STASHPAY.IO

STASHPAY.IO SOFTWARE

TECHNICAL WHITEPAPER V2

INDEX

PLEASE NOTE: CRYPTOGRAPHIC TOKENS REFERRED TO IN THIS WHITE PAPER REFER TO CRYPTOGRAPHIC TOKENS ON A LAUNCHED BLOCKCHAIN THAT ADOPTS THE STASHPAY.IO SOFTWARE. THEY DO NOT REFER TO THE ERC-20 COMPATIBLE TOKENS BEING DISTRIBUTED ON THE ETHEREUM BLOCKCHAIN IN CONNECTION WITH THE STASHPAY TOKEN DISTRIBUTION.

DISCLAIMER: This STASHPAY.IO Technical White Paper is for information purposes only. All STASHPAY.IO documentation, designs, and sources are in the research, development and conceptual phase and subject to change. Stash Labs Pty Ltd does not guarantee the accuracy of or the conclusions reached in this white paper, and this white paper is provided “as is”. Stash Labs Pty Ltd 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. Stash Labs Pty Ltd 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 Stash Labs Pty Ltd or its affiliates be liable to any person or entity for any damages, losses, liabilities, costs or expenses of any kind, whether direct or indirect, consequential, compensatory, incidental, actual, exemplary, punitive or special for the 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 intangible losses.

INTRODUCTION

STASHPAY.IO is an open source cryptographic software that combines many innovative protocol features from Bitcoin, Dash and Zcash while solving numerous problems currently experienced by various open source blockchain software. While different blockchain software possess diverse and valuable attributes each also has their own problems. These issues include slow transaction speeds, high transaction costs, poor scalability, a fair launch, strong privacy, practical governance framework, a continuous funding structure and correct user incentives. The goal of STASHPAY.IO is to bring together many of the most cutting-edge blockchain software features and build on top of proven block chain technology to solve or eliminate these problems. This, in turn, should create a blockchain software that is increasingly useful and desirable for end users and long-term holders alike.

It is envisioned that over time new features will be developed internally as well as sourced from the crypto community at large as new innovations become available and the STASHPAY.IO users decide that such features can be implemented to improve the utility of the STASHPAY.IO software.

Rather than being static and rigid the idea of STASHPAY.IO is for the blockchain software to evolve organically through the help of its community. To this end, Stash Labs will look to raise awareness as well as attract talented and like minded developers from all over the globe to help grow, develop and innovate the software.

While much progress has already been achieved Stash Labs intends to speed up development of the STASHPAY.IO blockchain software privacy feature through the integration of a zero-knowledge security layer (ZSL). ZSL in STASHPAY.IO will be designed to anonymously settle transactions on the blockchain.

Additionally the STASHPAY.IO budgeting system, which will be funded monthly from the block reward will mean the project will have a chance to gather resources in the form of tokens which may be utilized for further development.

STASHPAY.IO will always endeavor to evolve and adapt by being nimble, open and flexible to new opportunities that may arise. To this end the STASHPAY.IO governance system has been setup to quickly adopt and take advantage of new opportunities as they become apparent without having to deal with some of the decentralized decision-making problems that are clearly evident with other blockchain software.

The ultimate end goal of STASHPAY.IO is simple, become the most useful and user-friendly blockchain software to the end user for every day and international transactions.

iNODE NETWORK

For a blockchain software to operate, full nodes are required. These nodes operate on P2P networks, and send updates to peers following events which take place on the network. However, in order to be effective, such nodes require high volumes of traffic, as well as support from additional resources, which come at a significant cost.

This can result in the steady decrease of full nodes, as has been witnessed on the Bitcoin network. The outcome of this is a major failing in performance, with block propagation times exceeding 40 seconds.

The STASHPAY.IO software combats this via a 2nd tier network layer which acts as a sort of safety net, guaranteeing high performance for longer. This is the iNode network of nodes, which are highly available and must provide a certain standard of service if they are to qualify for the iNode Reward Program.

HOW ARE iNODES REWARDED

The iNode Reward Program serves to incentivize the network, growing the number of full nodes that are operational at any one time. Without such a program, the network operator must pay the costs of the full node as traffic across the network increases, which can be unsustainable.

The iNode network is different because the individual nodes are tied into a specific level of service, which is secured by collateral. This collateral remains protected while the iNode remains in operation, encouraging stability across the network and giving iNode operators the opportunity to earn additional STASHPAY.IO tokens.

