Incognito

The privacy layer of the decentralized web.

White Paper Draft v0.2

June 20, 2019

Intro

Crypto networks have introduced an entirely new asset class: crypto assets. Bitcoin was the first crypto asset; today there are over 1,600. People have started buying bitcoin, instead of gold, as their long-term store of value. Stored under the mattresses of volatile economies, the world's most desirable fiat currencies are being replaced by stablecoins, that can be sent and received with borderless freedom. Waves of startups now sell crypto assets to investors, not equity.

For those who value privacy, crypto assets come with a big tradeoff. Transactions are recorded on a public ledger, displaying amounts involved, inscribing virtual identities of their senders and receivers. Given the choice, we strongly believe that very few people will willingly disclose their crypto financials to the entire world.

Incognito offers anyone the option to turn on privacy mode in this new world of crypto networks.

Incognito

Incognito is a decentralized privacy network composed of hardware, software, and a new blockchain protocol.

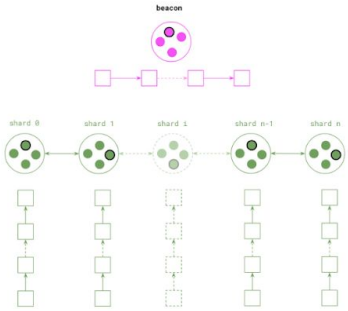
- **Blockchain.** Incognito's privacy-preserving sidechain can be attached to any commonly used blockchain, such as Bitcoin or Ethereum, enabling users to store, send and receive crypto assets, like BTC and ETH, with total privacy.

- **Hardware.** Incognito's low cost, efficient and streamlined mining hardware removes typical barriers to entry. It allows for anyone to become a validator and earn passive income, paid out in various crypto assets such as BTC and ETH.

- **Software.** Incognito's wallet is a simple and secure tool for anyone to manage their crypto assets confidentially. It's available on Android, iOS, and Chrome Extensions.

Hardware

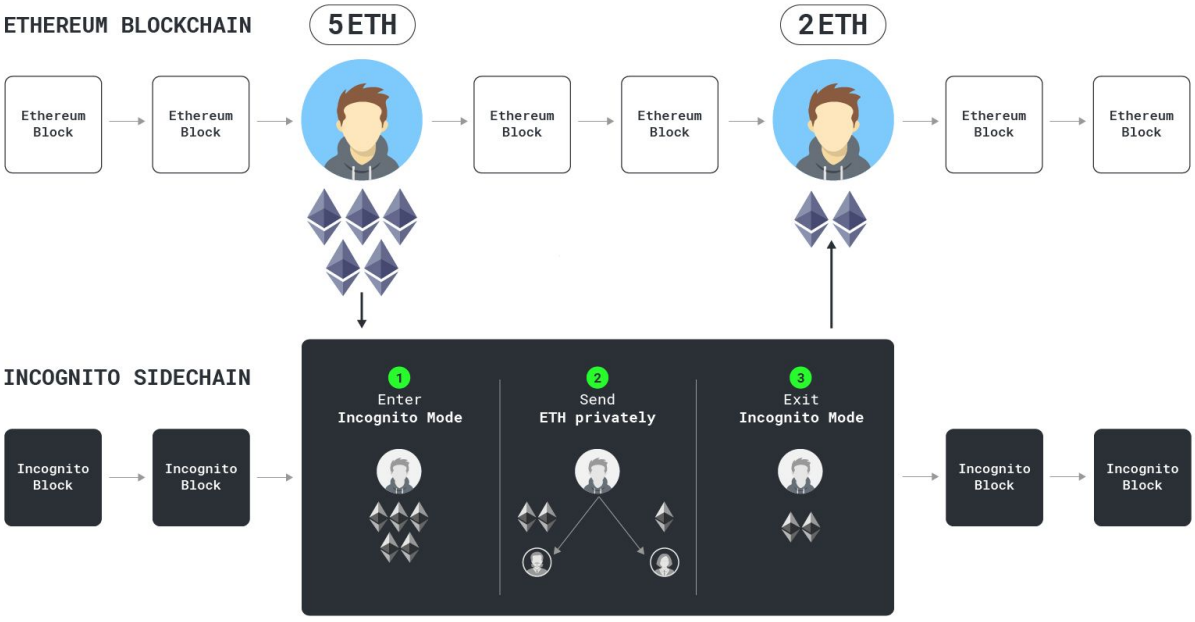
Software



Blockchain

Blockchain: A privacy-preserving sidechain

Incognito's privacy sidechain can be attached to any blockchain to conduct confidential asset transfer. The Incognito sidechain runs parallel to the main blockchains, allowing for secure two-way transfers of crypto assets whenever privacy is needed.



Tokens

There are 3 types of tokens:

- **Privacy.** Privacy (PRV) is Incognito's native token — a work token[1]. Users stake Privacy to become miners. Miners earn block rewards in Privacy and transaction fees in various crypto assets (i.e. BTC, ETH, etc).

  This model avoids speculators and only attracts people interested in growing the network. If the demand for private transactions grows, miners will earn more revenue, which naturally triggers an increase in the price of Privacy.

- **Private tokens.** Anyone can convert tokens on other blockchains (i.e. BTC, ETH, DAI) to private tokens on Incognito (i.e. pBTC, pETH, pDAI). Private tokens maintain 1:1 peg and are completely confidential. Because of this, anyone can store, send and receive any crypto assets with total privacy.

  Private tokens can be used to pay for transaction fees.

- **Custom tokens.** Anyone can issue their own privacy-preserving token on Incognito.

