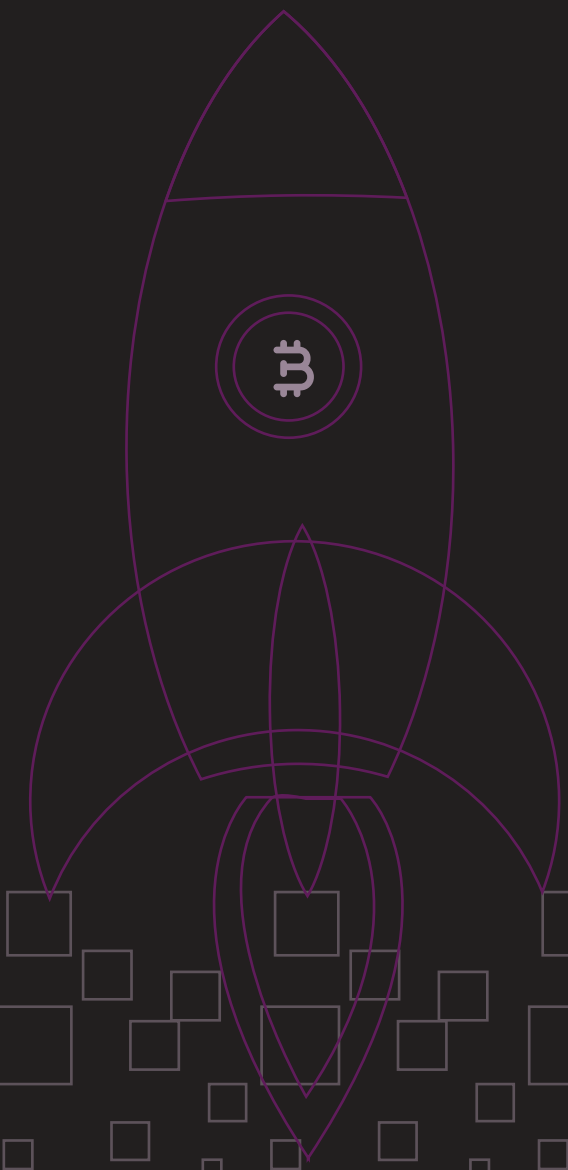
DAPS

WHITEPAPER



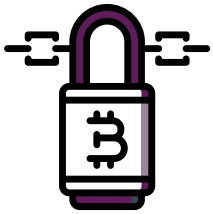
INTRODUCTION

DAPS is a planned experimental hybrid fork-swap of Peepcoin, to be conducted in 2018. The goal of DAPS protocol is to create a fully anonymous coin and eventually payment system with a trustless governance structure, a first in crypto-currencies.
How will we do that? We have crafted a unique blend of tested obfuscation techniques, some redundant, all vetted. We believe this will offer the most complete anonymity package in any Protocol to date, with on-chain Trustless Governance solution, called Proof-of-Audit, a first in the sphere. Utilizing various successful features of competing protocols, we hope to implement a multi-layered and fully anonymous system with mandatory privacy while also removing the "trust issue" of completely private networks.

The legacy of DAPS is rooted in Peepcoin, a coin based on the libzerocoin protocol with anonymity features removed. We will be enabling these features, running on DAPS network, and allow Peepcoin holders to swap to this new chain upon completion. The swap will be credited on a 1:1 basis at a to-be-confirmed (TBC) date.

A main push for DAPS is to anonymize assets, and secure an infrastructure for development of further features. DAPS aims to be more than a coin, but a culture.

WHY DAPS?