These payments are derived from the block rewards accrued on the network, with around 45% of the total paid out in tokens to iNodes who uphold their level of service. However, there is some fluctuation in the total amount payable per day, as the iNode Rewards Program percentage is fixed, and yet the number of nodes are variable. Payment per day of iNode operation is calculated thusly;

$n \times r \times s \div t$ in which

$n =$ Blocks Per Day

$r =$ Block Reward

$s =$ iNode share of each block reward

$t =$ Total number of iNodes

For calculating the reward payments on an iNode, the following formula is used, based on the same definitions as to the left;

$$\text{Rate of return per iNode} = (n \times r \times s) \div t \times 365.25 \div 10{,}000$$

Where 10,000 = the amount of STASHPAY.IO tokens collateral required to operate an iNode.

As there is only a limited amount of STASHPAY.IO software tokens available and there is a cost involved with running an iNode. There is a limit in terms of how many iNodes can be running on the network at any given time. This limit is based on the amount of STASHPAY.IO tokens generated in the genesis block plus any STASHPAY.IO tokens that have been mined.

iNODE ARRANGEMENT

An algorithm based on the mining block hash is used to order iNodes in a pseudo-random deterministic way. The mining network provides the security of this functionality by using the hash from the proof of work for each block.

COLLATERAL SYSTEM

It is critical for the security of the system that no one individual or body gains control of the entire network of iNodes. To achieve this, the after mentioned collateral system has been implemented, by which anyone who wants to control an active iNode must put down 10,000 STASHPAY.IO tokens as a deposit.

Given that STASHPAY.IO tokens will be limited in supply it means that the price of STASHPAY.IO tokens respond directly and quickly to demand. To gain control of a significant section of the iNodes on the network, the individual would need to purchase a vast amount of STASHPAY.IO tokens units from the open market, driving up the price and making it impossible for them to achieve their goal.

This enables the overall STASHPAY.IO software to utilize the 2nd tier iNode structure to carry out sensitive tasks. No trust or overall responsibility is awarded to any one node or group of nodes, and so no one is able to control the network for their own ends because iNodes are selected at random to perform the same task concurrently.

NETWORK CHECKS AND BALANCES

The role of an iNode is not limited to relaying and validating transactions. There are other, highly important, benefits which these nodes can provide. As such, it is critical for the network to be able to assess which iNodes are online, which ones are actively responding, and which ones are behaving in line with the code of service they have agreed to.

This requires proof of service. It is not enough simply to assess which iNodes are functioning, as a certain level of service must also be attained. To ensure this level of service, the iNode network uses Quorums; two Quorums are chosen for each block, and Quorum A assesses the service level of Quorum B. Quorum A is made up of the nodes closest to the hash of the current block. Quorum B, on the other hand, is made up of nodes furthest away from this hash.

In this way, the system is kept trustless by randomly selecting nodes through the quorum system which makes the network self-accessing.

iNODE PROCEDURES

The basic function of an iNode is very simply to relay and validate transactions and as such a node requires only two protocol messages to become active on the STASHPAY.IO software. These two messages are the iNode announce message and the iNode ping message.

The announce message protocol is used to announce the presence of the node on the network when it initially starts up. Following this, the ping message protocol will be sent every 15 minutes, as part of the proof of service procedure. If this is not carried out at a satisfactory rate, the node will eventually be deactivated. Additionally, the node must have its ports open ready to receive pings, if not, it is deemed to be inactive.

However, in practice, their function is rather more complex and relies upon additional protocols, including PrivateSend and InstantSend, which are both used to ascertain proof of service.

An iNode becomes active when a user sends 10,000 STASHPAY.IO tokens units to a designated address in a designated wallet on the network. Once this action is confirmed, the node will be able to use the announce and ping protocol messages to propagate itself across the network.

The network includes in-built security measures by using a cold mode to prevent malicious activity on the system. For example, if an iNode sends the private key in a message following activation and this is used on a second machine, the system will deactivate the original node, protecting the 10,000 STASHPAY.IO tokens units from theft.

The 10,000 STASHPAY.IO token collateral need not be stored in the actual iNode wallet but rather can be stored remotely in a safe location to prevent the STASHPAY.IO token collateral from being stolen.

FINDING ACTIVE iNODES

If the STASHPAY.IO software is to be successful, new users must be able to understand quickly and easily which iNodes are currently active. To achieve this, users are sent a known list of iNodes and their status whenever they join the network. Following the receipt of this list, the user's cache the list so that when they restart they can just look up the directory rather than having to ask for the whole list again.

TRANSACTION SPEED AND SCALABILITY

By implementing 150 second block times and a second-tier iNode structure that is capable of supporting up to 20-megabyte blocks, STASHPAY.IO provides 80x Bitcoin transaction capacity and as a result, ensures transactions fees are kept low. This also means STASHPAY.IO software will have no near-term capacity issues which will allow the STASHPAY.IO team to research and implement further capacity improvements over time.

MINING

On the STASHPAY.IO software, there are complex cryptographic problems which must be solved in order to secure a block on the blockchain. This procedure is known as mining, and the STASHPAY.IO software will reward users who engage in mining activity with STASHPAY.IO software.

