



Incognito

A full-stack approach to decentralized privacy.
For a rapidly tokenizing world.

White Paper Draft v0.7
Oct 1, 2019

www.incognito.org
go@incognito.org

Intro	3
Incognito: A Full-Stack Approach to Decentralized Privacy	3
Physical Layer	5
Why Hardware?	5
Incognito Node	5
Network Layer	6
Design	6
Proof of Stake	7
MuSig	7
Practical Byzantine Fault Tolerance	8
UTXO-based	9
Full sharding	9
Overview	9
Round Robin	10
Shard Block	10
Shard-to-Beacon Communications	10
Shard-to-Shard Communications	11
Beacon Chain	11
Data Layer	13
Ring Signature: Untraceable Sender	13
Stealth Address: Unlinkable Receiver	13
Confidential Transaction: Unknown Transaction Amount	14
Application Layer	15
A Simple, Secure, Privacy-Preserving Wallet	15
Zero-Knowledge Proofs on Mobile	16
Bridges	16
Incognito as a Sidechain	17
Bridges	18
Privacy (PRV) Mining & Distribution	19
Total Supply	19
Self-Funded	19
95M Fair-Mining	19
5M Pre-Mining	19
Initial Staking	19

Block Reward Split	20
PRV Denominations	21
Tokens	21
Fees	22
Governance	22
Applications	22
Privacy Token Systems	22
Privacy Stablecoin (aka. Cash)	22
Privacy DAO	23
Anonymous Prediction Market	23
Network Analysis	23
Team	26
Risks & Mitigations	27
Risk 1: Nothing at stake problem	27
Risk 2: Single shard attack	27
Summary	28
Parameters	29

Intro

Cryptonetworks 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.

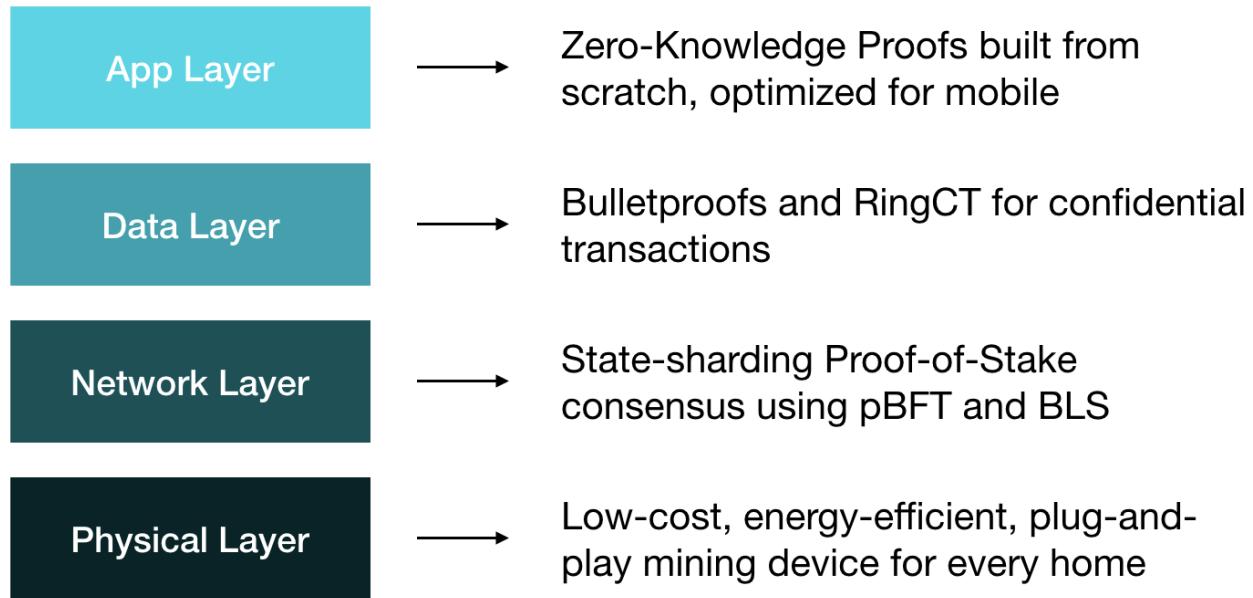
Incognito offers anyone the option to turn on privacy mode in this new world of cryptonetworks.

Incognito: A Full-Stack Approach to Decentralized Privacy

Incognito embraces a full-stack approach to decentralized privacy. Every layer of the stack works to deliver a simple, fast and secure end-to-end privacy experience for the new decentralized web.

- **Physical Layer.** 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.
- **Network Layer.** A high-throughput proof-of-stake blockchain, made possible by the implementation of state sharding with 1 beacon chain and N shard chains.
- **Data Layer.** Incognito uses zero-knowledge proofs, ring signatures, stealth addresses and confidential transactions to mask the sender, receiver and transaction amount.
- **Application Layer.** Incognito is mobile first. The Incognito wallet is a simple and secure tool for anyone to manage their crypto assets confidentially. Incognito built the

entire Zero-Knowledge Proof (ZKP) stack for mobile from scratch. Send a private transaction on mobile in seconds.



Incognito operates a number of **bridges** that connect Incognito with other blockchains (i.e. Ethereum), to allow two-way transfers of crypto assets whenever privacy is needed.

Physical Layer

Why Hardware?

Technical users can host a virtual node by running software on their computers. Incognito will also ship its own mining hardware. This will:

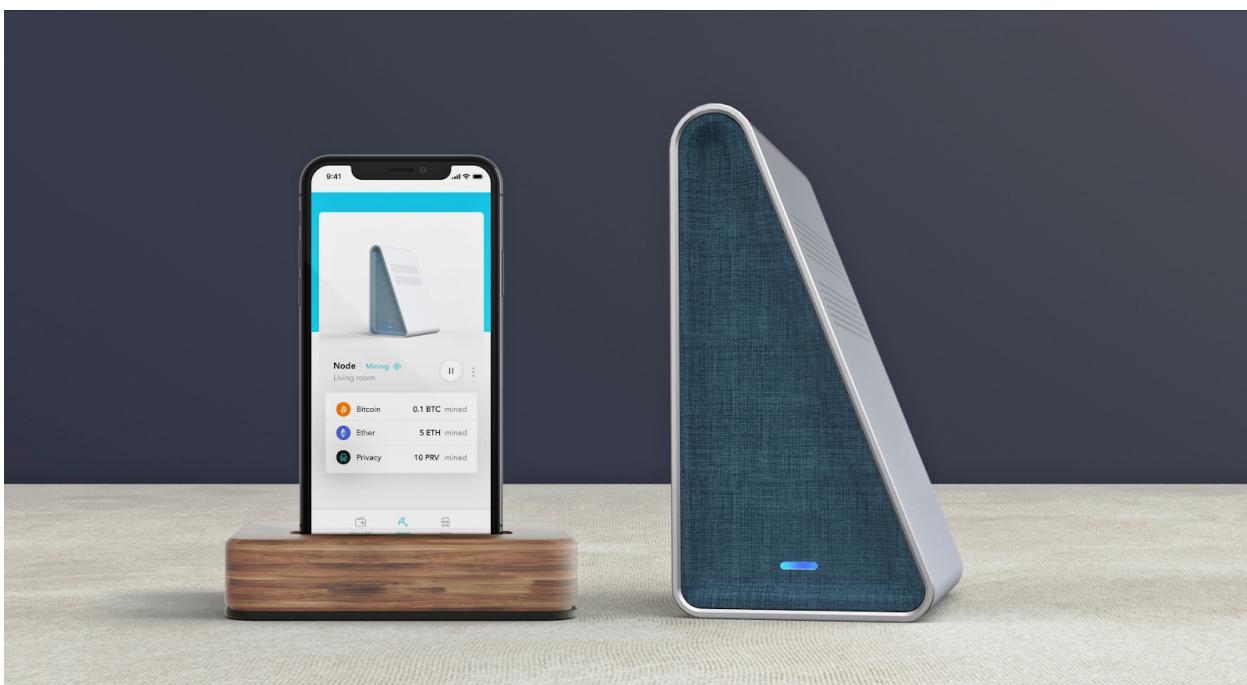
- **Broaden the validator base.** For Incognito to be truly decentralized, we need as many users as possible to host nodes - including less technical users. With user-friendly hardware and software, any user can stake from their phone and become a validator.

