DAPS WHITEPAPER

V.2.0.2

INTRODUCTION

DAPS is a planned privacy blockchain with a focus on security, scalability and total obfuscation. DAPS is currently hosted on the Ethereum network, pending the DAPS coin main net deployment. The goal of DAPS protocol is to create a fully anonymous staking coin and payment system with a trustless governance structure, a first in crypto-currencies. **DAPS chain verification and consensus will be achieved via Proof Of Audit miners, Masternodes, and Proof Of Stake nodes**.

How will we do that? We have carefully selected certain tested protocols and utilizing these features together will enable a fully private blockchain network. We plan to offer the most complete anonymity package in any protocol to date, with an on-chain solution to the "Trust Problem" that prevents such a fully-private network from being created. Our unique solution to the "Trust Problem" is called **Proof-of-Audit**, which is the keystone to our protocol.

A main goal for DAPS is to anonymize assets and secure an infrastructure for development of further precedent-setting technology. DAPS aims to be more than a coin, but a culture.

WHY DAPS?

In traditional blockchains and various "partial" anonymity chains, the users are exposed to analytics and malicious attack vectors. Many around the world use this exposed data to exploit cryptocurrency users. We aim to preserve everyone's right to control their finances as they see fit. DAPS will merge successful and tested privacy protocols in an attempt to create the most private blockchain to date.

users are exposed to analytics and malicious attack vectors.

HISTORY OF HARPOCRATES (DAPS) PROTOCOL

The Zerocoin Protocol (libzerocoin) is the foundation for many of the privacy coins we see today. Used by other assets to create relatively safe and secure privacy assets, this protocol is highly vetted and is considered the standard for privacy implementation.

Using this privacy foundation, many coins expanded on the Zerocoin (libzerocoin) protocol ideas in many ways, with one notable example being DASH.

The DASH Team created a new layer called "Masternodes" on top of Bitcoin, essentially creating an "incentivized" node that runs 24/7, to strengthen the network and allow additional chain features to be added. These features include Instantsend, Privatesend, and enabling Masternodes to vote on proposals, decentralizing the network's governance out of developer's hands.

"incentivized" node that runs **24/7**

PIVX merged the Zerocoin protocol with the Masternode protocol. PIVX expanded on this concept by enabling a "see-saw reward scheme" for Masternodes, to strengthen Masternode incentives vs staking.

Following the Decentralized Anonymous Payment scheme protocol definition as described by Sasson et al (2014), DAP scheme is described as a method of payment that allows users to make direct, private payments to one another by hiding the origin and destination of the payment including the payment amount. This approach to cryptocurrency employs “zero-knowledge” proofs that prevents analysis of transactions or addresses.

["An obvious way to negate the downsides of the CryptNote protocol... would be to implement hidden amounts for any transaction" -Shen Noether, Ring Signature Confidential Transactions for Monero]

Utilizing proposals and initiatives like RingCT in conjunction with other well-tested features, we hope to achieve complete obfuscation of users. This mix of features, featuring Proof-Of-Audit, will be called the Harpocrates Protocol, providing a trustless completely-anonymous blockchain network.

THE BITCOIN PROBLEM

Bitcoin is not anonymous. By design to prevent double-spends, the blockchain is fully public and visible to anyone. This makes Bitcoin trustless. You do not need to "trust" any bitcoin node operator or the person sending you Bitcoin to be truthful, you can verify the chain status with third party means. You can easily verify your own balances and transactions on a public ledger.

This is one of the ways Bitcoin network secures network health, at the cost of completely exposing the end users to analytics and tracking. But, there is a drawback to this "trustless" (fully transparent) network: Transactions, balances and other data are easily tracked and can used by bad actors. This issue has driven the idea of "private" blockchains to become a focus for the industry.

"PRIVACY" AND SECURITY

Privacy currencies are not fully private. In theory, in a completely anonymous chain, no matter the protocol, node owners can collude off-chain to run their nodes maliciously. This can be disastrous in many ways for any network and represents a built-in security risk to current iterations of private blockchains. If nodes were to collude, generate infinite coins for themselves in secret, and spend them, the world would be unable to discover this as the transactions and balances will be hidden from public view.

As you cannot "roll back" these exploits without causing a chain split, it is critical to be able to detect attacks or off-chain collusion as they happen. How do you verify the status of the network, when the people telling you the status have incentive to be dishonest?

Most teams avoid the idea of private blockchains due to inherent exploitability. This exploitability is caused by the inability to track the network status and emissions by a neutral third party. The most prominent example of this critical weakness is constant exploitation of 'Zerocoin minting' and CryptoNote networks.

WHAT IS THE "TRUST ISSUE"?

WHAT IS THE "TRUST ISSUE"?

