Worktips

Decentralised & Private transactions.

Worktips is an ASIC resistant cryptocurrency designed for mining and perfect for rewarding(tipping) everyone.

Version 1

December 01st 2021

Abstract

A hybrid proof of work/proof of service system offers a unique way to financially incentivise the operation of full nodes. Worktips leverages these incentivised nodes to create a secondary private routing layer. Minimum node functionality on the second layer is monitored and enforced by a novel method called swarm flagging. Worktips is based off Loki/Oxen which is a modified version of the Monero source code, assuring that all transactions achieve a high degree of privacy.

This white paper outlines the technology used in Worktips. We anticipate that changes to this technology will occur as Worktips continues to be developed. New versions of this white paper will be released to reflect any substantial future changes and updates.

Huge Thanks to Loki/Oxen and Monero Team for their open-source code.

Huge Thanks to uPlexa Team for their algo code.

1 Introduction

The demand for privacy in digital communications and transactions is ever increasing. User data is being collected, processed, and traded at unprecedented levels. Everything from a users browsing data and email contents, to credit score and spending habits, are gathered and sold between the worlds largest corporations and state level actors. Worktips aims to provide a censorship-resistant suite of tools that will allow users to transact and communicate in private.

Bitcoin came with the promise of privacy, but what has resulted is more traceability than ever. Companies like Chainalysis and BlockSeer have taken advantage of Bitcoin's transparent blockchain architecture to track and follow specific transactions [1]. Worktips is built off Monero, a cryptocurrency that has established itself as one of the most secure and private transaction networks to date [2]. However, we recognise that Monero has inherent drawbacks. Monero transactions are orders of magnitude larger than Bitcoin transactions, with significant bandwidth, processing, and disk space requirements. As the network grows, this results in a large burden on Monero node operators and offers no incentive or reward for their contributions to the network. This makes running a node a costly and often thankless exercise. The introduction of a node reward scheme, called *Service Nodes*, mitigates this by providing economic incentives for node operators.

Service Nodes can also be used to provide a range of other privacy-centric functions if properly incentivised. Primarily, the Service Node network will allow users to transmit and receive data packets anonymously. This private communication is facilitated by each Service Node acting as a relay in a novel Sybil resistant mixnet, having similar properties to Tor and I2P [3][4].

2 Basic Parameters

Worktips difficulty target (blocktime)	120 Seconds
Difficulty algorithm	Zawy LWMA [5]
Hashing algorithm	CryptoNight UPEX(cryptonight v8 upx2)
Elliptic curve	Curve25519 [6]

3 CryptoNote Elements

Although a full-node incentives scheme could be implemented on top of any cryptocurrency, Worktips uses the Monero source code because of the high level of privacy it affords to transactions. Monero is an evolution on the CryptoNote protocol, which uses ring signatures, stealth addresses, and RingCT, giving users the ability to sign transactions and obfuscate amounts while maintaining plausible deniability [7].

For the Worktips ecosystem to maintain privacy, it is important to not only provide a medium of exchange that underpins the internal economy but to also minimise the risk of temporal analysis when interactions occur across Worktips's independent layers. For example, when engaging in layer-one transactional services, users should never lose the privacy guarantees they receive from the second-layer and vice versa.

3.1 Ring Signatures

Ring signatures work by constructing a ring of possible signers to a transaction where only one of the signers is the actual sender. Worktips makes use of ring signatures to obfuscate the true history of transaction outputs. Ring signatures will be mandatory for all Worktips transactions (excluding block reward transactions), and uniquely, a fixed ring-size of ten is enforced on the Worktips blockchain. This means that each input will spend from one of ten possible outputs, including the true output .

3.2 Stealth Addresses

Worktips makes use of stealth addresses to ensure that the true public key of the receiver is never linked to their transaction. Every time a Worktips transaction is sent, a one-time stealth address is created and the funds are sent to this address. Using a Diffie-Hellman key exchange, the receiver of the transaction is able to calculate a private spend key for this stealth address, thereby taking ownership of the funds without having to reveal their true public address [8]. Stealth addresses provide protection to receivers of transactions and are a core privacy feature in Worktips.

3.3 RingCT

RingCT was first proposed by the Monero Research Lab as a way to obfuscate transaction amounts [9]. Current deployments of RingCT use range proofs, which leverage Pedersen commitments to prove that the amount of a transaction being sent is between 0 and 2^{64}. This range ensures that only non-negative amounts of currency are sent, without revealing the actual amount sent in the transaction. Recently a number of cryptocurrencies have proposed implementing bulletproofs as a replacement to traditional range proofs in RingCT because of the significant reduction in transaction size [10]. Worktips will utilise bulletproofs, reducing the information that nodes are required to store and relay, thereby improving scalability.