- **Make it more affordable to be a validator.** Designed for the individual then produced en masse, Node saves on manufacturing and software maintenance costs. Affordability opens up access and leads to a greater degree of decentralization.
- **Distribute tokens more effectively.** Our team wants to build a thriving, engaged community focused more on the health of the network than price speculation. Instead of participating in a public token sale, users will receive Privacy tokens preloaded into Incognito hardware, so they can reap rewards and add value to the network right away.

Incognito Node

Node is a plug and play device that powers the Incognito network. Whenever anyone makes a private crypto transaction (say, in BTC or DAI), Node earns its owner rewards in that currency. Node also earns Incognito's native coin, Privacy (PRV), for every block created.

Node comes with a mobile app that you can use to start, pause, resume and track your earnings - from your couch, at the beach or on the go.



Network Layer

Incognito is a high-throughput proof-of-stake sidechain, made possible by the implementation of state sharding. Incognito takes a practical approach in designing and implementing its consensus mechanism, based on previous research and existing engineering by OmniLedger¹, Bitcoin², Ethereum 2.0³, and Zilliqa⁴.

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.

Proof of Stake

Incognito implements the more energy efficient Proof-of-Stake (PoS) in lieu of Proof-of-Work⁵. Anyone can be a validator candidate by staking the native coin of Incognito, Privacy (PRV). The minimum stake is currently 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 the validator committee.

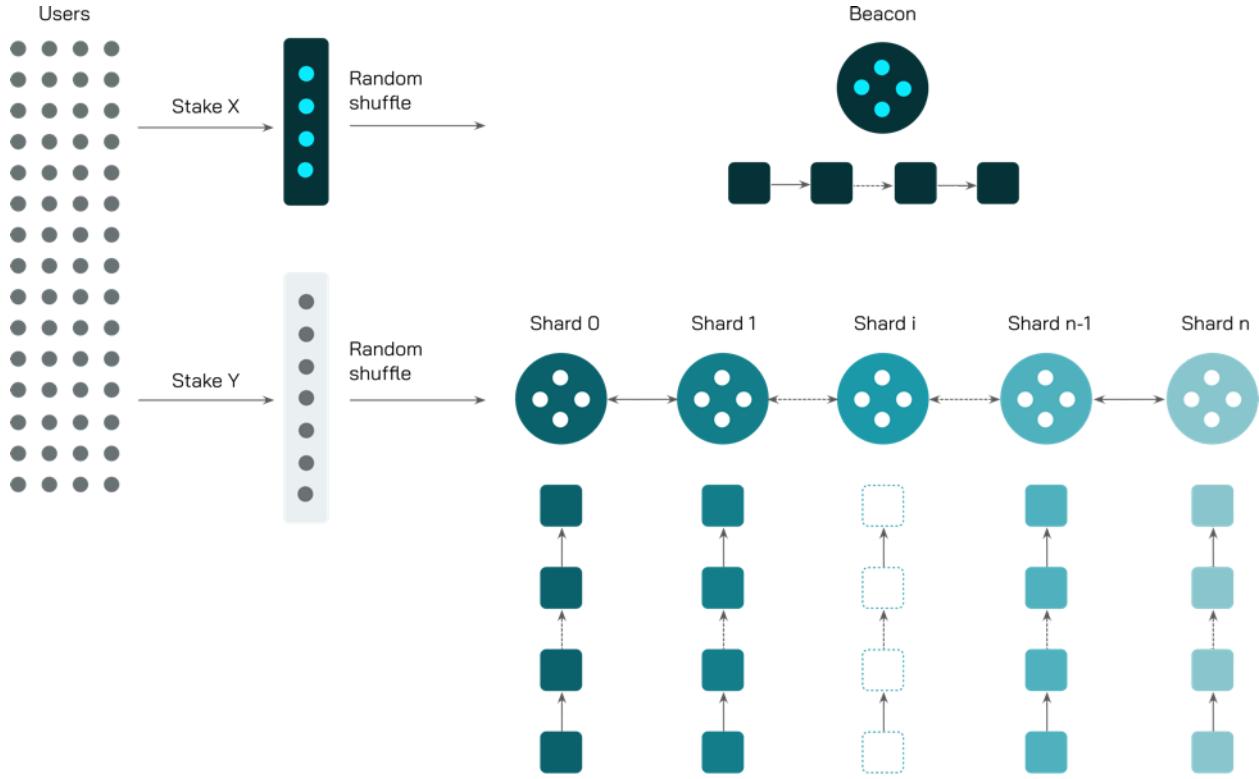
¹ <https://eprint.iacr.org/2017/406.pdf>

² <https://bitcoin.org/bitcoin.pdf>

³ <https://github.com/ethereum/eth2.0-specs>

⁴ <https://docs.zilliqa.com/whitepaper.pdf>

⁵ <https://digiconomist.net/bitcoin-energy-consumption>



When randomly selecting N validators from M candidates ($M \geq N$), the top $4N$ candidates by staked amount will be eligible. This mechanism encourages validators to stake more tokens, increasing the safety of the chain while preserving randomness and inclusiveness.