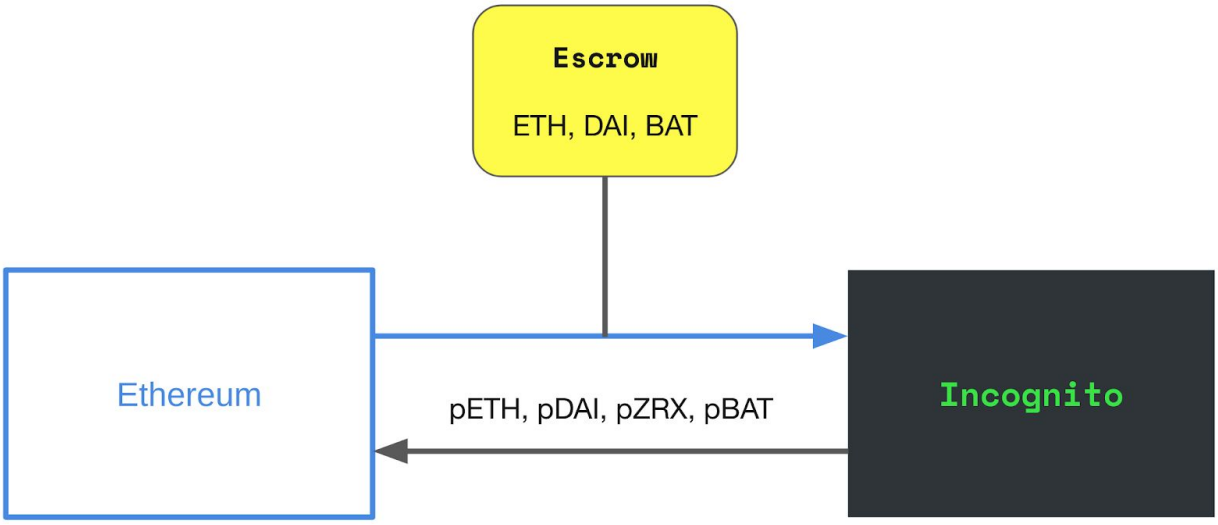
Fees

Users can pay the transaction fees in any cryptocurrencies of their choice (PRV, pBTC, pETH, pDAI, etc).

Bridges

Bridges are mechanisms that allow tokens from one blockchain to be securely used in Incognito sidechain and then be moved back to the original chain if needed. There are fundamentally two types of bridges: **custodial bridges** and **noncustodial bridges**.

[1] https://multicoin.capital/2018/02/13/new-models-utility-tokens/



Incognito is implemented with a mixture of custodial bridges and noncustodial bridges. The key difference between custodial bridges and noncustodial bridges is in the management of the escrow.

- **Custodial bridges.** The funds are managed by independent third parties. Currently, two trust companies are managing the funds: Bitgo[2] for crypto asset custody (insured up to $100M) and PrimeTrust[3] for fiat custody (insured up to $130M).

- **Noncustodial bridges.** The funds are held in trustless smart contracts which run as programmed, without anyone's intervention. Our preference is to implement noncustodial bridges whenever it's possible.

Regardless of the difference in the management of the escrow, in both cases, the Incognito team never touches the funds. Incognito users work directly with either trust companies or smart contracts.

Hardware: A low-cost mining device for everyone

At launch, Incognito will ship its own mining hardware, because of the following reasons:

- **Broaden the validator base.** We want non-technical users to participate too. With good software + hardware UX, non-technical users can simply stake and become a validator via their phone.

[2] https://www.bitgo.com/
[3] https://primetrust.com/

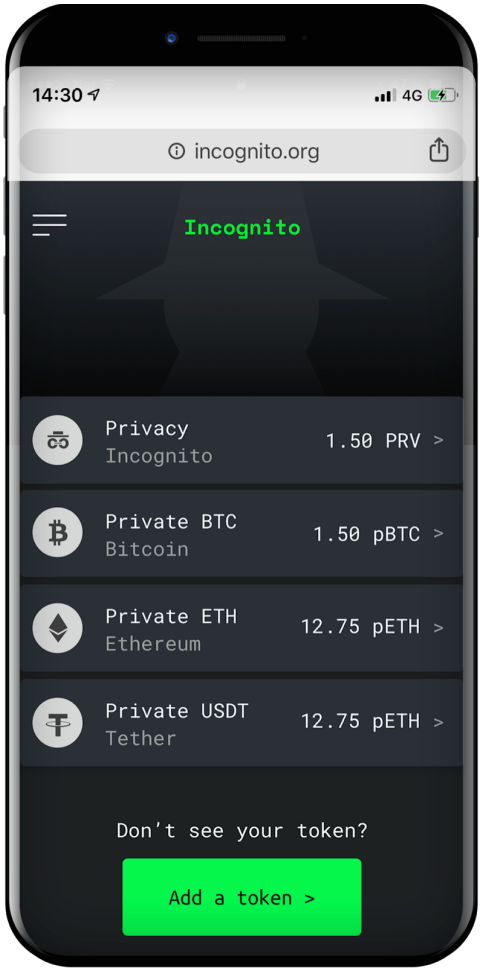
- **Make it cheaper to become a validator.** By producing mining devices in large batches, we reduce both the hardware manufacturing cost and the software maintenance cost significantly and pass them on directly to validators.

- **A better token distribution mechanism.** Our team wants to build a thriving, engaging community. Instead of doing a public token sale, which most likely will attract speculators, our team opts to preload Privacy tokens initially in Incognito hardware, which will start adding value to the network right away.

By shipping low-cost, easy-to-use hardware, we hope that we can get a lot more people to become validators, and therefore make Incognito more decentralized.

Software: A simple, secure privacy-preserving wallet

Incognito provides simple, fast and secure mobile wallet apps on iOS, Android and Chrome Extensions. Users hold their own keys and sign all transactions locally. Our team has made significant efforts to implement high-performing zero-knowledge proof generation on the client side.