In order to secure blocks on the STASHPAY.IO software, we propose miners will need to find solutions to the X11 algorithm. This can be achieved on a variety of different hardware devices, including the basic CPU which is found within standard desktop and laptop computers.

Modern CPU's are fairly powerful, but they are also designed with numerous different applications in mind. This versatility is actually a hindrance when it comes to mining, which instead requires a high number of vectors to be calculated concurrently.

A standard CPU can be enhanced using AES or AVX, making it more suited to mining operations. GPU's offer improved performance due to their numerous pipelines for predictable calculations required in mining. However, ASIC's, which are specifically designed for high-performance resolution of a particular type of algorithm are far superior than CPUs and GPUs.

REMUNERATION AND IMPLEMENTATION

The STASHPAY.IO software is set up to ensure that each iNode receives its due share of the block reward. This requires the network to enforce payments between the block in question and the correct iNode, which in turn requires conscientious behavior and practice from the miner. If the miner is not able to uphold these standards, the blocks they process will be rejected by the network, in order to discourage cheating.

But this must be enforced. To achieve this enforcement, iNodes create Quorums, then broadcast their choice of the correct iNode (the one which must be paid). The process is completely decentralized and trustless, so there is no way that iNodes can collude on the matter and defraud the system. Once a certain number of messages have been received, a voting consensus can be reached and the block will be obligated to pay the chosen iNode.

Miners using pool software can obtain information on how to get a block through the use of the RPC API. When accessing the API, the user extends the form and adds a secondary recipient in the GetBlockTemplate. If the block is successfully mined, the payment is split between the miners and the iNodes.

GOVERNANCE AND FUNDING

The conundrum of governance is a tricky one for developers of a blockchain software network to resolve. On the one hand, the network needs to be effective, with decisions taken quickly and effectively to ensure positive development in the short and long term. On the other hand, the decentralized nature of the blockchain software should be protected.

This requires a structured governance system; something which the STASHPAY.IO software implements via a system of Self-Governance.

WHAT IS SELF-GOVERNANCE?

Self-Governance is the governance solution that STASHPAY.IO software uses to allow for quick decision making in a decentralized network. Rather than debating options and decision possibilities Self-Governance provides rules which allow for quick resolutions. Taking Bitcoin as an example, a debate on this network regarding the size of an individual block has taken years to resolve, while in the STASHPAY.IO software, such a question can be voted on and put to rest in a matter of hours. The result is a far more efficient network.

The Self-Governance system requires proposals to be put forward to the network as a whole, and then voted on. In practice, this means that iNodes are able to cast a vote on important changes to the system or network, and, as no one can assume control of too many iNodes, dominance of the vote is not possible.

WHAT IS SELF-FUNDING?

Included in the Self-Governance system is the way in which block rewards are utilized to provide ongoing funding to the network. For each block that is mined, the miner receives 45% of the reward, while the iNode receives another 45%, which leaves 10% remaining. This 10% is not created until the end of the month. During the month, anyone can make a budget proposal, which is voted on by the network. At the end of the month Treasury blocks are created and if 10% of iNodes vote for any proposal then that proposal is approved. If no proposals are approved or the 10% reward amount is more than needed to cover the cost of the proposal, the reward goes to the treasury and is available for funding future proposals. This system allows the network to fund itself and also provides the opportunity to build up assets in the form of STASHPAY.IO tokens which can be used to fund future as well as potentially larger proposals.

FUNGIBILITY PROBLEM

With Bitcoin, it has become apparent that transactions aren't fully private. This leads to a fungibility issue. Fungibility just means that my Bitcoin is worth exactly the same amount as yours as they are perfect substitutes. However, by analyzing the public ledger third parties are able to link Bitcoin transactions to people's identities. This can lead to Bitcoins being tainted due to their unfavorable past histories. STASHPAY.IO software will integrate a zero-knowledge security layer (ZSL) on top of the STASHPAY.IO software in order to provide users superior transaction privacy and solve the fungibility issue.

The zero-knowledge security layer is based on zk-SNARKs a form of zero knowledge cryptography that provides transaction privacy for users on the network. Privacy is achieved by enabling full transaction encryption on the blockchain, but retaining verifiability by network consensus.

This section deals with how this is possible, and the benefits it provides to users and to the network as a whole.

SUPERIOR PRIVACY THROUGH ZERO KNOWLEDGE CRYPTOGRAPHY

Unlike other methods for blockchain software privacy that rely on obscuring the linkage between transactions, STASHPAY.IO software encrypts transactions on the blockchain. This allows for the amount, origin and payment destination to stay hidden while still verifying the transfer of funds under the network's consensus rules using zk-SNARK proofs.

UNDERSTANDING ZK-SNARKS?