4 Service Nodes

Although Worktips implements novel changes on top of the CryptoNote protocol (see 7), much of Worktips's networking functionality and scalability is enabled by a set of incentivised nodes called Service Nodes. To operate a Service Node, an operator time-locks a significant amount of Worktips and provides a minimum level of bandwidth and storage to the network. In return for their services, Worktips Service Node operators receive a portion of the block reward from each block.

The resulting network provides market-based resistance to Sybil attacks, addressing a range of problems with existing mixnets and privacy-centric services. This resistance is based on supply and demand interactions which help prevent single actors from having a large enough stake in Worktips to have a significant negative impact on the second-layer privacy services Worktips provides. DASH first theorised that Sybil attack resistant networks can be derived from cryptoeconomics [11]. As an attacker accumulates Worktips, the circulating supply decreases, in turn applying demand-side pressure, driving the price of Worktips up. As this continues, it becomes increasingly costly for additional Worktips to be purchased, making the attack prohibitively expensive.

To achieve this economic protection, Worktips encourages the active suppression of the circulating supply. In particular, the emissions curve and collateral requirements must be designed to ensure enough circulating supply is locked and reasonable returns are provided for operators to ensure Sybil attack resistance.

4.1 Block Reward

Distribution of block rewards in Worktips is conducted through proof-of-work, a robust and well-studied system for the creation of blocks and the ordering of transactions. Miners collect and write transactions into blocks and collect fees for doing so. As a consensus rule in Worktips, each block contains multiple reward outputs of which only one goes to the miner.

Mining Reward:
As well as collecting transactions fees, 45% of the block reward is awarded to the miner that constructs the block.

Service Node Reward:
The second output in each block (50% of total reward) goes to a Service Node, or two Service Nodes if a relay is selected. Service Nodes are rewarded based on the time since they last received a reward (or time since they registered), with a preference for nodes that have been waiting longer. Each time a Service Node registers with the network it assumes the last position in the queue. If the Service Node maintains good service and is not ejected from the queue by a swarm flag, it slowly migrates to the higher positions in the queue. Nodes at or near the front of the queue are eligible for a reward, and once awarded, the node again drops to the last position in the queue and begins slowly working its way back up.

Governance Reward:
The final 5% portion of the block reward is distributed towards governance operations.

4.2 Verifiable Collateralisation

Service Nodes must prove to the network that they are holding the required collateral. Privacy features inherent in Worktips's design make this difficult, specifically the inability to audit public address balances or to use viewkeys to see outgoing transactions.

Worktips makes novel use of time-locked outputs, which allow Worktips coins to be time-locked until the blockchain reaches a defined block-height. Until this defined height, the Worktips network will invalidate attempts to spend these time-locked outputs. Worktips utilises this process to prove that an amount is being held by a specific Service Node, preventing shuffling of collateral.

To register as a Service Node, an operator creates a locked output of the required amount. In the extra field of the transaction, the Service Node operator includes the Worktips address which may receive Service Node rewards. This address will also be used as the public key for Service Node operations such as swarm voting. Wallets may avoid using these Service Node registration transactions as mixins, as their true amounts and destination are disclosed and therefore are not useful in providing extra anonymity to a transaction.

Before each node joins the Service Node network, other nodes must individually validate that the said nodes collateral outlay matches the required amount, as per the decreasing collateralisation requirement.

5 Worktips Services

Similar to the investment that miners make into hardware, each Service Node operator freezes Worktips coins when they begin to operate a Service Node. This frozen capital serves two purposes.

1. Every Service Node operator has a sufficiently large stake in the success of the network. Should any Service Node operator provide poor performance to the network, or act dishonestly, they undermine and risk devaluing their own stake within the network.

2. It provides an opportunity for more aggressive enforcement; if the network is able to effectively limit dishonest nodes from receiving a reward, then dishonest nodes must bear the opportunity cost of both the reward loss and the remaining lockup time on their collateral.

If we take the above points to be true, and we can enforce aggressive punishments for poorly behaving nodes , then we can create groups of Service Nodes which can be queried to come to consensus on the state of the blockchain or to enforce special off-chain node behaviour. In Worktips, this behaviour pertains to both networking and storage activities. These off-chain activities are combined to be the back-end of user-facing applications that leverage these desirable properties, which are called *Worktips services*.

5.1 Remote Nodes

On any given cryptocurrency network, storing a full copy of the blockchain is not possible or practical for many users. In Bitcoin and Ethereum, users can choose to connect to a public full node that holds a copy of the blockchain and can query and submit transactions to the network. This works because Bitcoin and Ethereum full nodes can efficiently search the blockchain for transactions that have the users public key as the target.

Due to the construction of CryptoNote currencies, public full nodes (called remote nodes) are put under much more stress. When a user connects to a remote node, they must temporarily download every block (upon wallet creation or since last checked block) to their local machine and check each transaction for a public transaction key which can be generated from the users private view key. This process can cause a significant performance impact on remote nodes. Considering that there is no reward for this service, it can dissuade users from operating syncing services for light clients. CryptoNote mobile wallets are often unreliable and sometimes have to switch between remote nodes multiple times before establishing a reliable connection to either scan the blockchain or to submit a transaction.