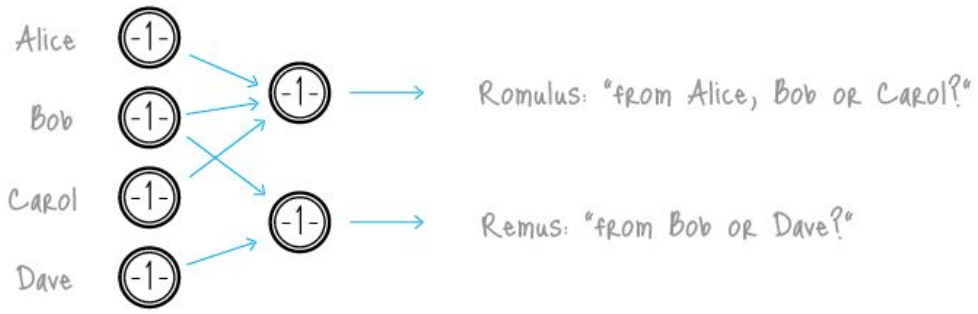
Privacy

Incognito privacy is implemented based on CryptoNote[4] and Bulletproof[5].

Ring signature: untraceable sender

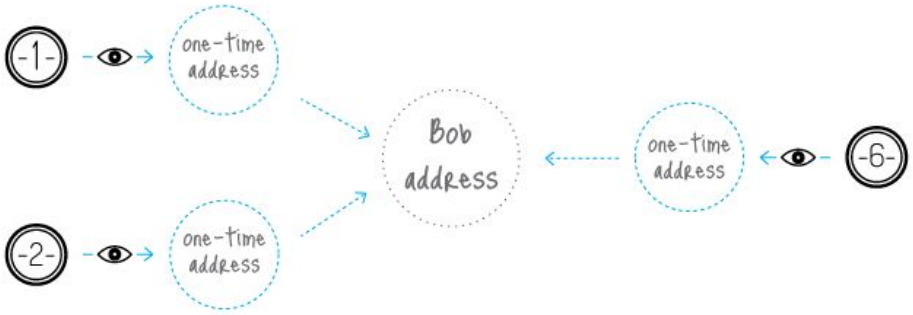
In a ring signature[6], we have a group of users. A ring signature proves that a member of the group has signed the transaction without revealing the identity of the signer. For example, if you encounter a ring signature with the public keys of Alice, Bob, and Carol, you can only claim that one of these users is the signer but you will not be able to pinpoint him or her.

[4] https://cryptonote.org/whitepaper.pdf
[5] https://crypto.stanford.edu/bulletproofs/
[6] https://people.csail.mit.edu/rivest/pubs/RST01.pdf



Stealth address: unlinkable receiver

In a normal crypto network, when you reveal your public address, anyone can check all your incoming transactions. To avoid linking, Incognito automatically create multiple unique one-time keys, one for each incoming transaction, based on the Diffie-Hellman exchange protocol[7].



Confidential transaction: unknown transaction amount

Confidential transaction[8] is recorded on the Incognito public ledger yet hides the amount that is transferred in the transaction. Miners can still verify the transaction without knowing the exact amount, as every confidential transaction includes a zero-knowledge proof that the transaction is valid. Zero-knowledge proof is a powerful cryptographic proof that enables the prover to demonstrate his knowledge of the truth of a particular statement without revealing anything

[7] https://ee.stanford.edu/~hellman/publications/24.pdf
[8] https://people.xiph.org/~greg/confidential_values.txt

beyond the fact that it is true. Incognito implements Bulletproof[9], a short non-interactive zero-knowledge proofs that require no trusted setup and shrink the size of the cryptographic proof from over 10kB to less than 1kB.

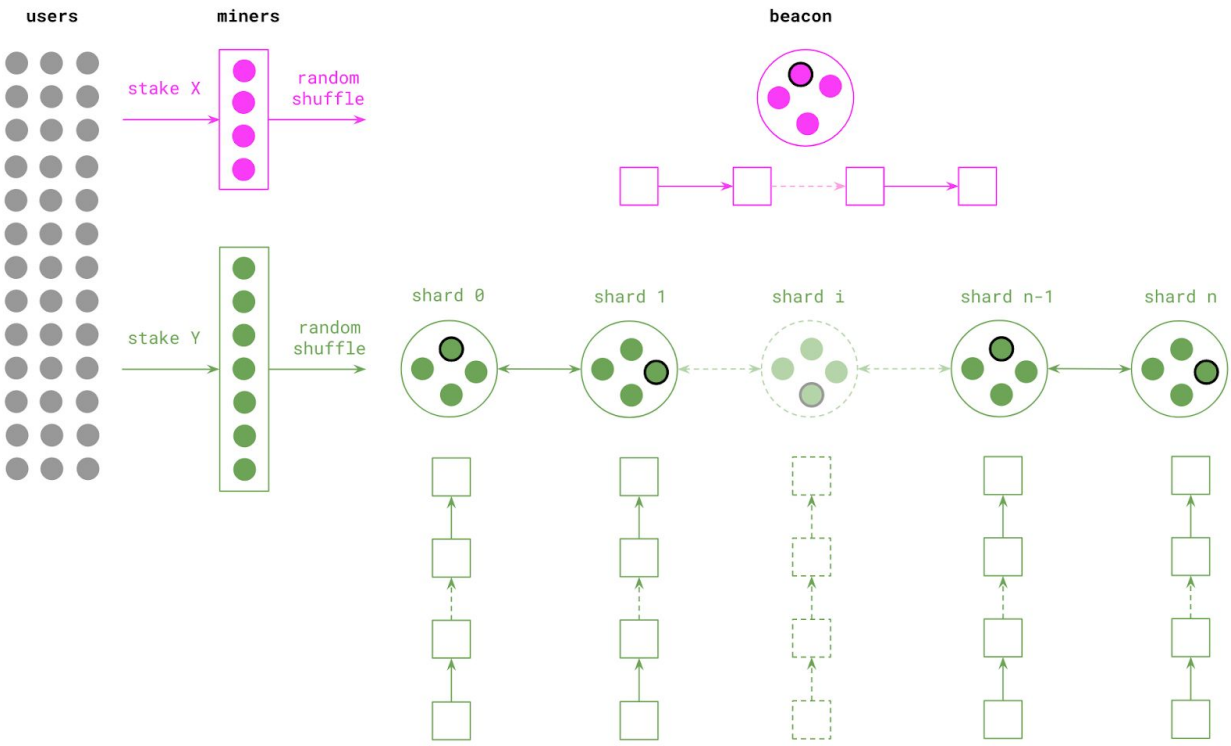
Scalability

Incognito takes a practical approach in designing and implementing its consensus mechanism, based on previous research and engineering works including OmniLedger[10], Bitcoin[11], Ethereum 2.0[12], and Zilliqa[13].

