockchain storage which will provide for appropriate level of storage redundancy, security and performance. This is an additional reason the kNET Apex network is initially maintained by Sky Vault LLC; if determined to be essential, the network infrastructure will be migrated to a sharded model prior to release of the network and associated software to the public, or a migration path will be created to allow for this eventuality. Discussion or design of the pruning/compression/sharding methods for kNET are ongoing and outside of the scope of this whitepaper.

[40] https://en.wikipedia.org/wiki/InterPlanetary_File_System

Summary and Conclusion

The Kuva Network, or kNET described in this paper is a dynamically decentralized economic and monetary network, operating as a Distributed Autonomous Entity (DAE).

kNET is a customizable multi-token/multi-coin blockchain with a two-tier network structure, a non-infrastructure end-user services layer and a single mineable native currency called the KUVA Util that collateralizes network operations as well as external service providers and is used for bonding and in which all network-related fees are paid.

The network is designed to optimize its strategic governance over time towards maintaining the high objective satisfaction of its end-users.

kNET is initially founded securely under private infrastructure, called the kNET 'Apex', followed by a staged migration to full public/community operation under an open source model. A founding business – the initial client -- (Kuvacash) uses kNET to deliver a mobile wallet and set of financial services to its users.

A performance-based democratically voted on-network 'Strategic Governance' is given a governance budget for writing and maintaining kNET software and provisioning various operations aspects including marketing and advocacy, strategic business development, integration support and partnerships, sets reward distributions for all network stakeholders and can also activate or deactivate various aspects of the network's operation for staging and security reasons.

kNET's utility is expanded through the use of Chainbond Protected Swaps (CPS), which allow for protected, trustless escrow and fully automated clearing of cross-network swaps/exchanges.

kNET allows for third-party businesses (as collateralized Licensed Service Providers) to be established on its infrastructure, and these can accrue reputation through providing quality services to end-uses and gain ongoing influence over the network's Strategic Governance, building value in their business and allowing for their eventual sale on-network as a going concern.

By involving users in the process of rating the services they use on the network in a verifiable way, the protocol aims to balance trusted and trustless aspects of the network, eliminating the need for an enforcement boundary superstructure[41] such as those required by traditional corporate structures that operate within the framework of nation states and international legal structures. Instead, the entity is

[41] Kuva Business Position Whitepaper – the enforcement boundary houses all superstructures required for a system to operate autonomously.

self-contained as a DAE without a need for extra-network enforcement, with the goal of maximizing the satisfaction of end-users intrinsic in its overall operation.