Additionally, malicious remote node operators running one of the few popular nodes can record the IP address of users as they broadcast specific transactions. Although no information about the actual transaction is revealed by this attack, specific IP addresses can be linked with transactions which can then be used to establish a link to a real-world identity, compromising privacy.

Worktips circumvents these issues by requiring each Service Node to act as a remote node that can be used by general users. Service Nodes naturally lend themselves to this work as they already hold a full copy of the blockchain and form a widely distributed network of high bandwidth nodes. By using Service Nodes as remote nodes, there is an inherent financial limitation as to how much of the remote node network any given party can own, and therefore, how much data a malicious node operator can collect.

5.2 Tachus

In a typical blockchain system, the confirmation time for any given transaction is the time it takes for a transaction to be included in a block. Because of competing miners, withheld blocks, and Finney attacks, recipients usually require a number of additional blocks to be created on top of the block which holds a transaction before it is considered to be complete [24]. Depending on a multitude of factors specific to each blockchain, this process can often take 10-60 minutes, which is inconvenient for merchants and customers who must wait for confirmations before they release goods or commence services.

Because of Worktips's Service Node architecture, near instant transactions are possible. *Tachus* enables the same transactions that would occur on the Worktips mainchain to be confirmed before being included in a block, assuring both the sender and the receiver of the validity of the transaction and protecting the receiver against a double spend.

Tachus works in a similar fashion to DASH's InstantSend. Each block, a Service Node swarm is deterministically selected to act as a set of witnesses that confirm a transactions validity and lock the transaction from being spent twice. Instead of the unspent outputs used in the transaction being locked (like in DASH), key images are locked. Key images are unique keys that are attached to each unspent output in a ring signature. To provide immediate confirmations, Tachus gives authority to the selected swarm to signal to the network that a key image associated with an output should be locked until the transaction is included in a block. If a double spend of the same unspent output is attempted, an identical key image is produced, which would be rejected by the swarm and thus the network as a whole.

Users will have the ability to pay a higher fee to send a Tachus transaction which will confirm in seconds rather than in minutes. This opens up a range of new use cases for Worktips where face-to-face payments become increasingly practical and online payments become easier to integrate. All of the privacy features inherent in Worktips are uncompromised throughout this process.

6 CryptoNote Alterations

As a cryptocurrency, Worktips is functionally similar to its fellow CryptoNote coins. However, there are key differences beyond the addition of Service Nodes and the associated functionality that comes with them.

6.1 ASIC Resistance

An Application-Specific Integrated Circuit (ASIC) is a computer chip that is built specifically for a single function. In the context of mining, ASICs are used to compute for specific hashing algorithms. They pose a risk to decentralisation because they outpace all other mining methods, are manufactured by specific companies, have very limited distribution channels due to the specialised nature of the hardware, and they require significant capital costs to develop and operate profitably. There are potential benefits to ASICs, such as the capital cost requirements that miners must undertake to invest in algorithm specific hardware which makes it less likely that they would behave in a manner that undermines their own investment by acting dishonestly. However, the distribution and manufacture of ASIC chips, with mature hashing algorithms, is still centralised around a few large companies. These companies can refuse shipment to certain areas, decide what regions and customers get the best performing ASICs, and they can structure limited runs and manipulate prices.

To prevent ASIC miners from monopolising the network hashrate, many cryptocurrencies developed ASIC resistant hashing algorithms, like Scrypt and Ethash [25][26]. Until recently, Monero used the CryptoNight hashing algorithm, which requires large amounts of L3 cache to operate. In theory, this should have made it difficult to produce an ASIC chip due to large memory requirements. However in 2018 Bitmain released the X3, a CryptoNight specific ASIC that could effectively mine at ten times the speed of a graphics processing unit (GPU) [27]. Other hashing algorithms have suffered similar fates, with Scrypt, Ethash, and Equihash all now being mined by ASICs.

To combat the use of ASICs, Monero proposed a strategy of hard forking every 3-6 months to slightly change the CryptoNight hashing algorithm (the first fork moving to CryptoNightV7 [28]). The capital and time required to build an ASIC is significant, and with highly specific hardware designs, slight tweaks in a hashing algorithm should invalidate the chip design, wasting the time and capital investment of ASIC manufacturers. However, this approach introduces its own issues. If changes made to the algorithm are insufficient to prevent ASICs being reprogrammed, then the network can become vulnerable to hashrate centralisation until another hard fork is possible. Field Programmable Gate Arrays (FPGAs) should also be considered in ASIC resistance strategies, where infrequent, slight changes to hashing algorithms can be easily reprogrammed for FPGAs. Another concern is that regular changes to core consensus mechanisms introduce the chance of unintended bugs and generally centralise the development of such changes around the core team of developers.