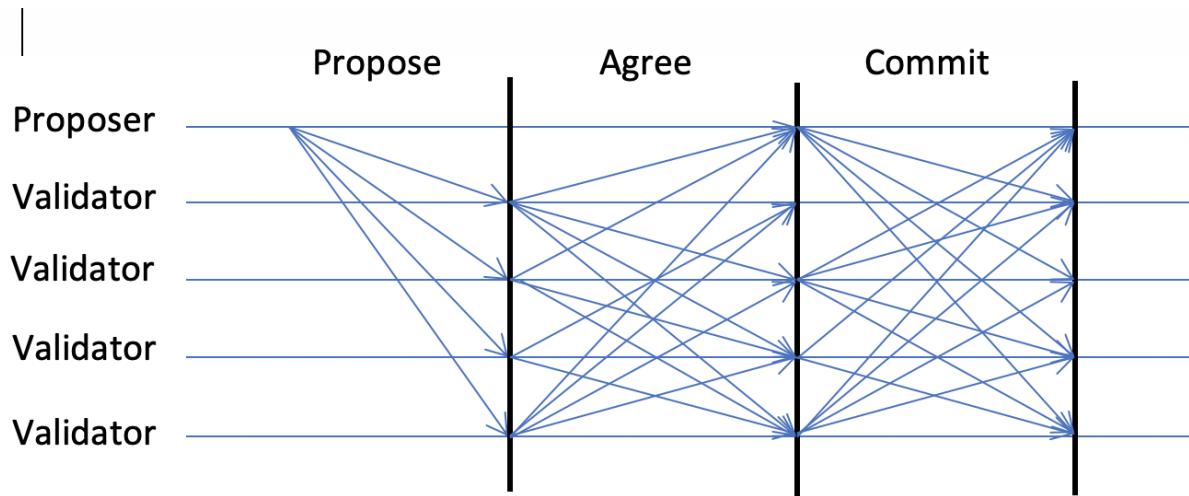
MuSig

Incognito implements MuSig⁶, a new Schnorr-based multi-signature scheme, for aggregating validator signatures into a short joint signature.

Practical Byzantine Fault Tolerance

Incognito implements pBFT at the consensus layer.

⁶ <https://eprint.iacr.org/2018/068.pdf>



Below are the details 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 $|\text{READY_MESSAGE}(s)| > \frac{2}{3} \text{ COMMITTEE_SIZE}$ 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 $|\text{AGREE_MESSAGE}(s)| > \frac{2}{3} \text{ COMMITTEE_SIZE}$ then calculate the aggregated value R from individual random R_i , 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 $|\text{signatures_list}[R]| > \frac{2}{3} \text{COMMITTEE_SIZE}$ then combine these signatures and return new block to consensus engine.
- Otherwise, return an error.

UTXO-based

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

- In a UTXO model, transactions can be easily 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, 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.

Shards are organized by sender 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 the previously described PBFT-like protocol to reach 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 broadcasts to the shard committee. Proposers take turns in a round robin fashion, based on their id in the current committee setup.

If a proposer fails to propose its block in less than the time taken to build the last three blocks, the next validator will be elected as a new proposer.

If a proposer fails to propose its block on time, it will lose its reward in the epoch. If a proposer fails to propose its block three times in an epoch, it cannot be a committee member for the next three epochs.

Shard Block

A shard block contains three main parts: signature, header, and body. The header stores information 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 includes a Shard-to-Beacon block which contains block header and control messages (if any), and sends it to the beacon committee.

Beacon-to-shard data structure:

Signature
Validator_List
Shard_Header
Instruction

Shard-to-Shard Communications

For cross-shard transactions, the sender shard creates a receipt containing all transactions to the receiver shard, then sends this receipt to 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 they cannot be double spent. The receiver shard checks the validity of the receipt and waits for confirmation of cross-shard info from the beacon chain, before approving the corresponding UTXOs as 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 as the shard chain.

- Beacon chain confirms the height of each shard chain based on the Shard-to-Beacon block data. The validators of the beacon chain reach consensus on the heights of each shard chain, which is then 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. In addition to 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 stakes 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 the candidate list and the validator list, of both the beacon chain and shard chains.

Proposer
Version
PreBlockHash
Height
Epoch
Timestamp
ValidatorsRoot
BeaconCandidateRoot
ShardCandidateRoot
ShardValidatorsRoot

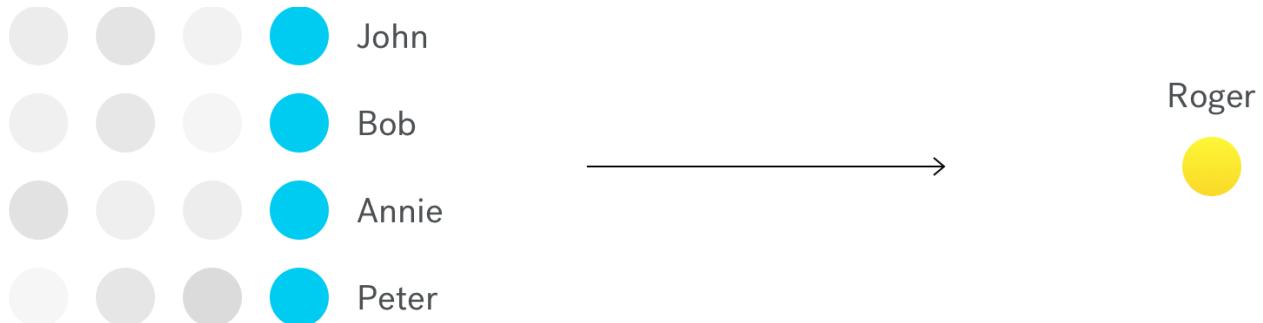
Data Layer

Incognito uses zero-knowledge proofs, ring signatures, stealth addresses and confidential transactions to mask senders, receivers and transaction amounts. Incognito privacy is implemented based on CryptoNote⁷ and Bulletproof⁸.

⁷ <https://cryptonote.org/whitepaper.pdf>

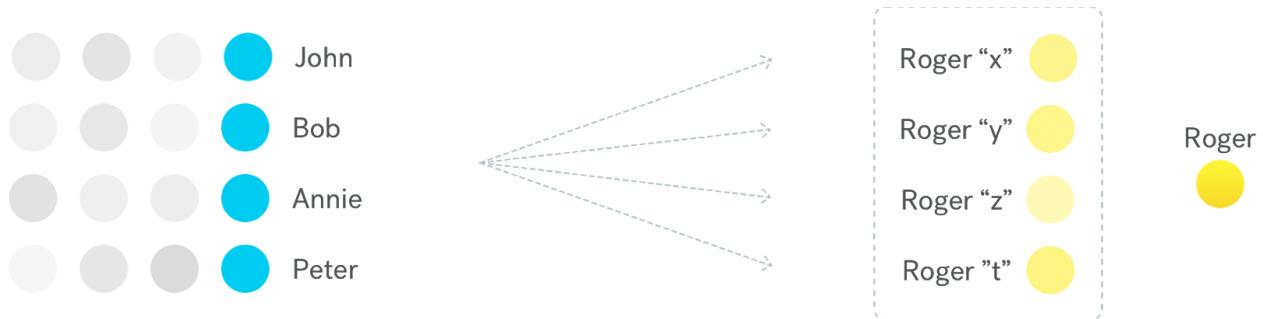
Ring Signature: Untraceable Sender

In a ring signature⁹, 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 Annie, Bob, John and Peter, you will be able to claim that one of these users is the signer, but not be able to pinpoint him or her.



Stealth Address: Unlinkable Receiver

In a typical cryptonetwork, your public address is all that is needed for anyone to view your incoming transactions. Your transactions are public and can be easily linked together to infer your total balances and spending patterns. To avoid transaction linking, Incognito automatically creates multiple unique one-time keys; one for each incoming transaction, based on the Diffie-Hellman exchange protocol¹⁰.