The zk-SNARK – or zero knowledge succinct non-interactive argument of knowledge – proof has been available for some time, but it was first deployed on a widespread scale within the ZCash blockchain software.

Via zk-SNARK, an individual can prove that he has certain information without revealing the information in question, and with no interaction between himself and another user; who are defined as prover and verifier.

With zero-knowledge, the prover is able to convince the verifier that a certain statement is true by only revealing information that proves the validity of the statement but not the statement itself. For example, it could be proved that a hash of a random number exists without revealing what that number is.

Zero knowledge 'proof of knowledge' takes this a step further. The prover can convince the verifier that not only does such a number exist but that they know what that number is without revealing any information about that number.

It is possible to confirm succinct zero knowledge proofs with only a few hundred bytes and within a few milliseconds even for large statements. Whereas early zero knowledge proof systems required numerous rounds of communication, non-interactive constructions only require a single message be sent between the prover and verifier. At this point the only zero-knowledge proofs that are short enough to publish on a blockchain consist of a setup phase that creates a mutual reference string which is shared between the prover and verifier. These shared reference strings can be referred to as public parameters.

If someone was able to access secret randomness used to create the public parameters, they could produce false proofs and, in turn, create fake STASHPAY.IO tokens which would be indistinguishable from real ones. However, the manner in which the parameters are created makes it impossible for this malicious activity to take place. Public parameters are generated in a sophisticated event involving multiple different users; an event which is known as a ceremony. Each user involved in the ceremony is then forced to destroy their minute piece of the parameters. Even if only a single user destroys their piece, the parameters are unusable, making it highly unlikely that these parameters could exist and fall into the wrong hands.

STASH LAYERED NETWORK

For a blockchain software network to function properly, there must be a structure in place; a transaction must undergo certain proofs before it can be verified.

In the case of Bitcoin, a transaction will be validated after the following three items have been proved;

1. That the Bitcoins being used have not been spent by the sender previously. The sender does not need to take any action to show that this is the case as this is ascertained simply by examining the ledger.

2. That the sender has the necessary authority to send the coins to the value agreed upon in the transaction. This is validated by signing the transaction with the secret key which relates to the address where the coins are being sent from.

3. That the transaction is balanced in terms of coins inputted and coins taken out. This should be evident from the transaction, as the amount being transferred is known to all parties.

STASHPAY.IO will use a form of zero-knowledge proofs known as zk-SNARKs to prove the above points without revealing any additional information. When each transaction is validated, there also exists a zk-SNARK which can be used to show that STASHPAY.IO tokens exist and have not been spent, the sender has the authority to send the STASHPAY.IO tokens, the amount of STASHPAY.IO tokens sent equals to the amount of STASHPAY.IO tokens received.

During this process, the information required for spending STASHPAY.IO tokens is attached to the transaction by creating a new zk-SNARK and is encrypted using the recipients public key which can only be used by the transaction recipient.

This results in a new distributed ledger which has been called the zero-knowledge security layer.

INSTANTANEOUS TRANSACTIONS

Transactions on the STASHPAY.IO software need to be secure and private, but also quick. STASHPAY.IO users iNodes quorums to provide the ability to send and receive irreversible transactions instantaneously.

When a quorum is formed the inputs of the transaction are locked for spending. This lock takes approximately four seconds to complete. If the iNode network achieves a consensus, any conflicting transactions or blocks will be rejected henceforth. Only exact matches on the transaction ID will be accepted.

The idea of this is to connect the STASHPAY.IO software with real world usage, for example via a mobile device at the point of sale. If users are able to settle commercial transactions using digitally encrypted blockchain software, with zero delay, then the STASHPAY.IO software could become a serious rival to traditional cash, credit or debit card forms of payment.

STASHPAY.IO TOKENS AND STASHPAY.IO SOFTWARE SUPPLY

The supply of STASHPAY.IO tokens will depend on the balance that is placed into the genesis block by the community. A maximum of 997.8million STASHPAY.IO Tokens will be minted which includes any STASHPAY.IO tokens that are created in the genesis block. as well as any STASHPAY.IO tokens that are mined over approximately the next 100 years.

STASHPAY.IO MINING SUPPLY

STASHPAY.IO software will be created to allow mining may result in STASHPAY.IO tokens being minted and therefore result in inflation of the STASHPAY.IO token supply. In order to counteract this inflation, the new supply will be reduced each year at the rate of 7.1% per annum.

As well as this measure, STASHPAY.IO software will implement a direct connection between the supply for each block and number of miners active on the network. If the number of miners decreases, the rewards received from each approved block increases accordingly and vis-versa.

The ongoing production of the STASHPAY.IO tokens are expected to continue until about midway through the next century, at which point the block reward will approach zero and miners and iNodes will be incentivized by transaction fees.