A number of alternative proof-of-work algorithms have been proposed to combat the need to hard fork regularly, including provably memory-hard hashing algorithms like Argon2, Balloon hash, and polymorphic hashing algorithms like ProgPoW and RandProg [29][30][31][32].

While this work is undertaken, Worktips will incorporate a version of CryptoNight called CryptoNight Upex (cryptonight v8 upx2), which maintains ASIC resistance against CryptoNight ASIC miners. CryptoNight Upex differs from CryptoNight in a number of ways: it provides cnv8 w/ 36,728 Iterations, 128kb mem, and reverse shuffle operations and also provide more robust protection against ASIC development until a more permanent solution is proposed.

6.2 Dynamic Block Size

Like other CryptoNote coins, Worktips does not have a fixed block size. Instead, the block size changes over time, growing to include more transactions as the network reaches higher transaction throughput. The Worktips block size scales by observing the median block size over the last 100 blocks and slowly retargets the maximum size of any new blocks accordingly.

The long-term concern in other cryptocurrencies is that large block sizes burden the nodes that store and verify transactions. As block sizes grow, nodes that run on lower grade hardware are unable to process and propagate new blocks, leading to centralisation of the node network among those with a commercial interest in maintaining nodes. This can be concerning because distributing the blockchain across many nodes allows for the state of the chain to be confirmed among many different parties, adding to its validity and censorship resistance.

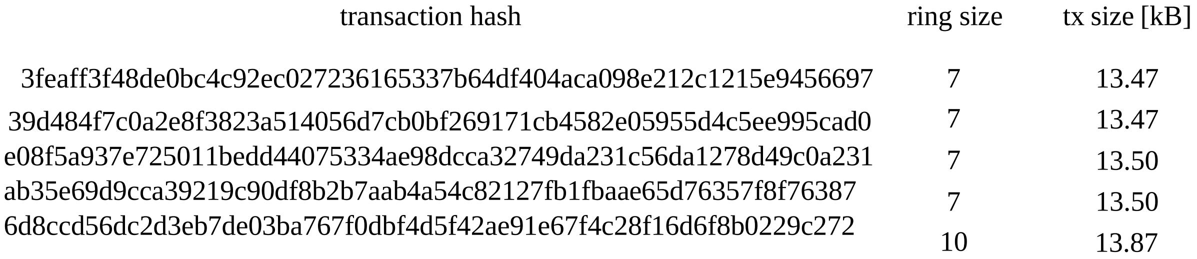
In Worktips, a portion of the block reward is given to Service Nodes that process and propagate blocks as full nodes. Because Service Nodes with insufficient bandwidth and performance are dropped from the Service Node network, the reward pool self-enforces a minimum performance requirement. This incentive structure not only ensures that the node count remains high, but that the said nodes are of a sufficient performance level to successfully share blockchain data across the network, irrespective of how large the blockchain grows or how demanding the bandwidth requirements are. Even so, transaction size optimisations are still required to ensure that the network scales efficiently so as to keep the Service Node operating costs down so that a high node count can be sustained in the long term.

6.3 Ring Signature Size

Ring signatures are used to hide real outputs amongst others in any given transaction. The size of a ring signature refers to how many mixins are used to construct the ring. Monero currently has an enforced minimum ring signature size of seven, with six mixins used alongside the real unspent output in a transaction.

The effect of larger ring-sizes has been sparsely studied, however, in paper 0001 (published by the Monero Research Lab), the effect of differing ring-sizes was analysed versus an attacker who owned a large number of outputs on the blockchain [34]. It was found that higher ring-sizes reduce the timeframe in which a malicious attacker who owned a large number of unspent outputs would be able to perform effective analysis of transactions. Mandating larger ring-sizes also protects against a theoretical attack known as an EABE/Knacc attack [35], where a third-party (i.e. an exchange) can perform limited temporal analysis on transactions between two users.

Additionally, Monero has no maximum ring-size enforced by network consensus rules. Many wallets like the Monero GUI wallet cap the ring-size at 26. However, a user is free to manually create a transaction with whatever ring-size they wish, as long as it is above a ring-size of seven. This is problematic since most wallets have a default ring-size of seven. Increasing a transactions ring-size above seven makes it stand out (Figure 4). Further, if an individuals transactions were to always use a non-standard ring-size in Monero (ten for example), a passive third-party could analyse the blockchain and infer patterns using temporal analysis.



transaction hash	ring size	tx size [kB]
3feaff3f48de0bc4c92ec027236165337b64df404aca098e212c1215e9456697	7	13.47
39d484f7c0a2e8f3823a514056d7cb0bf269171cb4582e05955d4c5ee995cad0	7	13.47
e08f5a937e725011bedd44075334ae98dcca32749da231c56da1278d49c0a231	7	13.50
ab35e69d9cca39219c90df8b2b7aab4a54c82127fb1fbaae65d76357f8f76387	7	13.50
6d8ccd56dc2d3eb7de03ba767f0dbf4d5f42ae91e67f4c28f16d6f8b0229c272	10	13.87

Figure 3: *xmrchain.net (Monero block explorer) showing how non-standard ring sizes stand out*

Worktips improves on both of these problems by statically enforcing ring-sizes, and setting the ring-size to ten. Statically setting the maximum ring-size protects users who construct rings with more than nine mixins and setting the ring-size minimum to ten more effectively prevents an attacker who owns a large number of outputs from discerning the true outputs spent in a ring signature. Larger ring-sizes also increase the default churning effectiveness non-linearly, becoming more effective as ring-sizes grow.