⁸ <https://crypto.stanford.edu/bulletproofs/>

⁹ <https://people.csail.mit.edu/rivest/pubs/RST01.pdf>

¹⁰ <https://ee.stanford.edu/~hellman/publications/24.pdf>

Confidential Transaction: Unknown Transaction Amount

A confidential transaction¹¹ is recorded on the Incognito public ledger but the amount is obscured. Validators can still verify the transaction without knowing the exact amount, as every confidential transaction includes a zero-knowledge proof of the transaction's validity. Zero-knowledge proof is a powerful cryptographic proof that enables the prover to demonstrate a statement is true without revealing any of its contents. Incognito implements Bulletproof¹², short non-interactive zero-knowledge proofs that require no trusted setup and shrink the size of cryptographic proofs from over 10kB to less than 1kB.



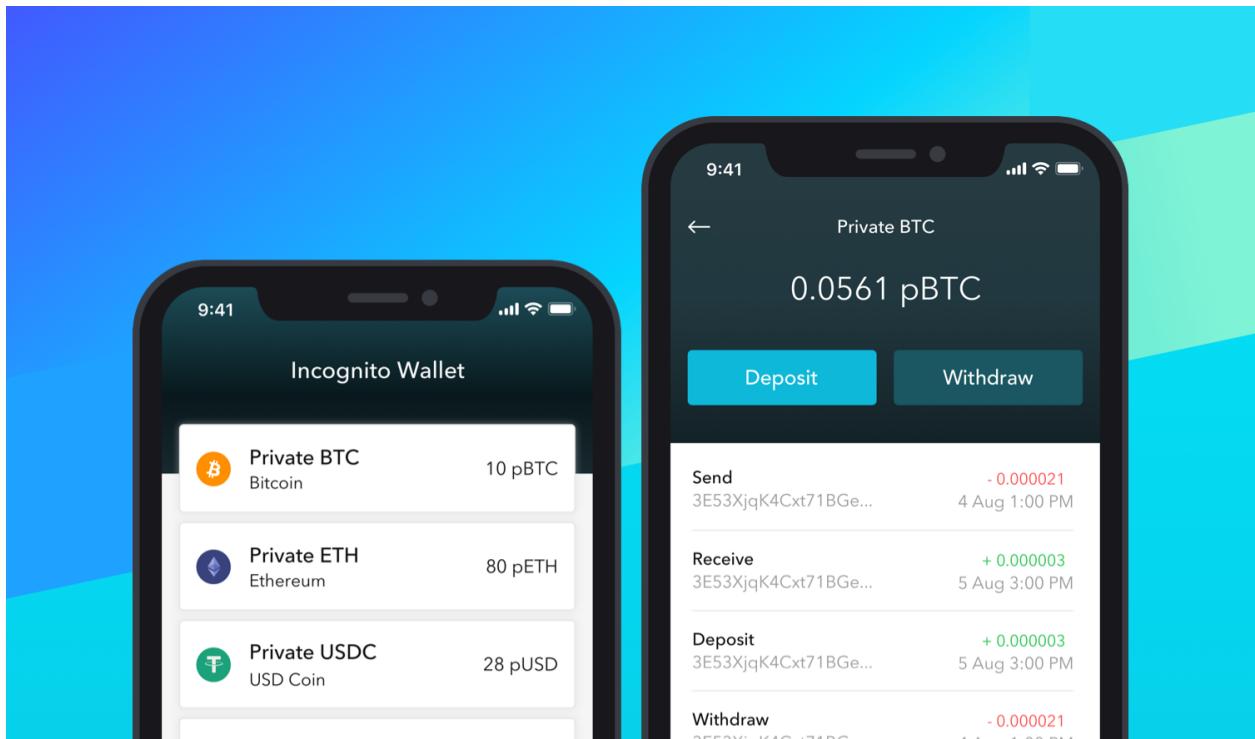
Application Layer

A Simple, Secure, Privacy-Preserving Wallet

The Incognito wallet is available on iOS, Android and Chrome Extension. Users hold their own keys and sign all transactions locally. High-performing zero-knowledge proof generation has been implemented on the client side, resulting in a fast, secure, privacy-first experience.

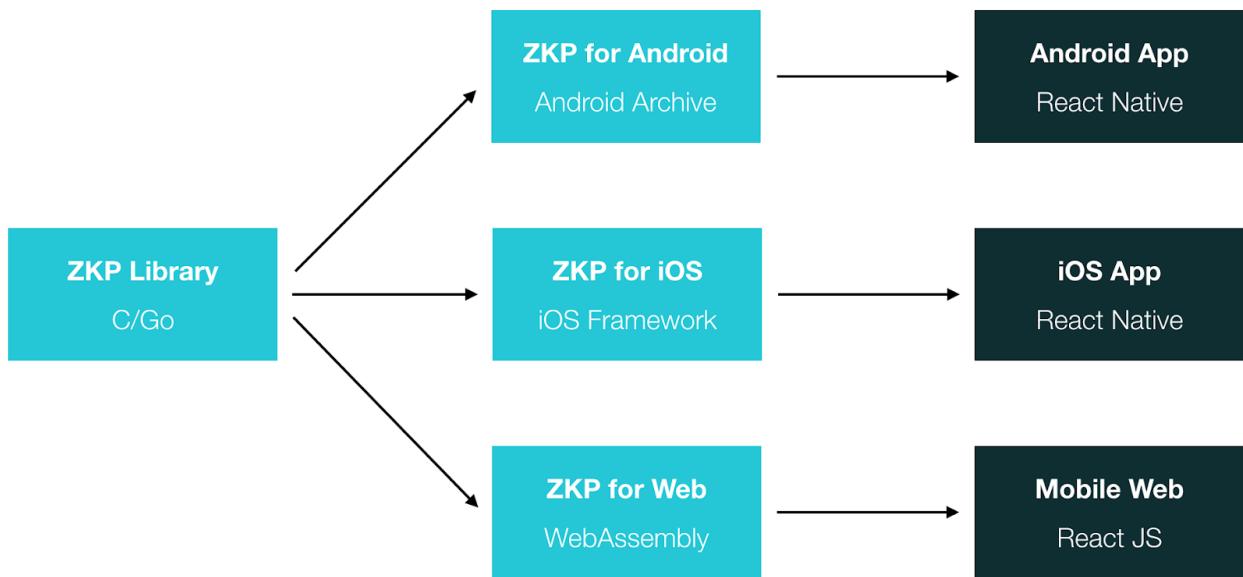
¹¹ https://people.xiph.org/~greg/confidential_values.txt

