Manifesto

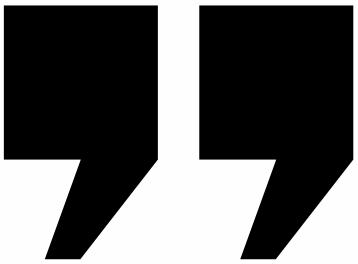
AUTHORS: [REDACTED]

VERSION: **3.0.1**

CIPHER: **6d617920637279707 46f20676f206461726b**

PROJECT: [REDACTED]

Foreword



Privacy is not something that I'm merely entitled to, it's an absolute prerequisite.

- Marlon Brando

Today, privacy is a scarce commodity. For many of us, it is often a privilege way out of reach; an intangible and desirable **freedom** we so desperately crave but don't seem to be able to obtain. Even when privacy is prioritised, developed and integrated by the few, the centralised totalitarian agenda forcefully quash it with haste. If the modern world hadn't already caused your internal self-sustaining alarm bells to start ringing, then you should probably wake up. Privacy is a fundamental human right. Without it, our whole lives are open books to any whom claim the authority to read them. The same principles **must** be applied to blockchain. Without default privacy, the decentralised revolution cannot be *truly* decentralised nor a revolution.

Allow us to introduce ourselves...

We are the ***CIA Collective***.

We are anon.
We are anarchists.
We are activists.
We are teachers.
We are students.
We are developers.
We are builders.
We are families.
We are friends.

Whoever we really are, whatever we really do, together we all make up the ***CIA Collective.***

As once separated and isolated actors in crypto; running our own teams, building our own protocols and obtaining our own freedom, we have assembled together through a common passion for **true** decentralisation to provide the same freedom to all.

Origin story out of the way, what is important is: The Collective is a living, breathing agenda for a fairer world fighting for the absolute right to privacy. Both we the anon founders, and you the speculative investor/empathetic privacy advocate make up The Collective. It is our mutual responsibility, and absolute duty to push, engineer and rightfully offer decentralised privacy to the masses.

Our mission is simple: ***to eradiate the unjust by building unstoppable, privacy-enabling decentralised protocols on Ethereum.***

Conspiracy ~ the first Ethereum-native privacy DEX, will be the pioneering illustration of our agenda. We hope this will serve as the idea that will spark the brains of the many to join us on our mission.

EDIT: *The unjust arrest of Tornado Cash co-founder Alexey Pertsev is a reminder to us all of the gravity of our situation in this very moment. Code is speech. We must act quickly.*

An outright ***Conspiracy***

Conspiracy is an Ethereum native privacy DEX that increases on-chain anonymity of DEX traders. By merging the well established AMM with zk-SNARKs, conspiracy is able to fragment the on-chain link between a trader and their trading activity.

Conspiracy is necessary.

Private trading is normal in centralised environments, and even in crypto. Centralised instutions and exchanges by design enable privacy and anonymity for their end users. Decentralised trading however is tainted with the optionless publishing of your entire transactional history. Anyone, friend or foe, can view your whole financial activity with just a few clicks should they link your wallet to your real or pseudonymous identity. When you think about it, this is a massively undiscussed and closed topic in the social circles of the crypto industry.

Wallet doxxing is a direct and present threat to your decentralised financial wellbeing. Financially astute players have, in the past, fallen victim to many attack vectors because their wallets were linked to their institutional or personal identity. When long or short positions are exposed publicly, a systemic risk of targeted liquidation through price manipulation arises. Malicious actors are always waiting for these opportunities, especially when it comes to big wallets. Attempts at hacking via malicious ERC-20 transfers and deliberate targeted frontrunning (to liquidate) are just two methods that have succeeded in harming a doxxed individual or institution on-chain.