In the current transaction scheme, increasing the ring-size to 10 would lead to a 2.6% increase in the size of the transaction. However, when Bulletproofs are implemented it will account for about a 8 - 13% increase in the size of a transaction. This is because of the overall reduction in transaction size caused by Bulletproofs. Increasing the minimum ring-size may present a problem on a network that lacks architecture to support larger sized transactions, due to the increased overhead. With Worktips however, this burden can be carried by Service Nodes that are incentivised to operate and provide sufficient bandwidth.

7 Attack Prevention

7.1 IP and Packet Blocking

Although the Service Node network has no central points of failure, two significant censorship threats face the network; namely harvesting attacks and deep packet inspection [36][37]. Harvesting attacks would seek to gather the IP addresses of all operating Service Nodes on the network and use ISP level firewalls to block connections to those particular addresses. This type of censorship is regularly performed on the Tor network in China [38]. Deep packet inspection (DPI), aims to investigate the structuring of each individual packet that passes through a firewall, and selectively drop or block packets that appear to relate to a particular service. Again, DPI has been used extensively by state-level actors [39].

Much work has been done to design systems which evade DPI. Users can leverage types of pluggable transports which alter the signature of each packet aiming to appear as normal unblocked traffic. IP blocking is generally avoided by running domain fronting bridges which will encrypt traffic as HTTPS requests to unblocked services like Azure or Cloudflare. Once they reach the unblocked service, the bridge will forward the request to the desired location. In the case of domain fronting, it becomes difficult for a state level actor to prevent the flow of all traffic to popular bridges without causing significant disruption to the general usage of the internet.

Governance mechanisms built into Worktips can be used to operate domain fronting bridges so that users can access Worktips services in countries where large-scale internet censorship policies are at play. Additionally, OBFS4 pluggable transport support will be bundled with the Service Node release of the Worktips wallet to help further protect against DPI [40].

7.2 Denial of Service Attacks

Users of decentralised blockchains are not required to provide digital or physical identifiers. This can be beneficial to users who lack identity or are being persecuted because of it. However, systems that do not require identification render themselves vulnerable to Sybil attacks, where a malicious actor produces numerous false identities (in Worktips's case, numerous public-private key pairs) and uses these identities to spam the network with requests.

Many cryptocurrencies have struggled with this problem, and are forced to implement either a fee-for-service model or a proof-of-work model. In fee-for-service models such as Siacoin, users pay for the services that they use. In Siacoins case, the cost is determined per TB of storage per month [41]. Fee-for-service models are effective at reducing Sybil attacks, however, they drive many users away from the system especially when similar services are available for free (such as Google Drive and Onedrive in the case of Siacoin). Proof-of-work systems such as those used in Hashcash and Nano require users to calculate a small proof-of-work before sending a message or transaction [42][43]. These small proof-of-work systems are arguably more egalitarian than the fee-for-service model but can fall prey to attackers who possess large amounts of computing power.

Worktips proposes a modified proof-of-work scheme to address the two largest Sybil attack surfaces in the Worktips system; offline messages and path creation. Offline messages present a potential target because each message must be stored by a swarm of nine nodes. Potential abuse could arise where a malicious user overloads a particular swarm with a high volume of messages that it would have to store. In path creation attacks, the attacker seeks to engage in the path creation process with as many nodes as possible, taking up bandwidth resources and denying service to users who create paths through the network for legitimate purposes.

To prevent both attacks, the Worktips network requires that a short proof-of-work be attached when both messages and paths are created. For messages, this proof-of-work is calculated as a Blake2b hash of the message. For path creation, the proof-of-work is sent along with the request for a node to be included in the path building process. To ensure scalability and accessibility for mobile users, the proof-of-work difficulty requirement is fixed based on the Time-to-live (TTL) of the message or the path, and not based on global network activity.

7.3 Swarm Flagging

When nodes operate in a trustless environment without a centralised leader enforcing overarching rules, maintaining proper node behaviour on the network becomes difficult. Although Service Nodes in Worktips must hold the correct collateral requirement, they may choose to not route traffic or store data in their memory pools. Because this option is financially beneficial (using less bandwidth/CPU cycles/storage), a system of distributed flagging must be proposed to remove underperforming nodes.

