DAPSCOIN

DECENTRALIZED-ANONYMOUS-PAYMENT-SYSTEM

WHITEPAPER 2019

«Privacy is a right, not a privilege»

INTRODUCTION

DAPS is a planned privacy blockchain with a focus on security, scalability and total privacy. The goal of DAPS protocol is to create a fully anonymous staking coin and payment system with a trustless governance structure, based upon the latest technologies derived from both Monero and PIVX. This is a first in crypto-currencies. DAPS chain verification and consensus models will be based upon PoS nodes (staking and Masternodes) and PoA miners.

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". 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. Privacy is a right, not a privilege.

DAPS is proud to say that at the time of writing this whitepaper, we are the first coin to successfully implement a Staking and Masternode hybrid (PoW - PoS - PoA) full privacy chain that fully incorporates RingCT and Bulletproofs.

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.

Another methodology that has proved extremely robust and successful is RingCT as implemented by Monero.
Below is an excerpt and link to the paper.
["An obvious way to negate the downsides of the CryptoNote protocol... would be to implement hidden amounts for any transaction" - Shen Noether, Ring Signature Confidential Transactions for Monero]

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

Not all privacy currencies are 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"?

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, Ring CT 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 Trustlessness 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.*

WHAT MAKES US DIFFERENT?

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

Utilizing the following key technologies:

- **Ring CT**
- **Bulletproofs**
- **Stealth Addresses**
- **Stealth Transactions**
- **Proof of Audit**

We achieve complete obfuscation of all users and transactions. This mix of features, featuring Proof-of-Audit - which we call "The Harpocrates Protocol" - creates a completely trustless anonymous blockchain network.

DAPS OVERVIEW

DAPS is a hybrid PoW-PoS-PoA (Proof-of-Audit) blockchain system that focuses on the privacy of the users. DAPS offers the following unique features:

- A privacy-focused blockchain system that ensures every user transaction in the network is kept private. It means that even though all user transactions are fully published to the blockchain, no third-parties (except the sender and the receiver of the transaction) can reveal the detailed information within the transaction. Specifically, the following information is kept private in DAPS system:
  - Transaction sender: the sender of the transaction is totally obfuscated
  - Transaction receiver: besides one time-generated public keys as the receiver in the transaction, no third-party can reveal the identity of the transaction receiver and the relationships between the receiver public key and the identity of the receiver.
  - Transaction amount is encoded that no third-party can reveal the transaction amount within the transaction.
- A hybrid blockchain system that is composed of different block types in the same blockchain:
  - 500 initial blocks are PoW blocks which are mined by the DAPS foundation to provide the initial supply, which is stated in DAPS whitepaper.
  - From the 501st block, DAPS blockchain becomes a hybrid of PoS and PoA blocks. PoS blocks are continuously minted by staking nodes to verify transactions from users of the DAPS blockchain. A PoS block is created every minute.
  - PoA blocks have a 1-hour block-time. The PoA blocks are mined by external actors in order to audit that the system has been functioning correctly to the specified rules. A PoA block must re-audit at least 59 PoS blocks for its correctness. For this work, PoA block miners are also rewarded to continue auditing the system.

DAPS COIN CONSENSUS MECHANISMS: MASTERNODES, STAKING NODES 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.

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

While DAPS is trustless, there still needs to be an element of trust.
Masternodes on any Masternode chain are seen as a trusted node. This is due to the collateral in coins that is locked away as part of collateralization transaction for the Masternode to be considered trusted. DAPS is by design, anonymous with hidden transaction amounts. This presents a specific problem when collateralizing a Masternode and ensuring that the collateral is correct and locked away.
Therefore all collateralization transactions for Masternodes have a visible amount that is neither Bulletproofed nor part of a Ring signature either.
As soon as the Masternode is de-collateralized, the UTXO that was collateralized is sent back to the designated wallet and is treated as a normal transaction.

