SYSTEM UPGRADE SPECIFICATION

Zen Application Platform: Tiered Node System and Sidechains to Decentralize the Network

March 2018
Pier Stabilini, Robert Viglione, and Alberto Garoffolo

INTRODUCTION

The ZenCash Secure Node system is a unique compensated blockchain network with enhanced client-to-node and node-to-node encryption. The system was designed to rapidly and massively decentralize the blockchain network to provide unparallelled censorship resistance, network capacity, and to lay the infrastructure for a high-performing privacy-oriented platform. Within just three months of operating this system, the network already rivals Bitcoin's in node count. Despite this huge success, it is only a starting point and this next generation system will provide significant upgrades to node tracking and payments and, importantly, lay the groundwork for a comprehensive application platform.

Technological improvements include:

- Creation of a new node class called Super Nodes that have significantly higher ZEN staking (500 ZEN), computation, and storage requirements.
- Migrating logic from off-chain server clusters to sidechains maintained on the new Super Nodes. The multilayer sidechains will also make it possible for ZenCash to support multiple applications such as ZenPub, Zero-delay payments (InstantZen), ZenGrid (computation-as-a-service), and ZenXchange (a decentralized exchange built on our network), to name a few.
- Providing a completely decentralized node tracking system with the node status relayed by its connected peer nodes and all the Secure Node messages being received through the core protocol.

Economic changes include:

- Node operators will receive 20% of block rewards, an increase from 3.5% previously. This will be split such that Secure Node operators will receive 10% and Super Node operators will receive 10%.
- Treasury will receive 10% of block rewards, an increase from 8.5% previously.
- Miners will receive 70% of block rewards, a change from 88% previously.

ZENCASH OVERVIEW

ZenCash is a privacy-oriented blockchain system built on zero-knowledge cryptography and modified Satoshi consensus. The system goes well beyond a traditional cryptocurrency in that it is designed to be a sort of startup nation, or full peer-to-peer economic system for money, media, and messaging.

The project started with its core product, ZenCash, which is a cryptocurrency with selective privacy or transparency. Users choose between fully private address types or those that are pseudonymous like Bitcoin. In addition to transaction privacy, the system then introduced SSL / TLS to the protocol for client-to-node and node-to-node encryption to further protect user data and connections.

Satoshi consensus introduced digital scarcity by preventing double spending and aligning miner incentives to participate honestly in block creation. However, the system did not provide such incentives to other stakeholders, such as full node operators. Our innovation was to reward full node operators directly from block rewards, but then to require these node operators to hold valid certificates, minimum computational capacity, and minimum uptime requirements. This created a higher quality and more reliable node network, but the weakness of the initial system is that all logic is hosted off-chain on server clusters and external databases. The next evolution is to bring all logic on-chain and to automate the entire process.

The Super Node class introduces sidechaining and platform applications. This is a major improvement to the system that moves the project well beyond a simple cryptocurrency.

SECURE NODES

The ZenCash Secure Node system was designed to massively decentralize our network so that the project can be censorship resistant across global jurisdictions. Full node operators who obtained a valid SSL / TLS certificate, held at least a 42 ZEN stake in a transparent address (t-address), and successfully responded to at least 92% of challenges sent to shielded addresses (z-addresses), would split 3.5% of mining rewards. None of these requirements change with this system upgrade, but we do introduce an improvement in node uptime measurements that are based on real network peers connectivity instead of websocket connections.

Current system configuration hosts tracking and payment servers in dedicated off-chain clusters in several regions around the world. This was sufficient for the first version of the system, but migrating all logic on-chain is important for true censorship resistance and network resiliency and to allow a verifiable and auditable set of information used to calculate the reward. This upgrade brings everything within-protocol and makes use of sidechains managed by Super Nodes to track Secure Nodes, queue nodes for payments, and coordinate autonomous distribution of payments with mining nodes.

To summarize, the new Secure Node version will provide many improvements including:

- Implementing all the logic at the protocol level in the core code instead of inside a separate codebase.
- Providing a completely decentralized node tracking system with the node status being relayed by its connected peer nodes and all the Secure Node messages being received through the core protocol.