Design

Incognito is designed with 1 beacon chain and N sharding chains. We'll start with 8 shards and slowly scale the number of shards. Each chain has its own committee.

[9] https://crypto.stanford.edu/bulletproofs/
[10] https://eprint.iacr.org/2017/406.pdf
[11] https://bitcoin.org/bitcoin.pdf
[12] https://github.com/ethereum/eth2.0-specs
[13] https://docs.zilliqa.com/whitepaper.pdf



Proof of Stake

Instead of the wasteful Proof-of-Work mining[14], Incognito implements Proof-of-Stake (PoS). Anyone can be a validator candidate by staking an amount of token (currently, a minimum of 1,750 PRV). The beacon chain randomly assigns validators for each shard. Each validator has one vote. A block is considered a valid block if it collects more than 2/3 valid signatures from validator committee.

In order to select N validators from M candidates (M ≥ N), only top 4N candidates – ordered by their staking amounts – are randomly selected. This mechanism encourages validators to stake more tokens, meaning that the chain is safer while preserving the randomness and inclusiveness.

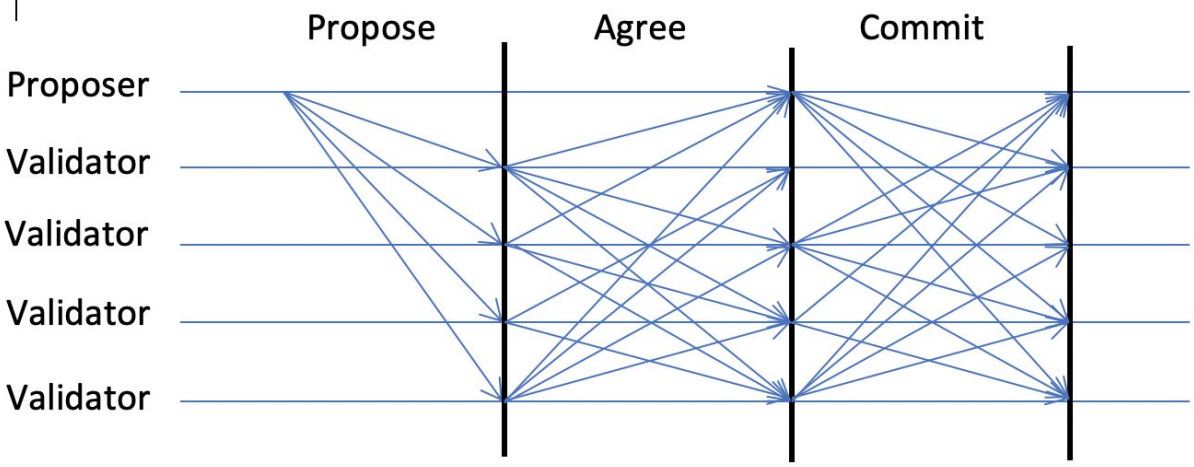
MuSig

Incognito implements MuSig[15], a new Schnorr-based multi-signature scheme, for aggregating the validators' signatures into a short joint signature.

[14] https://digiconomist.net/bitcoin-energy-consumption
[15] https://eprint.iacr.org/2018/068.pdf

Practical Byzantine Fault Tolerance

Incognito implements pBFT at the consensus layer.



Here is the detail of our pBFT approach:

LISTEN PHASE
Block Validators broadcast READY_MESSAGE then listen for PROPOSE_MESSAGE from the Block Proposer.

- Within a bounded time T, if Block Validators receive a valid PROPOSE_MESSAGE, they will continue to the next phase.
- Otherwise, return a timeout error.

PROPOSE PHASE
Block Proposer collects valid READY_MESSAGE(s) from Block Validators.

- Within a bounded time T, if |READY_MESSAGE(s)| > ⅔ COMMITTEE_SIZE then Block Proposer broadcasts the new block.
- Otherwise, return a timeout error.

AGREE PHASE
Everyone broadcasts AGREE_MESSAGE and collects valid AGREE_MESSAGE(s).

- After bounded time T, if |AGREE_MESSAGE(s)| > ⅔ COMMITTEE_SIZE then calculate the aggregated value R from individual random R_i and sign new block with R and continue to the next phase
- Otherwise, return an error.

COMMIT PHASE
Everyone broadcasts COMMIT_MESSAGE (sig, R) and collects valid COMMIT_MESSAGE(s).

- Within bounded time T, if |signatures_list[R]| > ⅔ COMMITTEE_SIZE then combine these signatures and return new block to consensus engine.
- Otherwise, return an error

UTXO-based

Incognito is UTXO-based. We choose a UTXO-based model over an account-based model because of the following reasons:

- In UTXO model, transactions can easily be processed in parallel. This makes it easier to scale through sharding.

- The UTXO model is stateless. Users can easily use a new address for every transaction. This improves privacy.

- Transaction inputs are always linked to existing UTXOs. Because of this linkage, a sequential transaction order is easily authenticated. It is also easy to verify if a UTXO is double spent.

Full sharding

Overview

Incognito has a single beacon chain (the “coordinator”) and 256 shard chains (the “workers”) which produce blocks in parallel. The idea was first proposed by OmniLedger. All shards work in parallel and are synchronized by beacon block time, which is divided into equal epochs (currently ~1 day or ~2,800 shard blocks).