MANDATORY STEALTH

DAPS has a mandatory stealth address system and all amounts in user transactions are hidden by means of encoding. While creating a transaction, the sender generates a transaction public key per UTXO, which is then used for generating a one-time generated public key (corresponding to a bitcoin address). The private key of the latter is then only derived by the receiver of the transaction, who has private spend and view keys (described later). Transaction amounts are encoded using a symmetric encryption scheme which uses the Elliptic-Curve Diffie Hellman ECDH to encode the transaction amounts, which can only be revealed by the sender and the receiver of transaction. The transaction public key will allow the holder of the generated private key to reveal only the amount of that transaction. No other transaction can be unlocked with the same key.

EMISSIONS

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.

The fee structure will be as such:
1050 emissions per PoS block
50 DAPS to the development fund
900 to be split between the staking node that minted the block and a Masternode
60/40 see saw system means 540 / 360 split as above
100 reserved for the PoA miner that audits the block

The “See-Saw Balance Reward System” is a method by which the network balances out the percentage of the reward paid out to the staking and master nodes.
If there are 1000 MN and 1000 staking nodes, the system sees that as equal and keeps the 60/40 See-Saw system in favor on Masternodes. This is because they have “invested” the 1 million DAPS by collateralizing their Masternode.

If the node numbers shift drastically in the direction of more Masternodes, the network rebalances the equation to be 40/60, this time favoring the staking nodes.

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

DAPS TOKEN SPECS:

ERC-20 Token
Supply: 60,000,000,000 DAPS
Distributed: via AIRDROP

DAPS COIN SPECS:

Initial supply: 60,000,000,000 DAPS
Supply cap: 60,000,000,000 [initial]+10,000,000,000 [emission] DAPS Consensus: Proof-Of-Audit, Proof-Of-Stake v3, Masternodes (See-saw rewards)
Privacy techniques: Secp256k1-based Ring Signature, RingCT, and range proof Bulletproof
Block time: 1 minute
Block reward: See Emissions above
Confirms required to spend: 4 blocks
Stake maturation: 100 blocks
Approximate emissions: ~551 million DAPS per year until 10 billion DAPS emitted

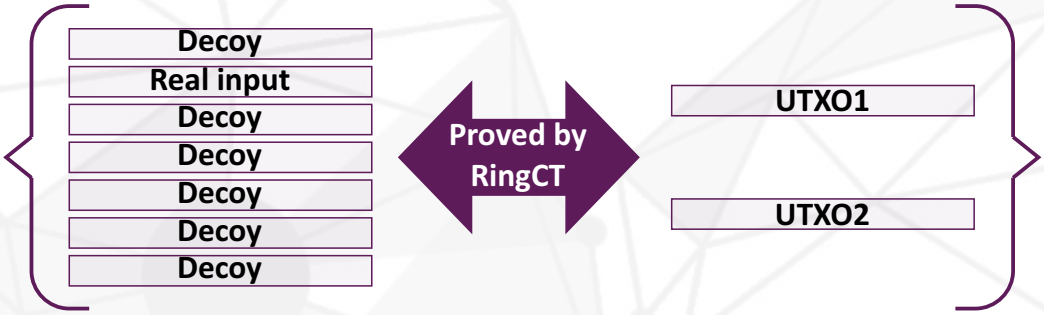
DAPS CHAIN SPECS:

RINGCT

RingCT or "Ring Confidential Transaction" is a way of mixing in a real transaction with a predetermined number of fake transactions. The Ring size determines the number of additional fake transactions that are added.
This means that the actual transaction is hidden within a mixture of fake transactions and thus the true transaction and its amount are much harder to discern.

Whereas Monero has implemented a set ring size - currently 11 - DAPS will have a randomly generated ring size per transaction within a given range (6 -12). This allows the network to be even more secure by ensuring that the user does not always select a specific size thus creating traceability through habit.

While Ring Signatures hide the true UTXOs used as inputs in a transaction (see the following figure) and detects any double spend, RingCT allows fullnodes to prove that the sum of transaction input amounts are equal to the sum of UTXO amounts plus the transaction fee. This is important because all transaction amounts in DAPS are hidden by default and only exist in the form of Pederson commitments and encoded amounts. RingCT does not require the revealing of transaction amounts, while still being able to prove that sums on both input and output sides are equal. The following figure shows how Ring Signature and RingCT are used together.