To be trustless an objective third party must be able to verify the coin supply, check coin emissions, and make sure nodes are not being used maliciously. We do not believe trusting the honesty of node owners should be the only backstop against malicious actions.

For Masternode-based privacy blockchains, a degree of trust must be given to these "Masternodes" as a central governance of the coin supply, inflation and various specifications. For non-Masternode privacy networks using ZK-snarks, the network requires a complicated deployment ceremony, where a network-controlling piece of information is exposed to a certain small group of members. If these members do not completely delete this data (and do not memorize it) then the network can be entirely controlled by them.

This is the "Trust Issue". You must TRUST nodes or a group of "administrators" and central figures who can control the entire network at a whim. Current iterations of Masternodes and fully private blockchains (Zk-snarks, RingCT with full obfuscation) diverge from the "trustless" status of public blockchains.

Many non-private coins also completely ignore these governance structures and trustless network setups, declaring themselves a fully centralized central-authority dominated network.

We believe these networks are dangerous to blockchain as a whole and violate the principles of Satoshi's vision. No man-made written constitution, agreement, or arrangements can ever be as secure as the fundamentals of a third-party-secured blockchain ledger.

How will we address these issues? Proof-Of-Audit will introduce Trust-less-ness to the Trust-based system of other privacy coins. This will enable deployment of fully private blockchains using currently available tools and can expand to many existing networks.

This will enable deployment of fully private blockchains using currently available tools and can expand to many existing networks.

Proof-Of-Audit can also be used in other non-privacy protocols, to enable a trustless status of their network. Proof-Of-Audit also has the added effect of causing a Proof-Of-Stake/Masternode system to be much more secure, while avoiding the issues of traditional Proof-Of-Work.

The Proof-Of-Audit idea and DAPS Protocol implementation is called the HARPOCRATES Protocol and will set out to be a new industry standard.

DAPS COIN CONSENSUS MECHANISMS: MASTERNODES, STAKING, SEE-SAWS AND PROOF-OF-AUDIT

DAPS Masternodes are required to have 1,000,000 DAPS coin collateral, a dedicated IP address, and be able to run 24 hours a day without more than a 1-hour connection loss. Masternodes get paid using the See-saw method as described in the next section. For offering their services to the network, Masternodes are paid a portion of block rewards to maintain the ecosystem. This payment will be in DAPS and it serves as a form of passive income to the Masternode owners.

The DAPS Masternode system is modelled after the PIVX Masternode system. This has many bonuses, including preventing a 51% attack unless both Proof-Of-Stake and Masternode layers are compromised simultaneously.

The SBRS (See-Saw Balance Reward System) will have a 60/40 MN/PoS reward split balancing to a maximum of 40/60 MN/PoS reward split. This will give a fair reward to holders with too little coins to partake in a Masternode, an issue in many Masternode coin networks.

Chain verification will be done using Proof-Of-Audit, Masternodes, and Proof-Of-Stake (v3). This will give the DAPS network resistances against most known attacks and ensure the chain is secure while allowing it to be publicly scrutinized.

TOR LAYER 

Nodes will be mandatory TOR Hidden Services with .onion addresses to prevent attacks on node operators by tracing IP or port usage.

As some areas block Tor access, OBFS4 will also be implemented so users from these areas may use the DAPS wallet safely. OBFS4 will be mandatory along with TOR Hidden services, to allow anyone to access the network from anywhere. One trade-off of this technology is slower wallet synchronization times on launch, which is acceptable in order to achieve wholly-obfuscated and protected nodes.

MANDATORY STEALTH, OPTIONAL TRANSPARENCY 

DAPS will have a mandatory stealth address system, with private being the default option. Users will be able to send a “public key” at any time, which will reveal the sender and amount sent. The public-key function will enable non-private payments and transparency on the fast and secure DAPS network.

EMISSIONS, FOUNDER'S FEE 

The DAPS coin emissions will be 1050 DAPS per block. There will be a 50 DAPS per block fee ("Founder's fee") allocated to the DAPS Development fund, used to further development and sustain the project long-term.

1000 DAPS Per block will be rewarded to MasternodeS, PoS stakers, and PoA miners.

900 Masternodes/PoS - rebalancing from 60/40 MN/PoS to 40/60 MN/PoS

100 PoA

This will ensure the long-term health of the network by balancing the mining and Masternode vs staking rewards, preventing runaway Masternode growth and disincentivizing mining exploits.

DAPS TOKEN - The Journey to DAPS

The DAPS coin main net, utilizing the features in this whitepaper, is being created now, and is scheduled for early 2019. DAPS is currently an ERC20 token. Details of main net deployment are to be announced.