For Worktips, such distributed flagging faces major implementation issues. Fundamentally, every Service Node is financially incentivised to flag every other Service Node as a bad actor. This is because when a Service Node is flagged it will face removal from the staking pool and thereby increase the flaggers chance at winning a reward. One potential method of distributed flagging is one in which evidence is provided when a flagging event occurs, however, this solution falls prey to nodes fabricating evidence in their favour. Conversely, flagging without restrictions allows either single nodes or groups of collaborating nodes to intentionally flag honest nodes in order to improve their chances of winning block rewards. To circumvent these issues, Worktips proposes *swarm flagging*.

Swarm flagging works by using existing swarms to choose members that will participate in each testing round. Each Service Node holds a copy of the blockchain, and each block created by a miner will deterministically select a number of test swarms. Every block, 1% of the networks swarms are selected for participation in a testing swarm. To calculate participating swarms, the hash of the five previous blocks is used to seed a Mersenne Twister function which then selects swarms by order of their position in the deterministic list.

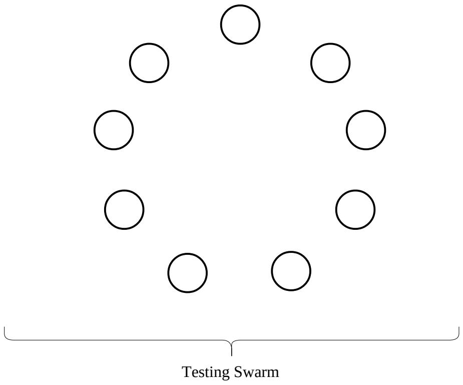


Figure 4: *A testing swarm is a selected swarm of 9 nodes*

When a swarm has been selected to participate, each node in that swarm is expected to conduct a number of tests on every other node in the swarm. These are not active tests; rather each node stores historical information about its interactions with every other node within its swarm. Information about bandwidth, message storage, blockchain requests, and exit node functionality are collected and retained over time. New swarm entrants that have yet to gather this information can query Service Nodes outside of their immediate swarm so as to gather data on each of the Service Nodes they test.

Each Service Node decides how to vote on each of the other swarm members. Once it has made its decision based on the aforementioned tests, it collects and broadcasts its votes to the swarm. Each node in the swarm can now check the votes for all members. If any single node in the swarm has over 50% of the nodes voting against it, any swarm member has the required information to construct a deregistration transaction. Once this transaction is validated and included in a block, all Service Nodes update their DHT, purging any nodes that were voted off.

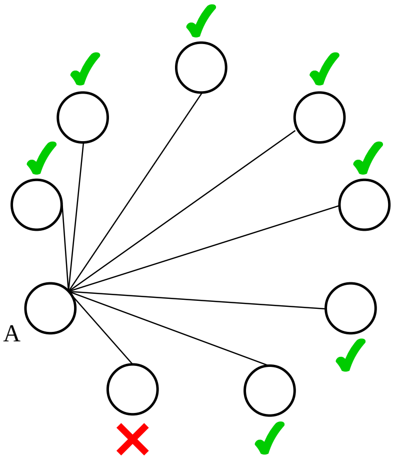


Figure 5: *Dishonest node is tested by node A and fails a test. Node A comes to local understanding of which nodes are failing or passing tests.*

7.3.1 Testing Suite

In order to allow the network to self-enforce performance standards, Service Nodes must be equipped with the required tools so as to test other Service Nodes. These tests should cover the scope of all functionality provided by Service Nodes to prevent lazy masternode attacks [44]. In this initial design, four fundamental tests are proposed. Further tests may be added to the test suite as the function of Services Nodes expands.

When an operator first runs the Service Node software, an empty file with a predetermined size is allocated on disk to ensure that space is present for tasks that require storage. Next, a simple bandwidth test is conducted between the Service Nodes. These checks are optional, and Service Nodes are allowed to skip, ignore or fail them, and join the pool of untrusted Service Nodes. However, running and passing these tests provides a good indicator to any would-be Service Node operator as to whether they should risk locking collateral in a node that may not meet minimum requirements. Once a Service Node joins the untrusted Service Node pool, their collateral is locked and they are tested by the next chosen swarm. Swarm tests are enforced via consensus and new entrants to the Service Node network cannot evade these tests. If a node passes all swarm tests, they are awarded the trusted node flag and can begin routing packets. Failing this, they are removed from the network and their collateral remains locked for 30 days.

Bandwidth Test

The bandwidth test forms the backbone of the Worktips network test suite. If a node passes this test then it is assumed to be honestly routing packets above the minimum threshold.

Each time a node interacts with another Service Node, it will make and retain a record of the incoming bandwidth provided. Over time, nodes will be included in thousands of paths and route millions of messages. These interactions will form the basis of each nodes bandwidth tables. From this table, a node can respond to bandwidth tests about Service Nodes inside its swarm.

All nodes are also expected to respond to queries of their own bandwidth tables from other nodes. This means that even nodes who have recently joined the network can query the wider network for information about any specific node in their swarm.