DAPS CHAIN SPECS:

BULLETPROOFS

Bulletproofs are short non-interactive zero-knowledge proofs that require no trusted setup. A Bulletproof can be used to convince a verifier that an encrypted plaintext is well formed. For example, prove that an encrypted number is in a given range, without revealing anything else about the number. Compared to SNARKs, Bulletproofs require no trusted setup. However, verifying a Bulletproof is more time consuming than verifying a SNARK proof.

Bulletproofs are designed to enable efficient confidential transactions in Bitcoin and other cryptocurrencies. Confidential transactions hide the amount that is transferred in the transaction. Every confidential transaction contains a cryptographic proof that the transaction is valid. Bulletproofs shrink the size of the cryptographic proof from over 10kB to less than 1kB. Moreover, Bulletproofs support proof aggregation, so that proving that m transaction values are valid adds only O(log(m)) additional elements to the size of a single proof. If all Bitcoin transactions were confidential and used Bulletproofs, then the total size of the UTXO set would be only 17 GB, compared to 160 GB with the currently used proofs.

DAPS uses Bulletproofs as range proofs to prove transaction amounts in the transaction are positive. This is critical because secp256k1 works under a circle space number and there is no way that a fullnode can verify that the encoded amounts are always positive. Without Bulletproofs checking transaction amounts are positive, an attacker can create a transaction with a UTXO having huge positive amount while the other UTXO having a negative amount and the sum of these two amounts plus transaction fees equal to the sum of inputs, which result in bypassing the RingCT check.

DAPS CHAIN SPECS:

STEALTH ADDRESSES

Stealth Addresses, just like Stealth Transactions are another cornerstone of DAPS.
Where standard addresses are fairly easy to read and can be easily identified such as:
3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

DAPS stealth addresses are quite different. The following is an example of a DAPS public address

41k8JcYj2EG4eDHbpPNneDdKvFqHFpQNMMGykRUorNnihiY4RaRNdLiUUfThfzugo5auHkq
ThwQgZ3EixmxyoDkj17c7Qy6BVWP

We call these "Privacy Accounts".

One might argue that if this address is public, how is anonymity achieved then?
In DAPS, if a sender wants to send to a recipient, the recipient's public address will then be used for generating a one-time generated public key/address based on a transaction public key generated by the sender per UTXO.

The particularity of this scheme is that while generating this one-time generated public key, the sender has no way to generate the corresponding private key to redeem the UTXO later. Such private key can only derive by the owner of the public address, who has both pairs of private keys in our dual-key system explained as below.

DAPS PUBLIC ADDRESS DUAL-KEY SYSTEM

DAPS use a dual key system to provide stealth addresses to obfuscate addresses.
A public address is derived from a private view-spend key pair. A public address can contain optionally payment ID, which is usually used by exchanges.

DAPS uses the EC secp256k1 curve to derive public keys from corresponding private keys.

Field	Description
Header	1-byte length. Header = 19 if it is an integrated address, otherwise Header=18
Public spend key	Public spend key in compressed form, whose length is 33 bytes.
Public view key	Public view key in compressed form, whose length is 33 bytes.
paymentID	8-byte field used by exchanges for recognizing transactions from different users
Checksum	4 first bytes of the hash of the above fields

DAPS CHAIN SPECS:

Public address is encoded in base58 format for every 8-byte block of the public address as follows:

- Normal public address: 71 bytes, divided into eight 8-byte blocks and a single 7-byte block. Each address block is encoded in base58 format, resulting in 11 base58 characters per address block => 99 Base58 characters
- Integrated address: 79 bytes, divided into nine 8-byte blocks and a single 7-byte block, resulting in 110 Base58 characters.