Most of the Secure Node will remain the same:

- Maintain the entire ZenCash blockchain on the system.
- Provide a valid SSL certificate to the ZenCash Node software to use for communicating with other nodes and wallets.
- Keep at least 42 ZenCash in a t-address for staking.
- Monitor the network messages for challenge messages.
- Respond to challenges with identifying information of the Secure Node.
- 92% daily uptime.

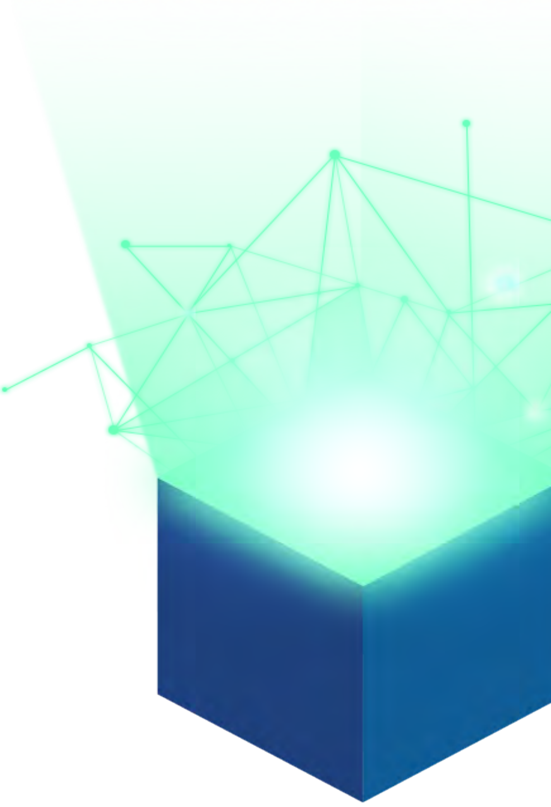
Changes that will be introduced:

- A new challenge mechanism relying on the new version of zk-snark that will require 1.7Gb RAM. This change is being introduced in a precursor software upgrade released to testnet in March 2018 and scheduled for mainnet start of May 2018.
- Uptime calculated on the real network peers connectivity and on blockchain sync.
- Secure Node rewards will increase to 10% of block rewards.

At the protocol level the message handler will support the messages necessary to:

- Broadcast the Secure Node information and status to the network.
- Verify a specific transaction, a set of transactions or a specific block hash to check if the node is in sync.
- Execute a challenge or some other check to verify that node requirements are satisfied.
- All the other information that is necessary is already implemented into the protocol.