Shards are organized by senders' addresses. Each shard has its own committee, randomly assigned by the beacon chain at the beginning of every epoch. A shard committee validates and detects double-spending locally within the shard.

Both shard chains and beacon chain use PBFT-like protocol, as described above, to reach the consensus on new blocks.

Round robin

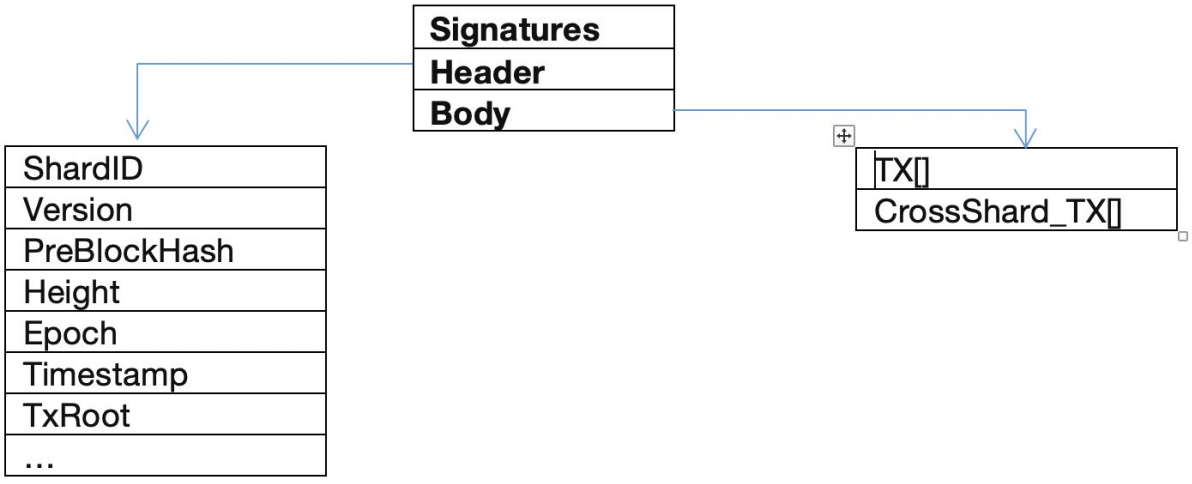
At the beginning of each round, the smallest id validator is the first proposer. The proposer proposes the block and broadcast to the shard committee. Proposers take turns in a round robin fashion, based on their id in the current committee setup.

If a proposer failed to propose its block earlier than the time to build the last three blocks, the next validator will be elected as a new proposer.

If a proposer failed to propose block one time, it will lose its reward in the epoch. If a proposer failed to propose block three times in an epoch it will not be allowed to be a committee member for the next three epochs.

Shard block

Shard block contains three main parts: signature, header, and body. The header stores info related to the current block including previous hash, epoch number, and timestamp. The body stores transactions.



Shard-to-Beacon communications

Every time a shard block is created, it also includes a Shard-to-Beacon block which contains block header and controls messages, if any, and then sends it to the beacon committee.

Beacon-to-shard data structure

Signature
Validator_List
Shard_Header
Instruction

Shard-to-Shard communications

For the cross-shard transactions, the sender shard creates a receipt containing all transactions to the receiver shard and sends it the receiver shard. A brief of cross-shard transactions is also sent to the beacon chain. The UTXOs in the sender shard are locked to make sure that they cannot be double spent. The receiver shard checks the validity of the receipt and waits for confirmation of cross-shard info from beacon chain before approving the corresponding UTXOs spendable.

Cross-shard data structure

Signature
Validator_List
Shard_Header
Destination_Shard
Merkle_ShardPath
CrossShard_UTXO

Beacon chain

The responsibility of the beacon chain is to coordinate shard chains. It is the global state of the entire network. Beacon chain has its own committee and uses the same pBFT consensus mechanism with the shard chain.

- Beacon chain confirms the height of each shard chain based the Shard-to-Beacon block data. The consensus engine makes agreement on the height of each shard chain will be confirmed on the beacon chain.

- Beacon chain confirms cross-shard information. Each shard-to-beacon block header includes cross-shard information, indicating which shard this block has cross-shard to. Besides the height of shard chain, this information also is included in the block body.

- Beacon chain manages the candidate and validator list: Whenever a user stake coin to become a validator, this action will be recorded in the block header.

- Beacon chain shuffles committees. When a new random number is generated, it is recorded in the beacon block header.

The beacon block stores the Merkle root of candidate list and validator list of both the beacon chain and shard chains.

Proposer
Version
PreBlockHash
Height
Epoch
Timestamp
ValidatorsRoot
BeaconCandidateRoot
ShardCandidateRoot
ShardValidatorsRoot

Privacy distribution

Allocation

A strict limit of 100M Privacy will be minted and never to be increased.

%	**Amount (PRV)**	**Purpose**
84%	84,000,000	Miner rewards
8%	8,000,000	Research & Development
8%	8,000,000	User adoption

Vesting Schedule

The Incognito team is fully committed to developing and maintaining the network. For current members, their granted tokens will be vested over 5 years.

Period	**Amount**
Mainnet launch	0%
1 year after mainnet launch	20%
2 year after mainnet launch	20%
3 year after mainnet launch	20%
4 year after mainnet launch	20%
5 year after mainnet launch	20%

For new members, their granted tokens will also be vested over 5 years since the token grant date.