STEALTH TRANSACTIONS

The Public address/integrated address of the receiver for a transaction should be sent to the sender, whose wallet does the following steps to create a fully private transaction:

- Parse the public address to extract public view key Pv, public spend key Ps, and payment ID (optional) of the receiver
- Check whether the wallet has enough balance to send
- Generate a one time-generated public key P for the receiver as follows:
  - Generate a transaction private key Ts and its corresponding transaction public key Tp
  - P = H(Ts*Pv) * G + Ps where
    - H is a hash function
    - * and + are the multiplication and addition in secp256k1 curve
    - G is the base generator point in secp256k1 curve
  - A one-time-generated public key is generated per transaction output in the being made transaction. Each transaction output has a different transaction private key to avoid any non-redeemable funds with ring signature described as below.
- Create a transaction output with destination as the above one time-generated public key and the expected sending amount
  - Create a Pederson commitment for the transaction output
  - Generate Elliptic Curve Diffie Hellman secret ECDHS
  - Encode transaction output amount with the ECDHS secret
  - Generate bulletproof for the transaction output amount
- Select a set of spendable UTXO to be transaction inputs
  - Compute transaction fee based on an estimated fee
  - Compute the change = Sum of transaction inputs - sent amount - transaction fee
  - Make transaction fee explicit in the transaction
  - Generate key images and put it in the transaction input
- Generate ring signature
  - Generate the random number of rings Ring _Size (6-12)
  - For each transaction input, select Ring _Size decoys
  - Compute multikey ring signature based on Monero RingCT and Ring signature

MASTERNODES AND STAKING NODES IN DAPS

In masternode-based systems such as PIVX, masternodes are rewarded for providing additional services such as "instant send" and the rewards are sent to the address which has the collateralized coins. If such a mechanism were used in DAPS, funds for masternodes would be lost because Ring Signatures would detect or mark a transaction as double spend even if two different UTXOs from the same address are spent in the transaction. This means that only one of masternode UTXO rewards can be redeemed if the rewards are sent to the same address.

DAPS is designed for such masternode incentive mechanism to generate a new address/public key every time the masternode is rewarded. DAPS does it by requiring users to push the public address (the long address) to the collateral transaction. The masternode public address will be put in the payment queue. During creation of a PoS block, a staking node will then take one of the public addresses in the queue and generates a one-time generated public key for masternode payment. This will ensure that masternode UTXO rewards will be all spendable.

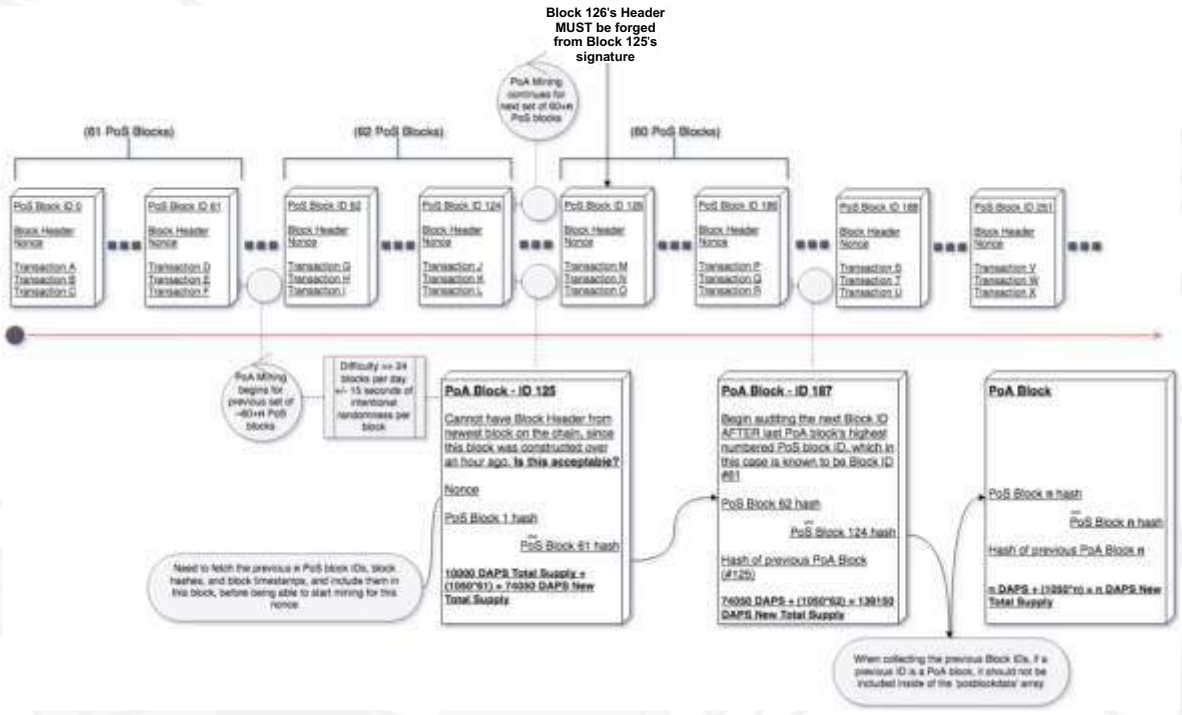
This mechanism is also applied to the staking node while creating PoS blocks to ensure all staking rewards are sent to different public keys.