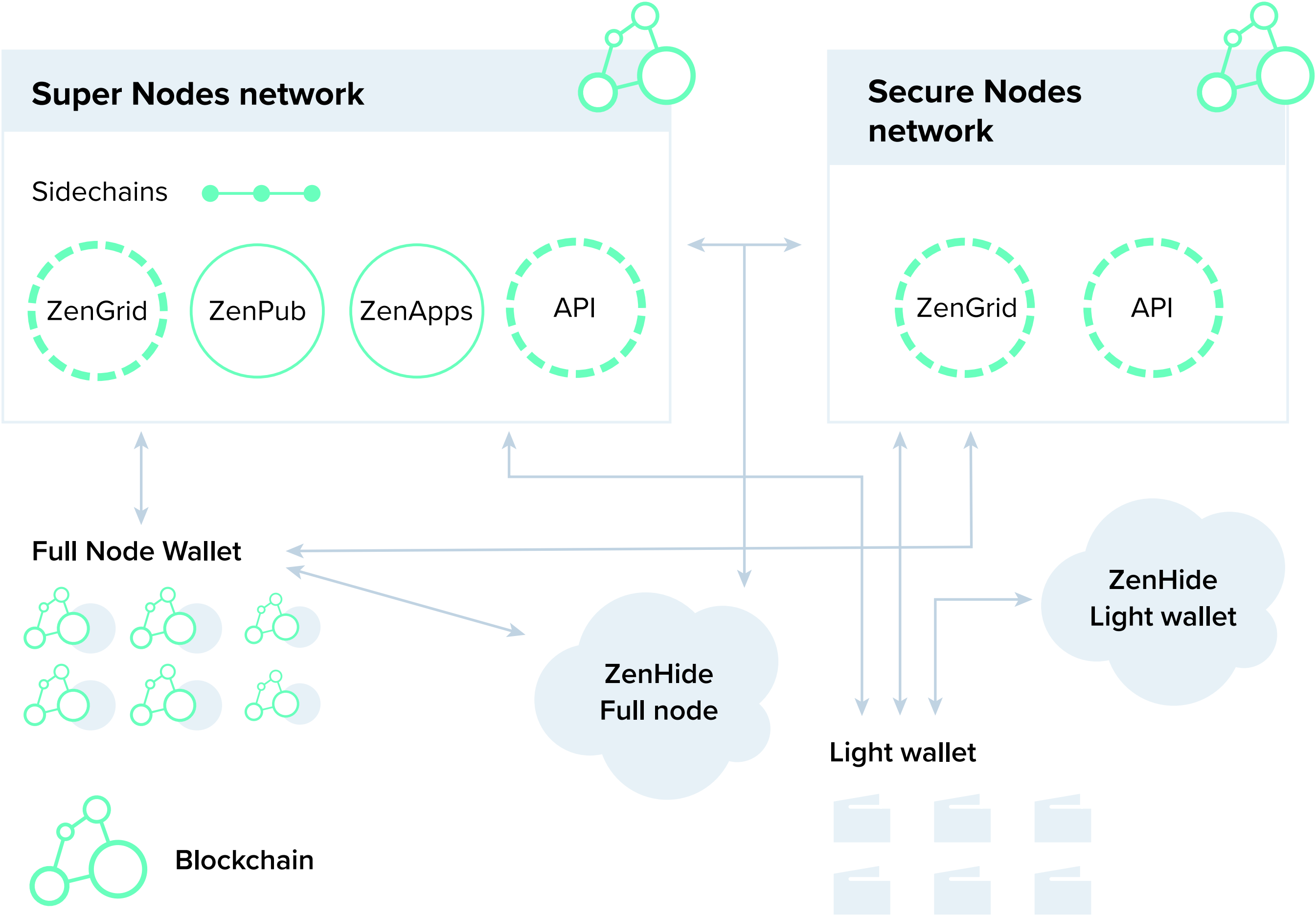
SUPER NODES AND SIDECHAINS



One of the first major differentiating features of our system was launching a compensated node network with enhanced point-to-point encryption, which we called Secure Nodes. The ZenCash network acquired more than 9,000 Secure Nodes, 3x more than expected, within just the first four months of launching this system. These special nodes on the network are composed of sufficiently high quality systems to meet minimum requirements, including possession of a valid SSL certificate, a vast improvement from other blockchains currently in the market. The next phase we introduce here is to create a new class of special nodes with higher requirements that we call Super Nodes. Super Nodes will be more powerful than Secure Nodes and will be tasked with managing key network and system functions such as hosting multiple services on sidechains, tracking and measuring Secure Node uptime, and queuing the node payment schedule for miners.

The two major improvements Super Nodes bring are to transition tracking and payments on-chain, or within protocol, a major change from the current system where such functions are executed on external server clusters; and the introduction of sidechaining elevates the ZenCash system from a pure cryptocurrency to a platform on which an unbounded set of services can be built. The value proposition of the system then becomes more than the utility of the currency, but now includes the utility of all future services that will be layered onto our infrastructure. A small sampling of such services which are already in planning include a distributed file storage system (ZenPub), a secure messaging system (ZenChat), a computation-for-rent system akin to AWS's Lambda Functions (ZenGrid), zero-delay payments (InstantZen), and a decentralized exchange (ZenXchange) with a fully-collateralized price-stable asset called ZenUSD (USDZ).

ZEN NETWORK



NODE PAYMENT MANAGEMENT

The Super Node network will support a multi-layer sidechain. One of the layers will be used to store all the information about the Secure Node status and the Super Node status. The idea is that the Super Node network will keep track of the status of both Secure Nodes and the other Super Nodes in a sidechain. That network will use the consensus to verify and validate all the necessary tracking information.

Such a queuing process could work as follows:

- Every n blocks the Super Nodes will read the sidechain to process nodes that are payable and move them into a queue.
- All Super Nodes should then provide consensus on each element of the queue.
- The mining nodes will pull elements from the queue (a subset) and create the payment for the nodes into a specific coinbase transaction (other than standard coinbase rewards for the miner and for the community), the paid nodes are removed from the queue.
- The paid nodes are removed from the queue and will be re-pushed into the queue from the Super Nodes for the next round of payment.