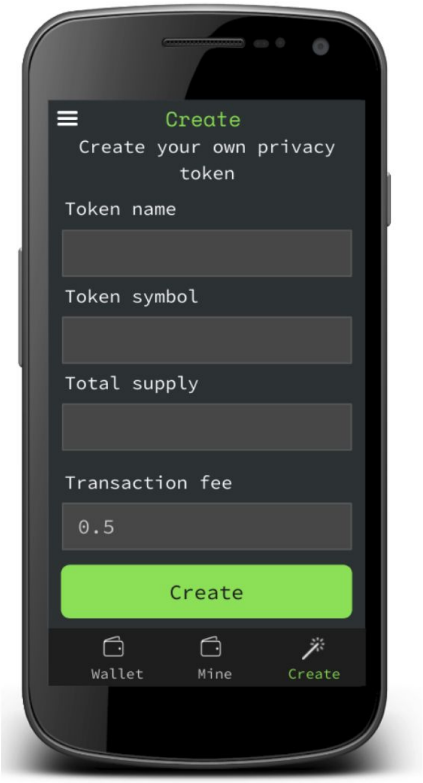
Governance

Incognito starts with a simple governance model where the Incognito core team will adjust the network parameters initially. Over time, Privacy owners will collectively run the network. They will vote on governance issues.

Applications

Privacy Token Systems

There are already 1,600 tokens created in the blockchain ecosystem as of the time of this writing. We believe that there will be many more tokens created to represent every asset out there, including stocks, fiats, gold, real estate, and any form of ownership. We also strongly believe that very few people will willingly disclose their token ownerships to the entire world. Incognito offers developers a simple way to create privacy-preserving tokens.



Privacy Stablecoin (aka. Cash)

Stablecoin is one of the most promising utilities of blockchain. Instead of relying on the ever-fluctuating Bitcoin, people can actually use stablecoins to make cross-border business payments or store their personal savings. However, it is unlikely that everyone wants to disclose how much money they have to the entire world. With Incognito, a privacy-preserving stablecoin, such as private DAI and private USDT, could be developed.

Privacy DAO

Decentralized Autonomous Organization[16] is a new form of organization where governance and decision making are automated via voting. The most common design is that everyone holds a number of voting tokens, and they can use them to cast a vote on a proposal. The problem is that the voting token owners are exposed, on a public ledger, and could be compromised. A privacy-preserving voting token would make the system more secure.

Anonymous Prediction Market

Prediction markets[17], or decentralized betting, was first proposed by Robin Hansen. It was later implemented by crypto projects like Augur[18] and Gnosis[19]. While these betting platforms remove the middlemen (the bookies), they still suffer from the identity problem. A privacy-preserving token could be used on these platforms to keep the users completely anonymous.

Network Analysis

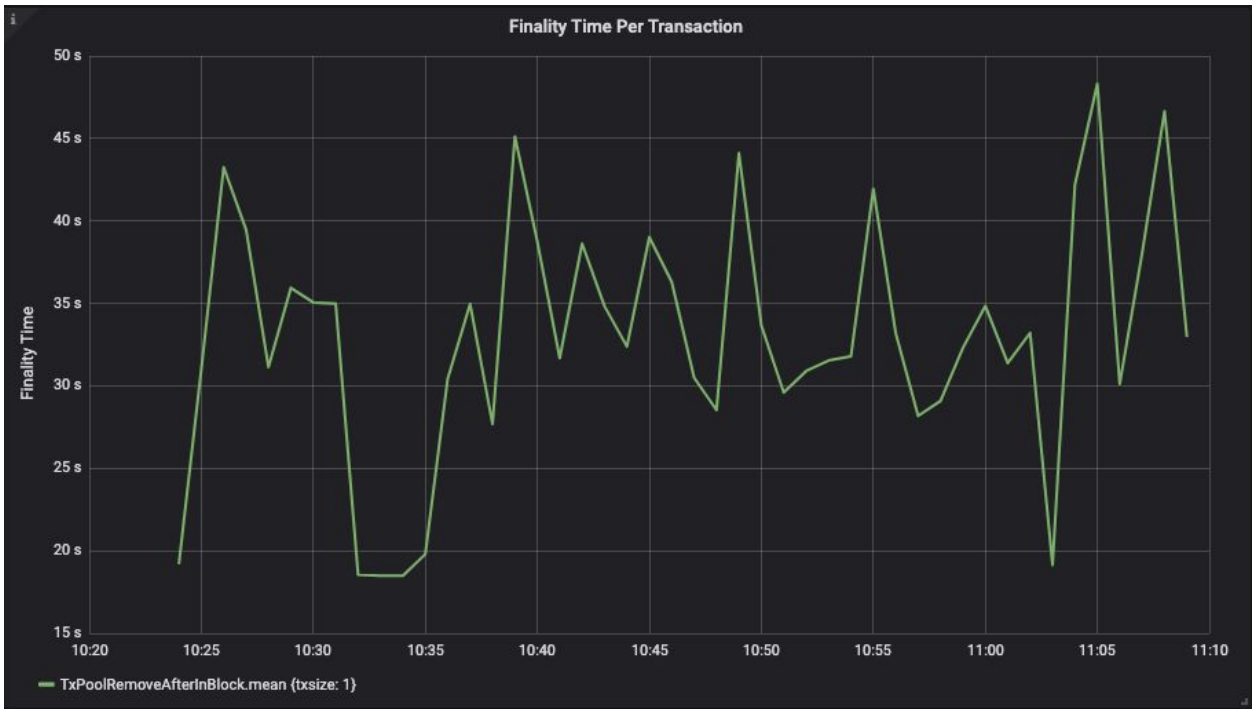
Our team continues to optimize our code. This analysis is on the current code base as of June 20, 2019. The code is open-source at Github. We expect the performance to be significantly improved over the next few months.