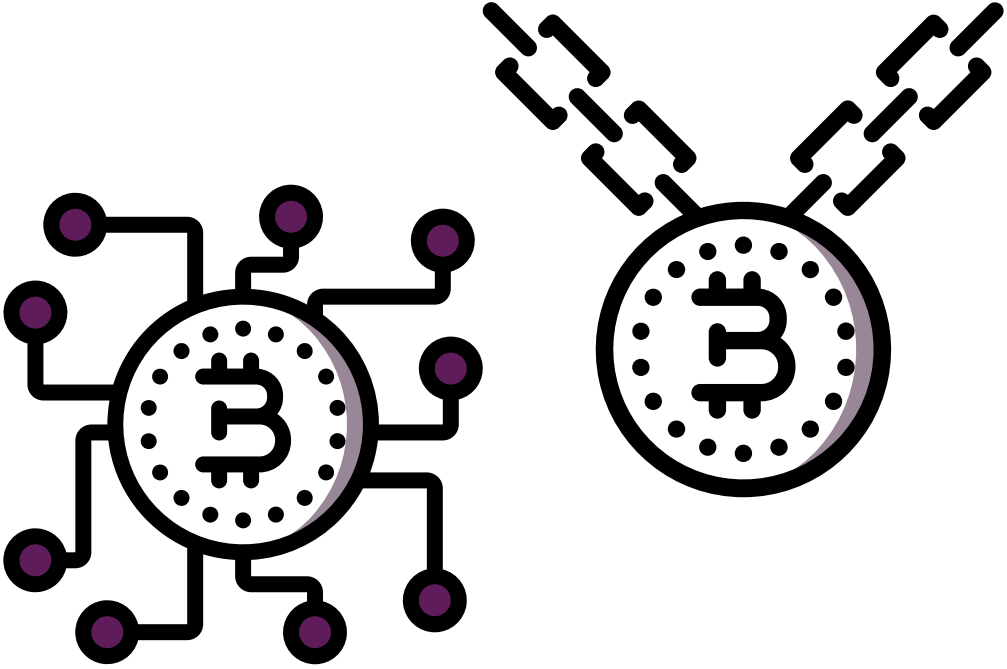
In traditional blockchains and various "partial" anonymity chains, the users are exposed to analytics and malicious attack vectors. Oppressive governments around the world use this data to track and punish cryptocurrency users. We aim to preserve everyone's right to control their finances as they see fit.

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 in various ways, with one notable example being DASH.

The DASH Team created a new layer called "Masternodes" on top of this Zerocoin Protocol, 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. 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

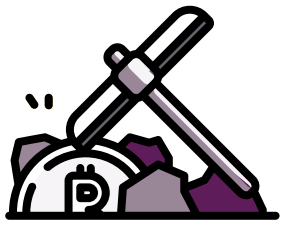
to directly make payments to one another privately by hiding the origin and destination of the payment including the payment amount. This approach to cryptocurrency employs “zero-knowledge” proofs that prevents analysis of transactions or addresses.

Utilizing proposals and initiatives like RingCT in conjunction with other vetted features, we hope to achieve complete obfuscation of users in a trustless network.

["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]

This mix of features and protocol will be called the Harpocrates Protocol, providing a trustless, completely anonymous network.

THE BITCOIN PROBLEM



Bitcoin is not anonymous. By design to prevent double-spends, the blockchain is fully public and visible to anyone. This data is easily tracked and used by unscrupulous actors. This makes Bitcoin trustless, i.e. you do not need to "trust" any bitcoin node operator, you can verify the chain status with third party means. This is one of the ways Bitcoin network secures network health, at the cost of complete monetary exposure.

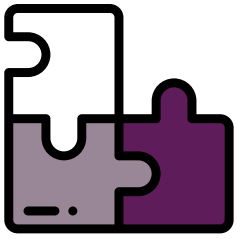
MAKING TRUSTED TRUSTLESS

Privacy currencies are not fully private. The only "fully private" chain is Zcash, which is not a trustless system. To become a fully private blockchain, a degree of trust must be given to the "Nodes" (Masternodes/Nodes) as a central governance of the coin supply, inflation and various specifications. This is the "Trust Issue" of completely private coins.

In a completely anonymous currency, node operators can collude off-chain to generate infinite coins (Zcash Hyperinflation Hack) in secret with no third party to verify if the chain is under such attack. As you cannot roll back changes, it is critical to be able to detect any such attacks or collusion as they happen and not after the fact like with Zcash's Zerocash protocol.

To introduce a degree of Trust-less-ness to the Trust system of a completely private coin is a sea-change in how privacy coins can be handled. This on-chain Trustless Trust solution will be called Proof-Of-Audit.

WHAT IS THE "TRUST ISSUE"?



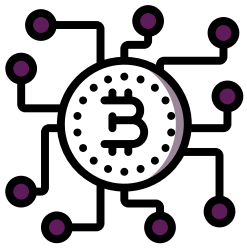
In a completely anonymous private coin network, you must trust the nodes to be working in good faith. There is no outside verification for transactions, balances, or emissions. To know how the chain is doing, you must be given information from "Trusted Nodes". How do you verify the chain's authenticity when the watchmen are the people who tell you the chain's status? It is a question major privacy coins have setup commissions to handle. This is the "Trust Issue" of completely anonymous crypto-currencies, since you have to trust the node operators are working honestly.

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 previous iterations of wholly private networks. 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.

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.