POA AND POS CONSENSUS DETAILS

1. No PoA block shall be accepted onto the chain unless at least 59-60 minutes have elapsed since the timestamp of the previously accepted PoA block. *This should ensure that PoA blocks remain spaced out across the chain and cannot end up back-to-back-to-back for any reason.*
2. A PoA block must contain the hash of the previous PoA block, thus forming a continuously stranded sub-chain-of-PoA-blocks.
3. A PoA block must not include another PoA block's hash, height, or timestamp in its own `posblocksaudited` array.
4. Every block hash included in posblocksaudited must be a valid hash of a PoS block that can currently be seen on the chain.
5. Every block timestamp included in posblocksaudited must be from a time that is earlier than the PoA block's own timestamp. No PoA block is allowed to audit blocks that have occurred after itself.
6. A PoA block is not allowed to audit a PoS block hash that another PoA block has already audited.

A PoA block can be added to the chain at any time. This allows for PoS blocks to carry on with their minting process uninhibited, and a PoA block would have to select a certain number of existing, sequential PoS blocks to audit, make a record of their block IDs + block hashes + timestamps as a relational list ordered by block ID, and then add itself to the chain as the next block ID in line.

Future PoA blocks look up the previous PoA's block ID, look inside it for the highest numbered PoS block ID, and then begin their audit process, taking into account that if any of those block IDs are a PoA block, they should be ignored.



«Privacy is a right, not a privilege»

TOR/OBFS4

Previous versions of this whitepaper made mention of the usage of TOR and OBFS4.
After extensive investigation, a decision has been made to exlude these from the technology stack for now.
The reasons for this are simple yet carry significant weight.
TOR is blocked by many ISP's globally, requiring extensive setup procedures to "bridge" communications, this may lead to many people not wanting to use DAPS because of a large barrier to entry.
Another issue relating to ISP's and TOR is that many ISP's - upon seeing someone using TOR, regardless of the reason - will either warn the person not to do it again otherwise their account may be closed or just simply close the account without warning. Either way, this is bad and sometimes may even end with a visit from law enforcement. This is not something we want for our users.

We are actively investigating TOR in depth and the general consensus is that we may introduce TOR as "optional" in a future release.
Because these are peripheral systems using TOR, the chain will not need to be reset, split or forked for this.

OTHER FEATURES

- Static emissions: No fancy inflation models, flat emissions
- Up to 2MB Block size
- Masternodes: Incentivized 24/7 nodes that can be used for advanced features.
- Multinodes: Multiple masternodes per instance. No more server spam!

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.

- DAPS Ecosystem & World: Initiatives will be undertaken to incorporate DAPS with real usage and utility to stimulate mass adoption.

NOTES:

Please note that this document is not a prospectus. It was constituted for informational purposes only, to present the DAPS Coin project as of 2019. 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.
DAPS completed a successful testnet in March 2019.
DAPS will undergo a third-party code audit before mainnet release.

DOCUMENTATION:

Bitcoin trustless

Z-cash Trust Problem

Libzerocoin Protocol

DAP Protocol, by Sasson et al

Masternodes

Masternodes

See-saw reward scheme

Posv3

Ring CT

Bulletproofs

Stealth Addresses