SIDECHAIN MANAGEMENT AND SYSTEM REQUIREMENTS

The Super Nodes will support multiple layered sidechains, which will form the basis for developing the system as a platform. These will be used for a variety of applications and will be exposed through a common interface to include RPC methods. The first implementation will be used to query the node status from the Insight API. The multilayer sidechains will make it possible for ZenCash to support multiple applications as described in the previous section. Additionally ZenCash will be able to leverage the side chains to integrate third party technologies such as FlowCrypt, a PGP extension for Gmail, to store the entire public key set into the sidechain. It is important to note that the set of applications will initially be constrained to internal development for security reasons, but the future goal is to open the platform to external dApp developers so that anyone can contribute to the ecosystem directly.

This is all a major improvement in system functionality and ecosystem value proposition.
In order to support this functionality, the Super Node requirements will be much higher:

- At least 500 ZEN in a t-address for staking.
- Multiple CPU cores.
- 8GB of RAM or more.
- 100GB of storage or more.
- 96% node uptime per day.

PAYOUTS, ADJUSTMENTS, AND NETWORK TARGETS

A major aspect of the ZenCash ecosystem is that we want maximum decentralization for censorship resistance. We understand that by setting a significantly higher staking requirement--from 42 to 500 ZEN--we run the risk of overly centralizing the Super Node architecture. One way to avoid over centralization is to increase the payout pool to incentivize greater node creation. This is the main motivation behind increasing node operator payouts from 3.5% of mining rewards to a total of 20%, with 10% going to Secure Node operators and a dedicated 10% pool going to Super Node operators.

Segregating the pools should create a joint equilibrium such that the network grows to the point of marginal cost equalling marginal revenue. Super Nodes will have a significantly higher marginal cost and so we expect fewer of them, but the revenue stream will be independent of the Secure Node pool so that the growth of one segment should not unduly cannibalize the state of the other. Our target Super Node and Secure Node counts are between 2,000-2,500 Super Nodes and 20,000-25,000 Secure Nodes, respectively. Major deviations from that target could induce future payout or staking adjustments.

IMPLEMENTATION SCHEDULE

Full implementation of this application system with Super Nodes is expected to be in Q4 of 2018 with a prototype available for testing at the end of Q3. The build-out of the network will start much sooner. Block reward adjustments will be implemented with the next hard fork system upgrade scheduled to be released to testnet mid-April and mainnet end of May.

To encourage the early and smooth expansion of the Super Node network, we propose the following schedule:

- Open Super Node staking system with the next hard fork end of May.
- Prospective Super Node operators register a t-address with at least 500 ZEN.
- Super Node operators will run a modified version of Secure Node software.
- 10% of block rewards will accrue to dedicated Super Node Multisig addresses.
- Super Node operators will be compensated similarly to the current Secure Node System until production-level software is available in Q4.

This proposed mechanism provides partial incentive to start planning Super Nodes early, but then to also follow through on setting up the nodes when the system becomes operational. Since the expected number of Super Nodes will require anywhere between 1 million and 1.25 million ZEN to be committed to stake addresses, it is better that this accumulation process initiate early and extend over a longer period than to start suddenly in Q4. We believe this hybrid reward system both incentivizes early accumulation and follow-through in setting up Super Nodes when the system goes live.

CONCLUSION

What we propose in this paper is a major system upgrade on multiple levels. The Super Node system will bring Secure Node tracking and payments on-chain and automate the process for big efficiency and reliability improvements. The economics of the system will be changing in a way that greatly incentivizes users to stand up more Secure Nodes and Super Nodes. A nearly 3-fold increase to payouts will greatly increase the number of operating nodes and the introduction of Super Nodes boosts the quality of systems comprising the network. However, the most noteworthy announcement is that this large and growing network (possibly the largest in the industry) will migrate into a platform upon which distributed applications will reside via multi-level sidechains. The applications already in our pipeline each bring major utility to the community, but this is just a starting point. The future goal is to open the platform to external dApp developers so that anyone in the world can contribute to the ecosystem. Our mission has always been to integrate societies, erode artificial frictions, and make the world a better place. These system upgrades will make for a much more powerful network upon which the real fun can begin!

References:

[1] -https://github.com/ZencashOfficial/
[2] -https://zencash.com/
[3] -https://securenodes.eu.zensystem.io/