The current network performance is:

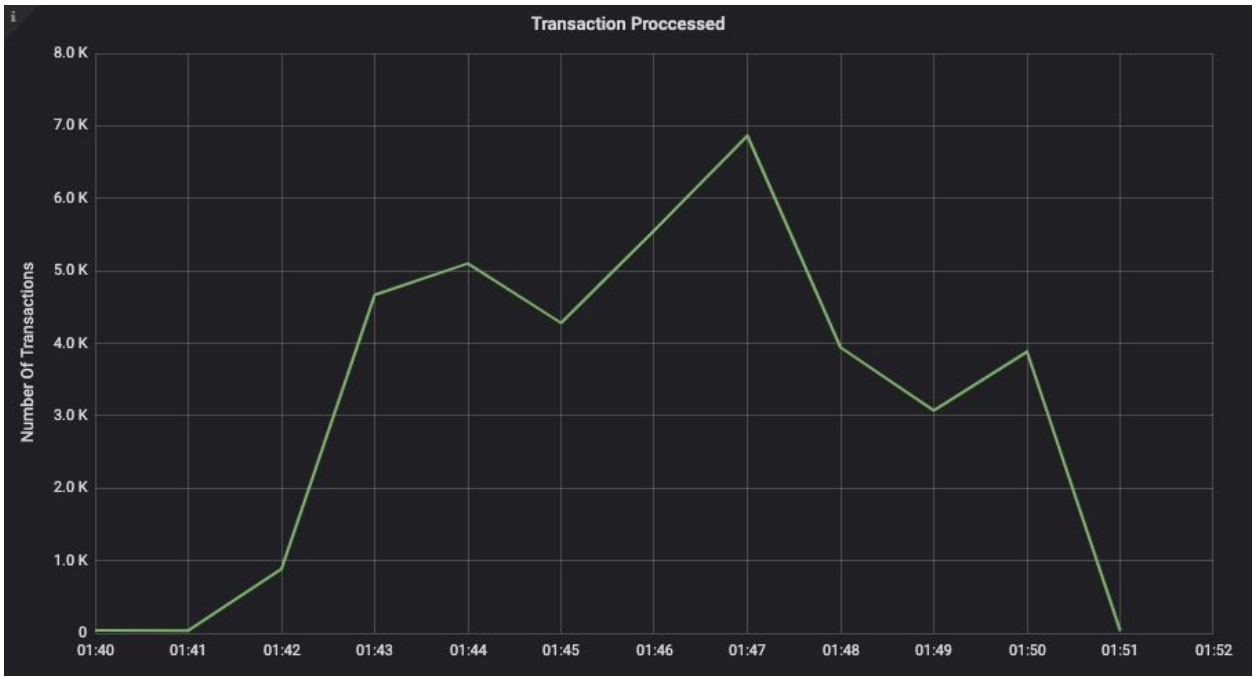
FINALITY TIME OF IN SHARD TRANSACTION	25s
FINALITY TIME OF CROSS SHARD TRANSACTION	75s
TRANSACTION PER SECOND	60 tps/shard

[16] https://download.slock.it/public/DAO/WhitePaper.pdf
[17] http://mason.gmu.edu/~rhanson/ideafutures.html
[18] https://www.augur.net
[19] https://gnosis.io/

In the testnet, we set up a system with two shard chains and one beacon chain. Beacon chain has 4 validators, and each shard chain has 8 validators. The validator node is equipped with CPU 4 core, RAM 8GB, SSD 512GB. The connection bandwidth is 1 Gbps. In shards transactions are continuously feeding to the mempool, starting with the rate at 200 tx/s then descending gradually to 5 tx/s in 3 hours. The finality times, transaction per block, and mempool size are shown in the following figures.

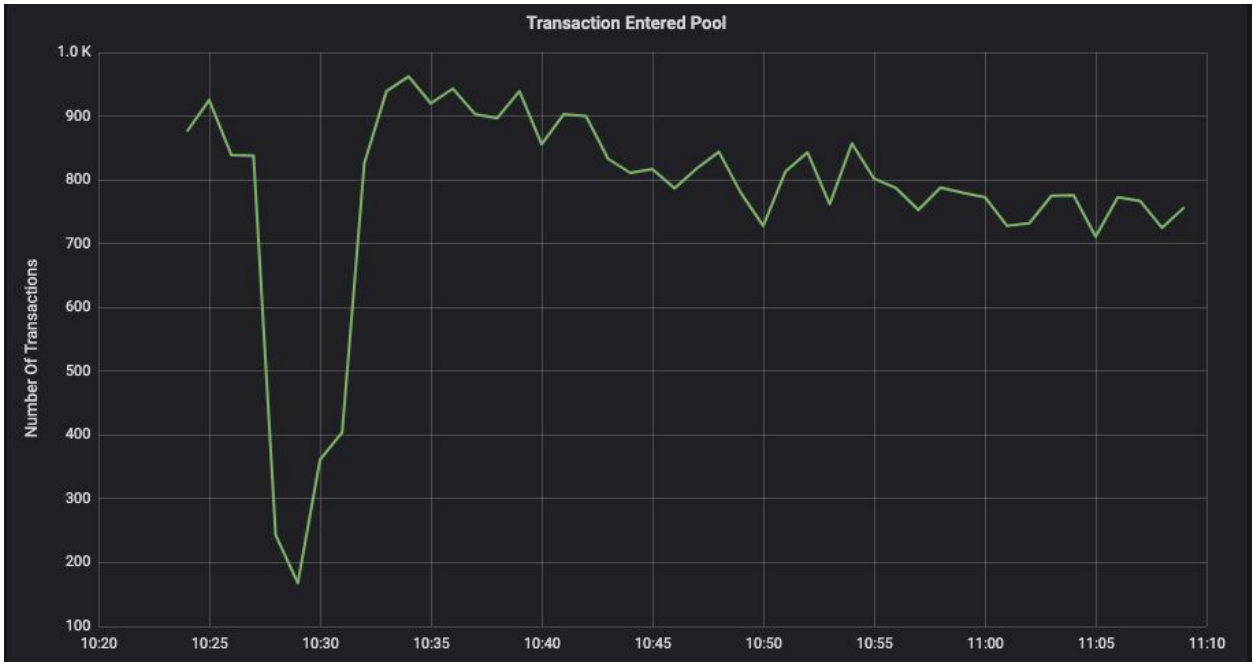


Finality time



Transaction per block

Mempool Size (Current Number of Transactions in Pool)



Number Of Transaction Entered Pool

Team

We’re a diverse team of 15 cryptographers, distributed system researchers, programmers and hardware makers - on a mission to build the privacy layer of the decentralized web.