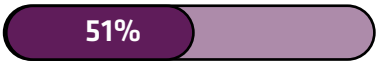
The Harpocrates Protocol will have a hard coded solution to the "Trust Issue" elegantly using the protocols already available. More details about this will be released in it's own white paper.

MASTERNODES AND YOU



APS Masternodes are required to have 1,000,000 DAPS 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 modeled after the PIVX Master node system. This has many bonuses, including preventing a 51% attack unless both 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.

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 countries block Tor access, OBFS4 will also be implemented so that users from these countries can continue to use the wallet as they wish. 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 nodes.

MANDATORY STEALTH

DAPS will have a public and a private address system, with private being the default option. Users will be able to create public addresses at any time, with a dynamic stealth address allocated to the public address on time of receiving transaction, being re-hashed on completion.

EMISSIONS, FOUNDER'S FEE, SPECS

Additionally, Posv3 will be integrated, with block rewards set to 1050. This is inspired by the Bitbean capped staking system, and will result in staking being more fair long term.

To help secure a development infrastructure, 5% of DAPS emissions will be used in the DAPS Development Fund, which will be split between DAPS Core and the DAPS Foundation to utilize for their respective missions. More information about DAPSCore and DAPS foundation will be released on future date.

DAPS COIN SPECS:

1:1 Fork-Swap of Peepcoin (1 DAPS for every Peepcoin)
Pure Proof of Stake with auxiliary PoA (Proof-Of-Audit) block
Block time: **1 minute**
Block reward: **1050**
Confirms required to spend: **4 blocks**
Stake maturation: **200 blocks**

Pure Proof of Stake - **1 "Proof-Of-Audit" block per hour**
Masternode collateral: **1,000,000 DAPS**
60/40 MN/PoS reward split, rebalance up to **maximum of 40/60 MN/PoS**

Initial coin supply: **10-50 billion DAPS**, if all Peepcoin swaps.
Development premine: **1 billion DAPS**, allocated **50%** to Airdrop and **50%** to Development/Outreach
Ongoing founder fee: **30%** airdrop fund, **50%** development fund, **20%** other
SWAP Process: Automated, no outside access, no development access to "Swap" Premine
DAPS daily emissions: **1,486,800 DAPS**, forever
DAPS emitted per year: **542,682,000 DAPS**, forever
Dynamic PoS%: **4-12%** annually, factor of difficulty and luck

DAPS CHAIN SPECS:

HARPOCRATES PROTOCOL

SECRECY - FULL CONFIDENTIALITY - TRUSTLESS

NODES/IPS

- Mandatory Tor relay for all nodes

  Hides all node/masternode IP addresses, which can be used as attack vectors
- Utilize OBFS4, will obfuscate in "blocked" countries

If TOR traffic is blocked, OBFS4 will activate, and mask the Tor layer, allowing normal function. This will allow the DAPS wallet to run on any network, anywhere.

TRANSACTIONS

- Privatesend, using CoinJoin++

  Coins will be mixed before all transactions, powered by Masternodes
- ZK-snarks

  All transaction metadata is completely encrypted
- Ring CT (confidential transaction)

  Hide amount sent or staked in raw TX

BALANCES

- Mandatory stealth address

  Stealth/Public address system, with STEALTH address dynamic for PUBLIC address, preventing tracking STEALTH address
- Ring CT, obfuscate address

  Ring CT will also obfuscate wallet balance

OTHER FEATURES

- PoSV3 - Energy efficient, fair
- Static emissions - No fancy inflation models, flat emissions
- 10MB Block size - Scalable into indefinite future
- Masternodes
- On chain supply "audit" - address "Trustless Trust" issue of wholly-private network - The Harpocrates keystone. This will be called "Proof-Of-Audit". As details of this are highly confidential, we will not release this information until it is implemented to prevent copycat

Protocols from emerging in other competitors.

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. Released under the MIT license, this unique mix of features will be called the Harpocrates Protocol and we believe it will change the standard for privacy coins.

As total Decentralization is the long term goal, future feature pushes will include cross-chain/off-chain swaps (Atomic Swaps) to help remove the influence of exchanges on the market.

Notes:

- OBSF4 is not as established as TOR, possible weaknesses
- TOR/OBSF4 increases sync times, trade-off for anonymity
- CoinJoin/Privatesend may be redundant with Stealth Addresses, will decide if performance trade-off is worth implementation
- Masternodes are not a Trustless governance model, must have auxiliary chain verification ("Audit")

Please note that this document is not a prospectus. It was constituted for informational purposes only, in order 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.

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

Daps

WHITEPAPER