¹² <https://crypto.stanford.edu/bulletproofs/>



Zero-Knowledge Proofs on Mobile

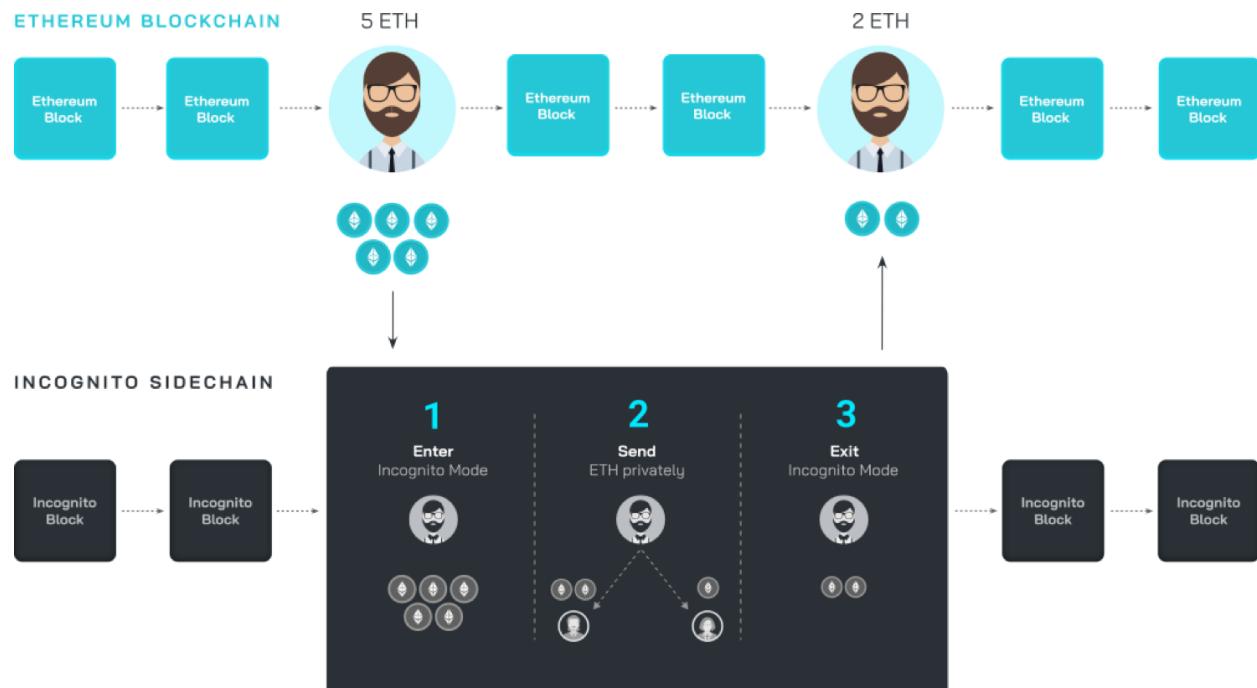
Incognito implements the entire Zero-Knowledge Proof (ZKP) stack for mobile from scratch. Users are now able to send a private transaction on mobile in seconds.



Bridges

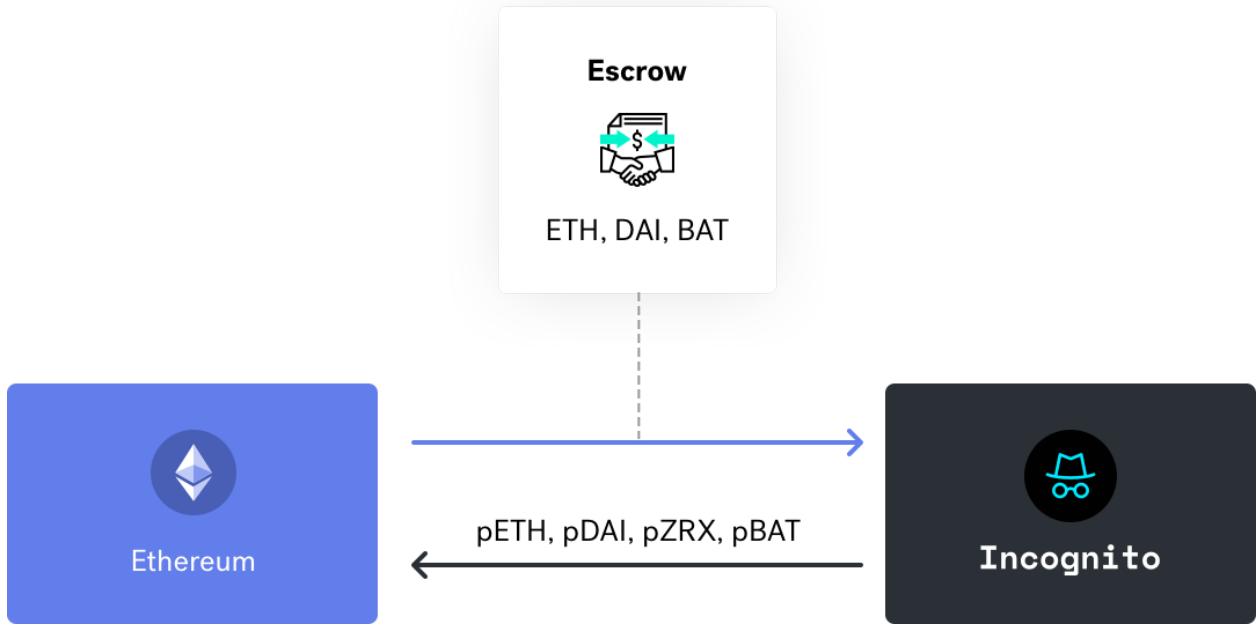
Incognito as a Sidechain

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



Bridges

Bridges allow tokens to be securely moved from their native blockchains for use in Incognito, then moved back to the original chain if needed. There are two types of bridges implemented in Incognito: **custodial bridges** and **noncustodial bridges**.



The key difference between custodial bridges and noncustodial bridges is in the management of the escrow.

- **Custodial bridges.** Funds will be managed by independent third parties like Bitgo¹³ or PrimeTrust¹⁴.
- **Noncustodial bridges.** Funds are held in trustless smart contracts which run as programmed, without the need for human intervention. Our preference is to implement noncustodial bridges whenever possible.

Whether escrow management is custodial or non-custodial, the Incognito team never touches the funds. Funds are protected by independent trust companies or smart contracts.

¹³ <https://www.bitgo.com/>

¹⁴ <https://primetrust.com/>

Privacy (PRV) Mining & Distribution

Total Supply

A strict limit of 100M Privacy (PRV) will be minted. This number will never increase.

Self-Funded

The founding team pooled together a collective \$2M to fund the project. No ICO, private sale or VC funding. Potential users and investors should not be asked to pay prior to any code being written. As such, the founding team bears all risks.

The first \$1M was funded in May 2018 and primarily used for protocol development. The second \$1M was funded in July 2019 prior to the testnet launch, and primarily used for adoption.

This funding structure will reduce price speculation around the project, avoid public market pressure, and keep the team laser-focused on building and shipping a great platform for decentralized privacy tokens.

95M Fair-Mining

Proof-of-stake networks often heavily pre-allocate tokens for the team, investors, and ICO. Incognito takes a different approach. Incognito is a proof-of-stake blockchain that designs its block rewards similarly to proof-of-work blockchains like Bitcoin.

95M of the 100M PRV total supply is mined through block rewards. The total block reward for the first year is 11,360,736 PRV. Block rewards are reduced by 12.5% for every subsequent year. PRV will be fully mined after 35 years.

5M Pre-Mining

5M PRV is pre-mined and purchased by the founding team for the aforementioned \$2M, and has been used to cover salaries, server costs, operational expenses, and marketing activities.