Blockchain Storage Test

Service Nodes are expected to hold a full copy of the Worktips blockchain. By holding a full copy of the blockchain, Service Nodes can perform a number of tasks that are essential to users of the network including acting as a remote node, validating transactions, and locking transactions in Tachus.

As honest nodes also hold a copy of the blockchain, a dishonest node could avoid holding a full copy by simply requesting blocks from an honest node when tested. To avoid this outcome, the blockchain storage test is designed so that honest nodes that hold a copy of the blockchain can pass this test, while dishonest nodes cannot.

To achieve this, the testing node requests each tested node to make a selection of K random transactions within the history of the blockchain which are then concatenated and hashed. This hash is then be returned to the testing node. By measuring the latency of this request, the testing node can compare the latency with the expected return time T. The exact value for T will be set to accurately differentiate expected latency between loading from disk and downloading blocks from the network. For any attacker, it should be infeasible to download and hash K blocks within T, and thus piggybacking attacks become difficult.

8 Governance, Funding, and Voting

Governance is an essential part of cryptocurrency design and should be supported at the protocol level. The risk of weak, informally defined governance has been studied extensively throughout the history of blockchain technology. Bitcoin and Ethereum experienced contentious hard forks that split the focus and efforts of their respective communities. Although hard forks can be used as a governance strategy, they should always be considered as a last resort rather than the solution to every contentious issue. The Worktips governance system is designed to resolve potential issues by providing a structured environment for discourse and representation, and also to source funding for the development of Worktips without reliance on external influence or altruism.

Beyond the prevention of hard forks, governance structures should create the means to internally fund new projects which improve upon the Worktips ecosystem. Internally funding projects can prevent the formation of special interest groups that do not necessarily have motives that are in line with the users, miners, or Service Nodes. We have seen this in Bitcoin and various Bitcoin forks with the formation of for-profit companies, such as Blockstream, Bitcoin ABC, and Bitcoin Unlimited, that have been frequently accused of hiring developers to make protocol-specific changes to Bitcoin and Bitcoin Cash aimed to further their own business objectives or follow their specific ideology.

It is for this reason that in every Worktips block, 5% of the reward is allocated for the purpose of network governance.

9 Conclusion

Worktips proposes a model for anonymous transactions and decentralised communication built on a network of economically incentivised nodes. Worktips uses the foundations of the CryptoNote protocol to ensure privacy and implements a collateralised node system to enhance network resilience and functionality.

Additionally, Worktips proposes improvements upon previous research and open source projects and presents a new anonymous routing protocol which offers significant advantages over existing protocols. The combination of a unique architecture and protocol design creates a network with market-based Sybil resistance, decreasing the efficacy of temporal analysis, and providing users with a high degree of digital privacy.

References

[1] Mike Orcutt, *Criminals Thought Bitcoin Was the Perfect Hiding Place, but They Thought Wrong* (September 11, 2017), https://www.technologyreview.com/s/608763/ criminals-thought-bitcoin-was-the-perfect-hiding-place-they-thought-wrong.

[2] *Monero*, https://getmonero.org.

[3] *Tor Project*, https://www.torproject.org.

[4] *I2P Anonymous Network*, https://geti2p.net/en.

[5] *LWMA Difficulty Algorithm*, https://github.com/zawy12/difficulty-algorithms/issues/3.

[6] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters, *Twisted Edwards Curves* (2008), https://eprint.iacr.org/2008/013.pdf.

[7] Nicolas van Saberhagen, *CryptoNote v 2.0* (2013), https://cryptonote.org/whitepaper.pdf.

[8] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Trans. Information Theory **IT-22** (1976), no. 6, 644–654. MR0437208

[9] Shen Noether, Adam Mackenzie, and Monero Core Team, *Ring Confidential Transactions* (2016), https://lab.getmonero.org/pubs/MRL-0005.pdf.

[10] Benedikt Bu¨nz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell, *Bulletproofs: Short Proofs for Confidential Transactions and More* (2017), https://eprint.iacr.org/2017/1066.pdf.

[11] Evan Duffield and Daniel Diaz, *Dash: A Privacy-Centric Crypto-Currency*, https://github.com/dashpay/dash/wiki/Whitepaper.

[12] *GitHub - loki-project/loki-network*, https://github.com/loki-project/loki-network.

[13] *Tor Project: Docs*, https://www.torproject.org/docs/faq#KeyManagement.

[14] *Possible upcoming attempts to disable the Tor network — Tor Blog.* (December 19, 2014), https://blog.torproject.org/possible-upcoming-attempts-disable-tor-network.

[15] Petar Maymounkov and David Mazi`eres, *Kademlia: A Peer-to-peer Information System Based on the XOR Metric*, https://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf.

[16] Philipp Winter, Roya Ensafi, Karsten Loesing, and Nick Feamster, *Identifying and characterizing Sybils in the Tor network* (February 25, 2016), https://arxiv.org/abs/1602.07787.