DAPS TOKEN SPECS:

ERC-20 Token
Supply: 60,000,000,000 DAPS
Distribution: AIRDROP

DAPS COIN SPECS:

Initial supply: 60,000,000,000 DAPS
Supply cap: 60,000,000,000 [initial]+10,000,000,000 [block reward] DAPS
Consensus: Proof-Of-Audit, Proof-Of-Stake v3, Masternodes (See-saw rewards)
Block time: 1 minute
Block reward: 1050 DAPS
Development allocation per block: 50 DAPS
Block reward split: 900 Masternode/PoS (see-saw), 100 PoA
Masternode collateral: 1,000,000 DAPS
See-saw rebalance: 60/40 MN/PoS reward split, up to maximum 40/60 MN/PoS
Confirms required to spend: 4 blocks
Stake maturation: 200 blocks
Approximate emissions: ~551 million DAPS per year until 10 billion DAPS emitted

DAPS CHAIN SPECS:

NODES/IPS

TOR/OBFS4

- Mandatory Tor/OBFS4 relay for all nodes. Hides all node/Masternode IP addresses, which can be used as attack vectors

- Utilize OBFS4, will obfuscate in "blocked" areas. If TOR traffic is blocked, OBFS4 will activate, and mask the Tor layer, allowing normal function. This will allow the DAPS wallet to run anywhere, anytime.

TRANSACTIONS

RINGCT

- RingCT "Confidential Transaction" Ring Signatures, allowing users to increase or decrease the level of obfuscation, with fees scaling according to the level set.

BALANCES 

STEALTH ADDRESSES

RINGCT

- Mandatory stealth address/public address system, allowing users to optionally track certain spending.
- Ring CT will also obfuscate wallet balances

OTHER FEATURES 

- Static emissions: No fancy inflation models, flat emissions
- 10MB Block size: Scalable into indefinite future
- PoSV3: Energy efficient, fair
- Masternodes: Incentivized 24/7 nodes that can be used for advanced features.
- Multinodes: Multiple masternodes per instance. No more server spam!
- Proof-of-Audit: Our unique solution to the Trust Issue of private blockchains and applicable to non-PoW-consensus networks.

Using the above chain features, we hope to completely obfuscate transactions, addresses, balances, and nodes/IP. With a built-in coin supply audit on-chain, the system will be trustless and avoid the "trust" issue of wholly-private coins. This unique mix of features based on a staking network will be called the Harpocrates Protocol and we believe it will change the standard for privacy coins. We believe Proof-Of-Audit can augment and enhance other contemporary protocols as well, making our project's mission beneficial to the industry as a whole.

Additionally, we have other objectives with DAPS as the centerpiece;
-Cross-chain liquidity: A future focus on atomic swaps and innovative cross-chain liquidity solutions.

- DAPS Ecosystem & World: Other initiatives will be undertaken, to spread DAPS with real usage and utility.

NOTES:

- OBSF4 is not as established as TOR
- TOR/OBSF4 increases sync times
- Blockchain size will be significantly larger than similar less feature-heavy chains
- Masternodes are not a trustless governance model, must have auxiliary chain verification ("Audit")
- ZK-Starks will be implemented if breakthroughs are made

Please note that this document is not a prospectus. It was constituted for informational purposes only, to present the Harpocrates Protocol as of 2018. Be aware that no purchase is necessary. You are free to take part in the project or not. It is your responsibility to review the existing laws in your country before buying or joining DAPS. You must read, understand and accept the terms of this document before involving yourself in the project.

Specs and technical information may be subject to change.

Thanks for reading!

DOCUMENTATION:

Bitcoin trustless:

https://keepingstock.net/explaining-block-chain-how-proof-of-work-enables-trustless-consensus-2abed27f0845

Z-cash Trust Problem:

http://weuse.cash/2016/10/28/the-untrusted-setup/

Libzerocoin Protocol:

http://zerocoin.org/media/pdf/ZerocoinOakland.pdf

DAP Protocol, by Sasson et al:

https://blog.acolyer.org/2017/02/21/zerocash-decentralized-anonymous-payments-from-bitcoin/

Masternodes:

https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146943/Masternodes

http://dashMasternode.org/what-is-a-Masternode/

See-saw reward scheme:

https://pivx.org/knowledge-base/see-saw-rewards-mechanism/

Posv3:

http://earlz.net/view/2017/07/27/1904/the-missing-explanation-of-proof-of-stake-version

Ring CT:

https://eprint.iacr.org/2015/1098

Tor/OBFS documentation:

https://github.com/Yawning/obfs4

https://www.torproject.org/docs/onion-services

Stealth Addresses:

https://steemit.com/monero/@luigi1111/understanding-monero-cryptography-privacy-part-2-stealth-addresses

WHITEPAPER

V.2.0.2

By

DAPS