Initial Staking

There is a chicken-and-egg problem with any Proof of Stake blockchain. How can validators start staking when they don't have coins to stake?

Incognito solves this in 2 ways:

- Testnet validators are rewarded with Testnet PRV, which can be converted 1:1 to Mainnet PRV at Mainnet launch.
- Incognito has its own hardware, Node. If Node owners don't have PRV to get started, they can borrow PRV from the Node Staking Fund, a decentralized fund where anyone can lend out their PRV to Node owners.

Block Reward Split

95% of PRV total supply is minted through block rewards. Block rewards are split between the validators and Incognito DAO, a decentralized autonomous organization designed to fund protocol development and network growth. Incognito DAO collects a gradually reducing percentage of the block rewards, from 10% to 3%.

With this income, Incognito DAO will fuel the growth of the network, fund interesting projects, and give the project longevity.

Incognito DAO's funds are initially managed by the founding team. Management responsibilities will be gradually distributed to the community.

Year	Validators	Incognito DAO
1	90%	10%
2	91%	9%
3	92%	8%
4	93%	7%
5	94%	6%
6	95%	5%
7	96%	4%
8+	97%	3%

PRV Denominations

Privacy is the native coin of Incognito. The smallest sub-denomination of Privacy is Nano. 1 Privacy is defined as 10^9 Nano. There exist other sub-denominations of Privacy.

In the future, we expect Privacy to be used for regular transactions, Milli for microtransactions, Micro for transaction fees, and Nano for technical discussions and implementations.

Multiplier	Name
10^9	Privacy
10^6	Milli
10^3	Micro
10^0	Nano

Tokens

There are 3 types of tokens:

- **Privacy.** Privacy (PRV) is Incognito's native token — a work token¹⁵. Users stake Privacy to become validators. Validators 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, validators will earn more revenue, which naturally triggers an increase in the price of PRV.

- **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 a 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 also be used to pay for transaction fees.

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

¹⁵ <https://multicoin.capital/2018/02/13/new-models-utility-tokens/>

Fees

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

Governance

The initial governance model is simple – the core team will adjust the network parameters. Over time, Privacy owners will collectively run and govern the network.

Applications

Privacy Token Systems

At the time of writing, 1,600 tokens have been created in the blockchain ecosystem. We believe that in the near future, tokens will increasingly represent everyday assets, including but not limited to stocks, fiats, gold, real estate and any form of ownership. We also strongly believe that very few people will willingly disclose their token holdings to the entire world. Incognito offers developers a simple way to create privacy-preserving tokens.

Privacy Stablecoin (aka. Cash)

The stablecoin is one of the most promising iterations of blockchain utility. Stablecoins are typically pegged to world currencies like the USD or Euro, thus not subject to the volatility of other cryptocurrencies. As a digital currency, stablecoins are borderless, making them the perfect vessel for cross-border business payments or simply a secure way to store personal savings. Stablecoins are digital cash. Very few people want the world to know how exactly how much cash they have. On the Incognito platform, a privacy-preserving stablecoin (such as private DAI or private USDT) can be created in a few taps.

Privacy DAO

In a Decentralized Autonomous Organization¹⁶, governance and decision making are automated. The most common design is that everyone holds a number of voting tokens, used to cast votes on proposals. The problem is that the voters are exposed on a public ledger, and could be compromised. A privacy-preserving voting token would make the system more secure.

Anonymous Prediction Market

Decentralized betting and prediction markets¹⁷ were first proposed by Robin Hansen. This concept was later materialized by crypto projects like Augur¹⁸ and Gnosis¹⁹. 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 users completely anonymous.

Network Analysis

Our team continuously optimizes the code. This analysis is based on the current code base as of June 20, 2019. The code is open-source on [Github](#). We expect performance to significantly improve 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

For the testnet, the system is set up with 8 shard chains and one beacon chain. Beacon chain has 4 validators, and each shard chain has 16 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 at a rate of 200 tx/s before

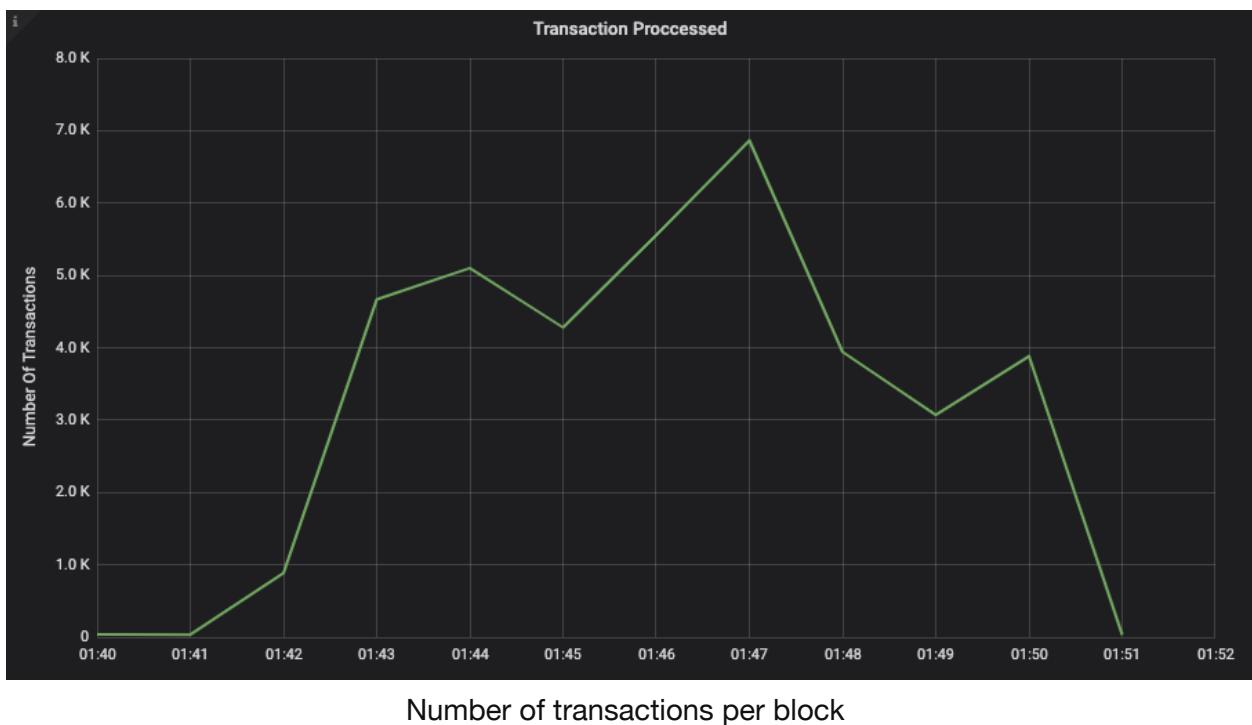
¹⁶ <https://download.slock.it/public/DAO/WhitePaper.pdf>