[17] *OSI model - Wikipedia*, https://en.wikipedia.org/wiki/OSI_model.

[18] Farid Farid, *No Signal: Eqypt blocks the encrypted messaging app as it continues its cyber crackdown* (December 26, 2016), https://techcrunch.com/2016/12/26/1431709.

[19] Matt Burgess, *Russia's Telegram block tests Putin's ability to control the web* (April 24, 2018), http://www.wired.co.uk/article/russia-google-telegram-ban-blocks-ip-address.

[20] *Go Ethereum - Postal Services over Swarm*, https://github.com/ethersphere/go-ethereum/blob/ddfc0a2a02ce574f4c252068ce81f0f5ada1c1ff/swarm/pss/README.md.

[21] Nikita Borisov, Ian Goldberg, and Eric Brewer, *Off-the-record Communication, or, Why Not to Use PGP*, Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society, 2004, pp. 77–84, DOI 10.1145/1029179.1029200.

[22] *NaCl: Networking and Cryptography library*, https://nacl.cr.yp.to.

[23] *Pidgin-Encryption - SourceForge*, http://pidgin-encrypt.sourceforge.net.

[24] *Irreversible Transactions - Bitcoin Wiki* (March 15, 2018), https://en.bitcoin.it/wiki/Irreversible_Transactions.

[25] *Scrypt - Litecoin Wiki - Litecoin.info* (February 12, 2018), https://litecoin.info/index.php/ Scrypt.

[26] *Ethash ethereum/wiki Wiki - GitHub*, https://github.com/ethereum/wiki/wiki/Ethash.

[27] *BITMAIN*, https://shop.bitmain.com/product/detail?pid=00020180314213415366s4au3Xw306A4. [28] *Monero Cryptonight V7 - GitHub*, https://github.com/monero-project/monero/pull/3253/files/ e136bc6b8a480426f7565b721ca2ccf75547af62.

[29] Alex Biryukov, Daniel Dinu, and Dmitry Khovratovich, *Argon2: the memory-hard function for password hashing and other applications* (December 26, 2015), https://password-hashing.net/argon2-specs. pdf.

[30] Dan Boneh, Henry Corrigan-Gibbs, and Stuart Schechter, *Balloon Hashing: A Memory-Hard Function Providing Provable Protection Against Sequential Attacks* (2017), https://eprint.iacr.org/2016/ 027.pdf.

[31] *GitHub - A Programmatic Proof-of-Work for Ethash*, https://github.com/ifdefelse/ProgPOW.

[32] *GitHub - hyc/randprog: Randomly generate a C (or javascript) program*, https://github.com/hyc/ randprog.

[33] *GitHub - curie-kief/cryptonote-heavy-design: Cryptonote Heavy deign essay*, https://github.com/ curie-kief/cryptonote-heavy-design.

[34] Surae Noether, Sarang Noether, and Adam Mackenzie, *A Note on Chain Reactions in Traceability in CryptoNote 2.0* (2014), https://lab.getmonero.org/pubs/MRL-0001.pdf.

[35] *Github Comment - EABE/Knacc Attack*, https://github.com/monero-project/monero/issues/ 1673#issuecomment-312968452.

[36] *I2P's Threat Model - I2P*, https://geti2p.net/en/docs/how/threat-model#harvesting.

[37] *Deep packet inspection - Tec Gov*, http://tec.gov.in/pdf/Studypaper/White%20paper%20on% 20DPI.pdf.

[38] Philipp Winter and Stefan Lindskog, *How China Is Blocking Tor* (2012), https://arxiv.org/abs/ 1204.0447.

[39] *Egypt Quietly Blocks VOIP Services Skype, Whatsapp - TorGuard* (October 26, 2015), https:// torguard.net/blog/egypt-quietly-blocks-voip-services-skype-whatsapp.

[40] *GitHub - Yawning/obfs4: The obfourscator (Development mirror)*, https://github.com/Yawning/ obfs4.

[41] David Vorick and Luke Champine, *Sia: Simple Decentralized Storage* (2014), https://sia.tech/ whitepaper.pdf.

[42] Adam Back, *Hashcash - A Denial of Service Counter-Measure* (2002), http://www.hashcash.org/ papers/hashcash.pdf.

[43] Colin LeMahieu, *RaiBlocks: A Feeless Distributed Cryptocurrency Network*, https://raiblocks.net/ media/RaiBlocks_Whitepaper__English.pdf.

[44] *Lazy Masternodes: do you actually have to do any work to get paid/vote?*, https://www.reddit.com/ r/dashpay/comments/5t6kvc/lazy_masternodes_do_you_actually_have_to_do_any/.

[45] *ACNC template constitution for a charitable company*, https://acnc.gov.au/ CMDownload.aspx?ContentKey=2efea0fa-af4f-4231-88af-5cffc11df8b7&ContentItemKey= 6046cbc5-d7fd-4b6b-93ba-c8e3114b07ba.