Risks & Mitigations

Risk 1: Nothing at stake problem

A validator may sign multiple competing chains at once.

Potential solution:

- Finality conditions - the longer chain and obtain more signatures is considered finalized.
- Slashing conditions - if a validator is voting for multiple conflicting blocks at the same time its entire deposit gets deleted.

Risk 2: Single shard attack

Attackers may take over the validators in a shard in order to submit false collations.

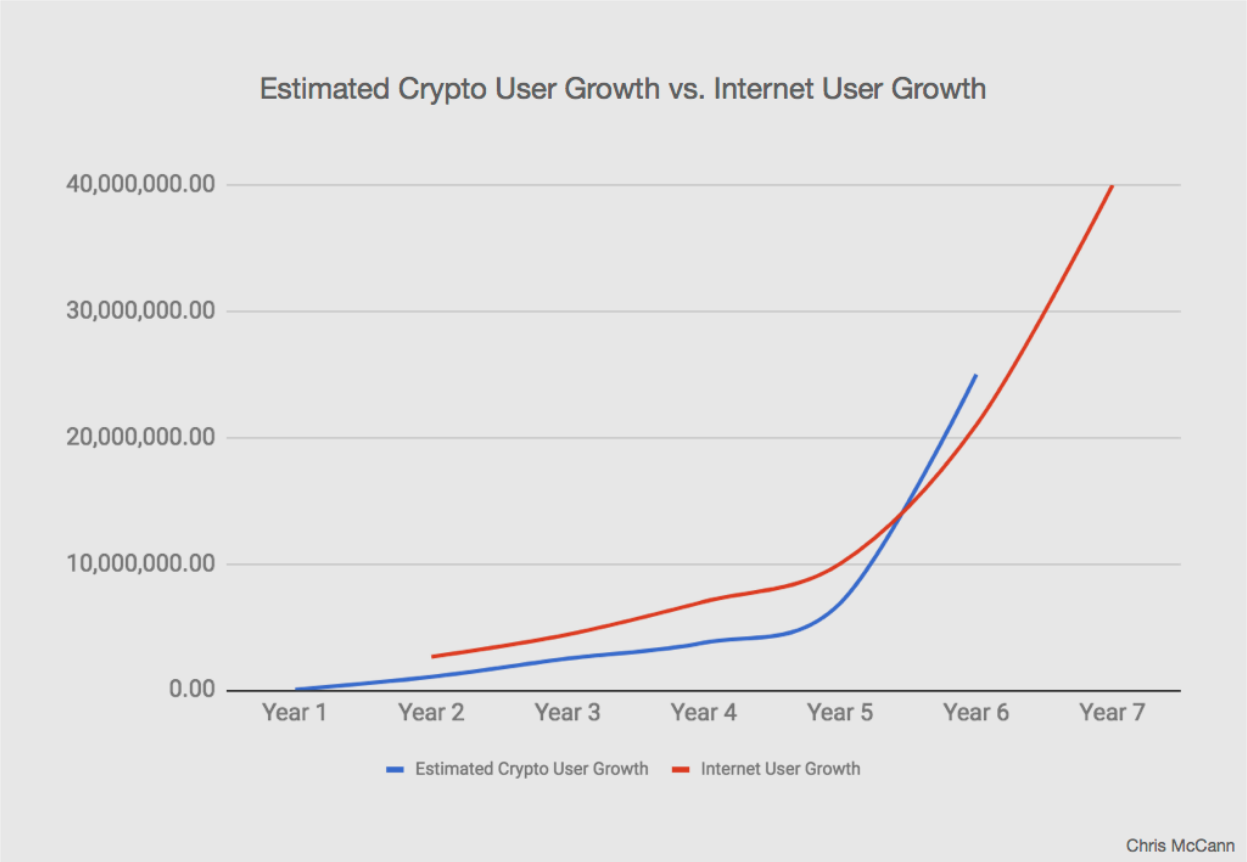
Potential solution: We'll randomly sample all validators. If one wishes to avoid a shard committee of size N being more than 50% corrupted by an attacker, and an attacker has p% of the global stake pool, the chance of the attacker being able to get such a majority in a single shard is as follows:

	N = 50	N = 100	N = 150	N = 250
p = 0.4	0.0978	0.0271	0.0082	0.0009
p = 0.33	0.0108	0.0004	1.83 * 10-5	3.98 * 10-8
p = 0.25	0.0001	$6.63 * 10^{-8}$	$4.11 * 10^{-11}$	1.81 * 10-17
p = 0.2	$2.09 * 10^{-6}$	$2.14 * 10^{-11}$	$2.50 * 10^{-16}$	$3.96 * 10^{-26}$

The data shows that, for N >= 150, the chance that any given random seed will lead to a sample favoring the attacker is very small indeed

Summary

The internet in 1994 looked nothing like what we have today. Blockchain's 1994 is happening right now.



There is an increasing number of crypto assets every day. Some of them wrap around existing assets like fiats (TUSD) and gold (DGX) and make them more efficient. Some of them are introduced as entirely new asset classes, like programmable governance token (MKR). We believe that crypto assets will play a very important role in the near future. Soon, a person's net worth will be mainly composed of the crypto assets they own, and a company's balance sheet will be calculated on crypto assets.

When the world of a million crypto assets arrives, Incognito hopes to provide these assets and their owners a little more privacy, simply because privacy is a fundamental human right.

Parameters

NUMBER OF SHARD	256
MINIMUM STAKING AMOUNT - SHARD CHAIN	1,750
MINIMUM STAKING AMOUNT - BEACON CHAIN	5,250
SUPPLY LIMIT	100,000,000
BLOCK TIME	5 seconds
BLOCK REWARD	0.5 PRV, reduced 15% every year.