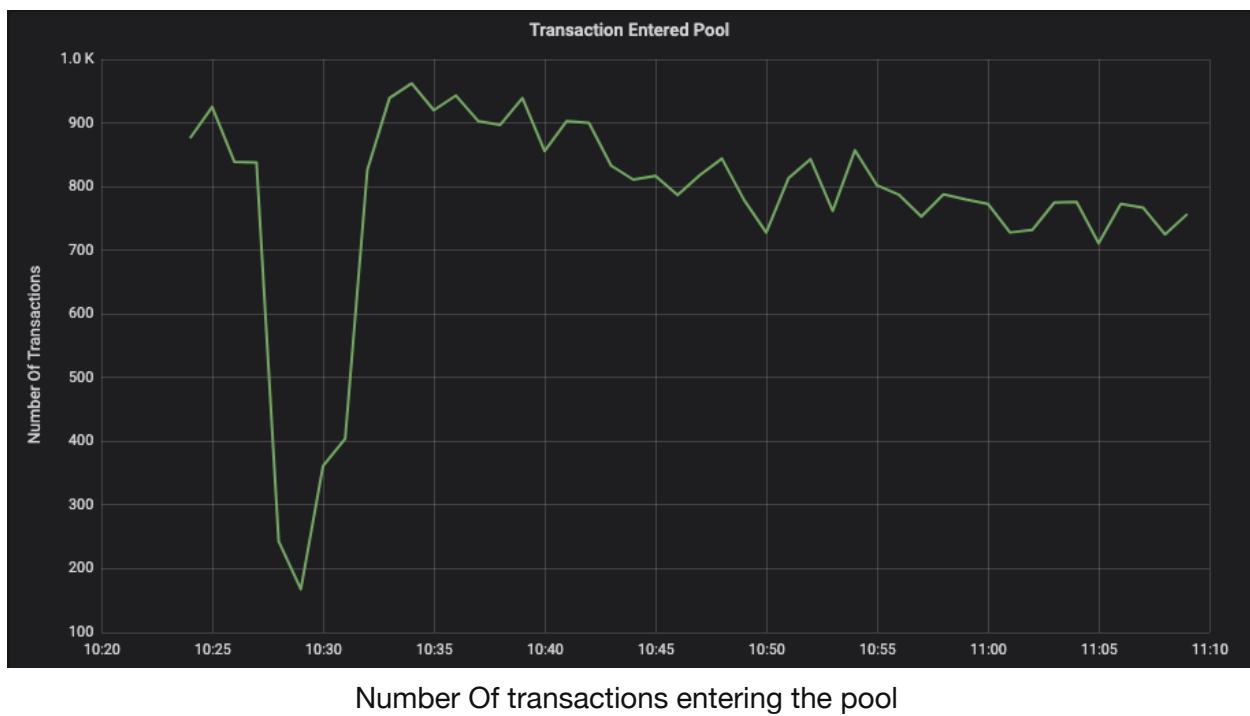
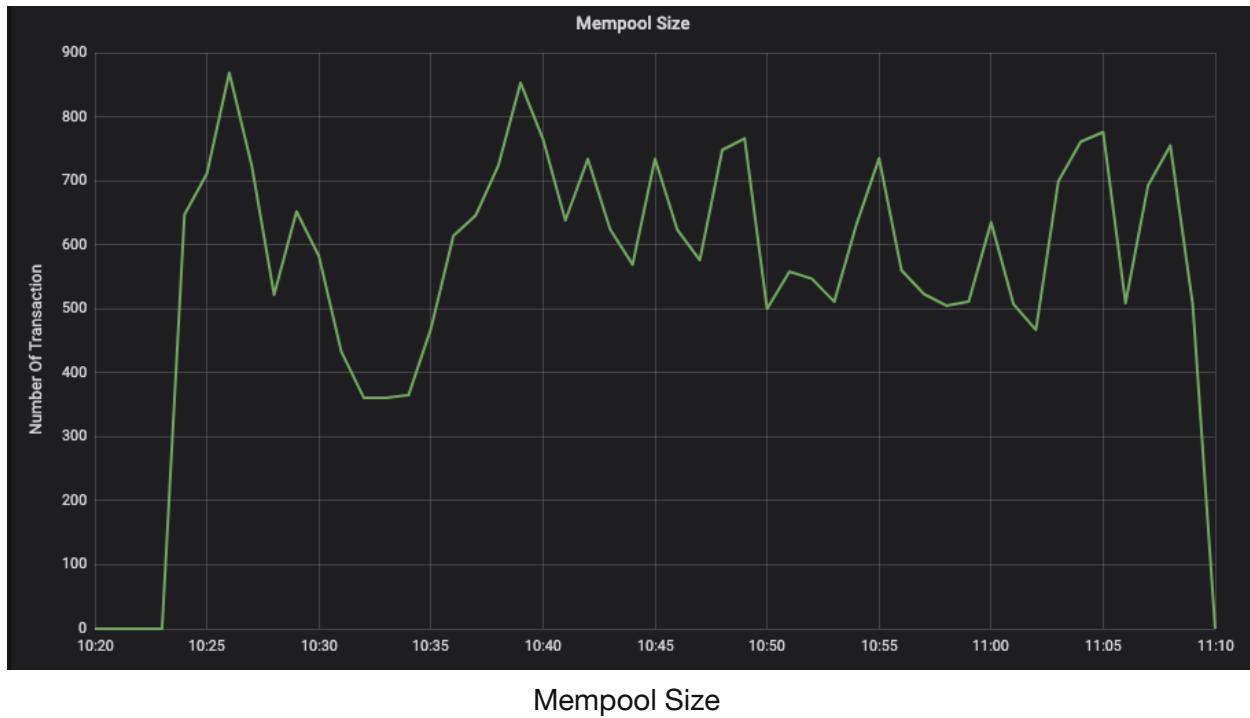
¹⁷ <http://mason.gmu.edu/~rhanson/ideafutures.html>

¹⁸ <https://www.augur.net>

¹⁹ <https://gnosis.io/>

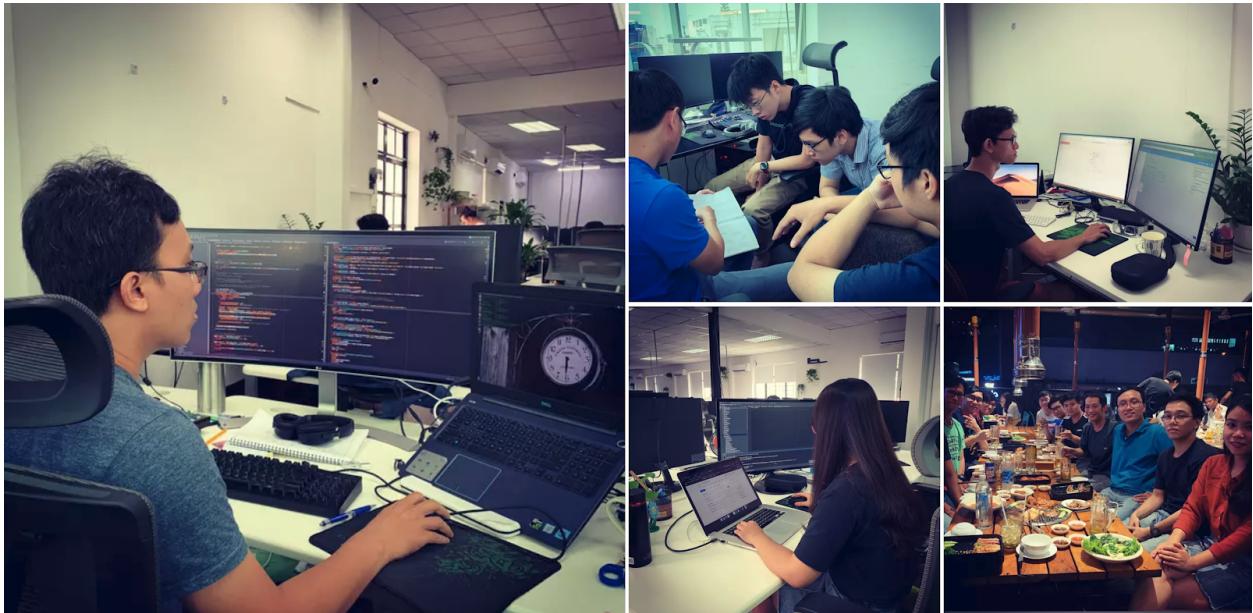
descending gradually to 5 tx/s over 3 hours. The finality times, transactions per block, and mempool size are shown in the following figures:





Team

We're a diverse team of 23 cryptographers, distributed system researchers, programmers and hardware makers. We're committed to building and sustaining 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 longest chain is considered final. In the event that there are multiple such chains of equal length, the one that obtains the most signatures is considered final.
- Slashing conditions - if a validator is voting for multiple conflicting blocks at the same time, its entire deposit will be deleted.

Risk 2: Single shard attack

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

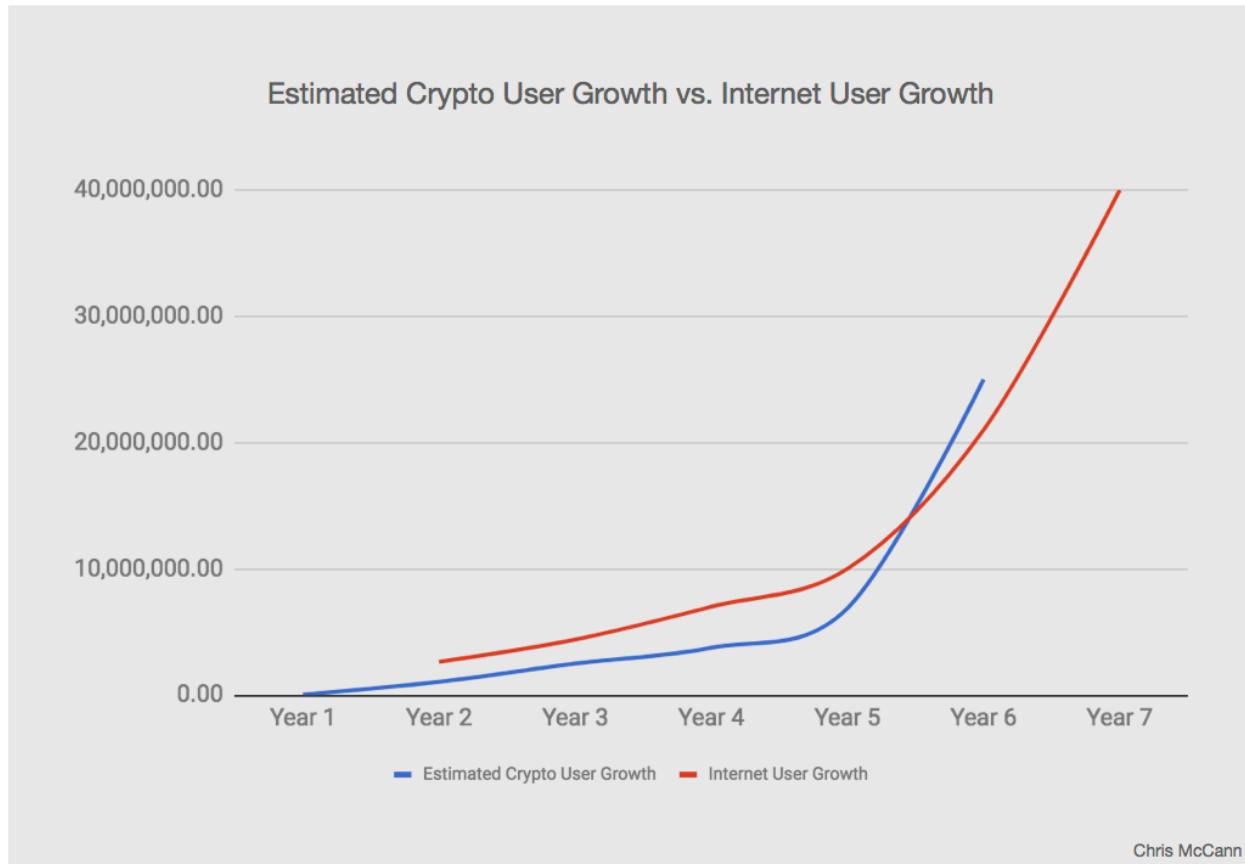
Potential solution: We'll randomly sample all validators. This way, the chances of a shard committee of size N being more than 50% corrupted by an attacker with p% of the global stake pool, are fairly low:

	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 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.



Crypto assets are increasing in number every day. Some of them wrap around existing assets like fiat (TUSD) and gold (DGX) and make them more efficient. Some of them introduce entirely new asset classes, like programmable governance tokens (MKR). If this development trend continues, as we believe it will, crypto assets are likely to play very important role in the near future. It is not far fetched to estimate that crypto assets will increasingly compose an individual's net worth, or a company's balance sheet.

Incognito hopes to give these assets and their owners - both now and in the future - the option to claim their right to privacy.

Parameters

NUMBER OF SHARDS	256
MINIMUM STAKING - SHARD	1,750 PRV
NUMBER OF SHARD NODES	Dynamic
SHARD REWARD WEIGHT	1
NUMBER OF BEACON	1

MINIMUM STAKING - BEACON	5,250 PRV
NUMBER OF BEACON NODES	Dynamic
BEACON REWARD WEIGHT	2
BLOCK TIME	~10 seconds
BLOCK REWARD	0.4 PRV (reduced by 12.5% annually)
TOTAL REWARD	BLOCK REWARD + TRANSACTION FEES
DEVELOPMENT FUND	5% OF TOTAL REWARD
GROWTH FUND	5% OF TOTAL REWARD
VALIDATOR REWARD	90% OF TOTAL REWARD
REWARD	VALIDATOR REWARD / (NUMBER OF SHARDS * SHARD REWARD WEIGHT + NUMBER OF BEACON * BEACON REWARD WEIGHT)
SHARD NODE REWARD	SHARD REWARD WEIGHT * REWARD / NUMBER OF SHARD NODES
BEACON NODE REWARD	REWARD * BEACON REWARD WEIGHT / NUMBER OF BEACON NODES
EPOCH LENGTH	~34,560 blocks (~4 days)