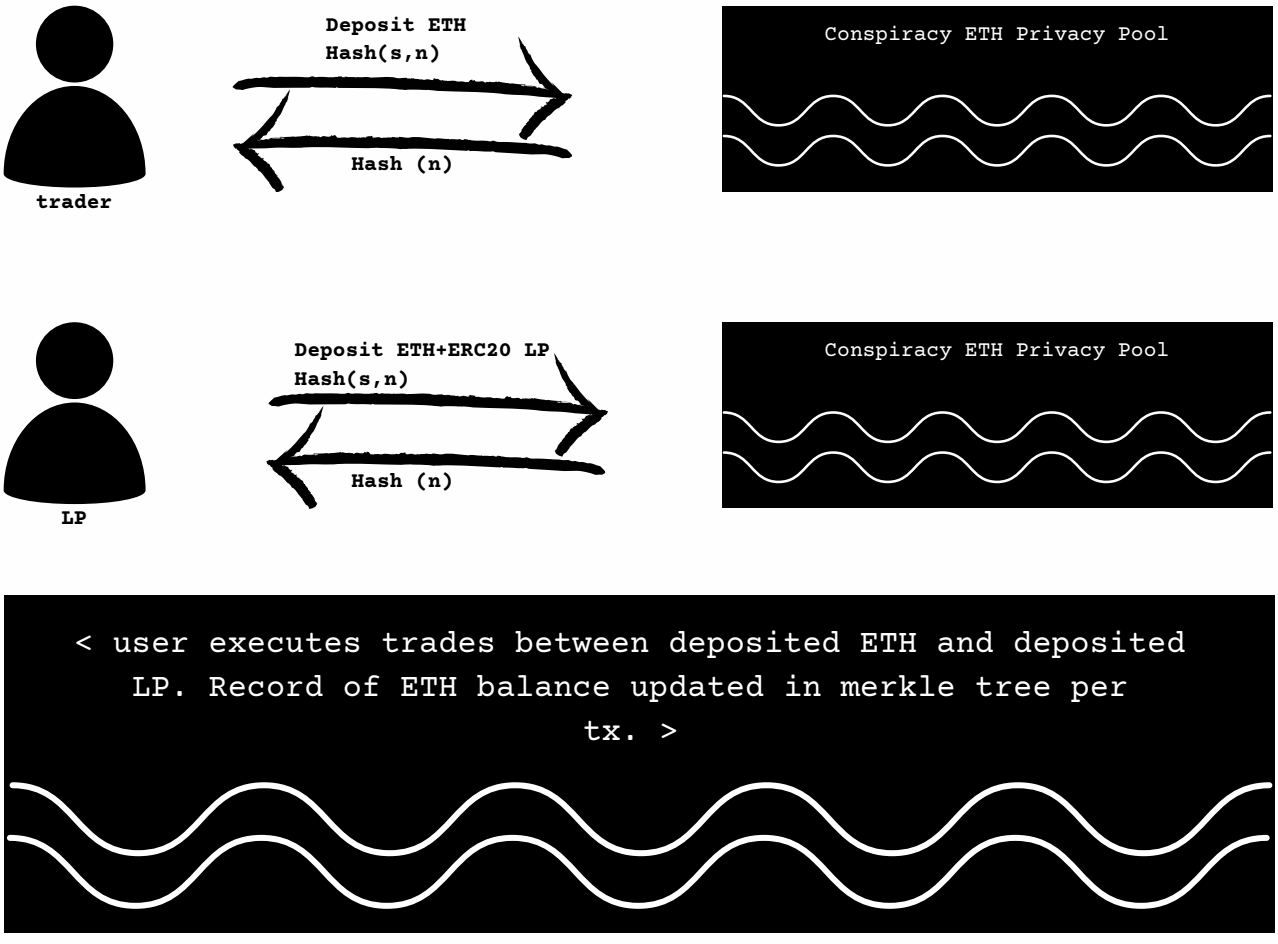
Wealth origin and investment positions are also threats to your right to privacy and ultimately, your fredom. It is not necessary that anyone and everyone is free to trace the origins of your wealth, not even on the blockchain.

Architecture

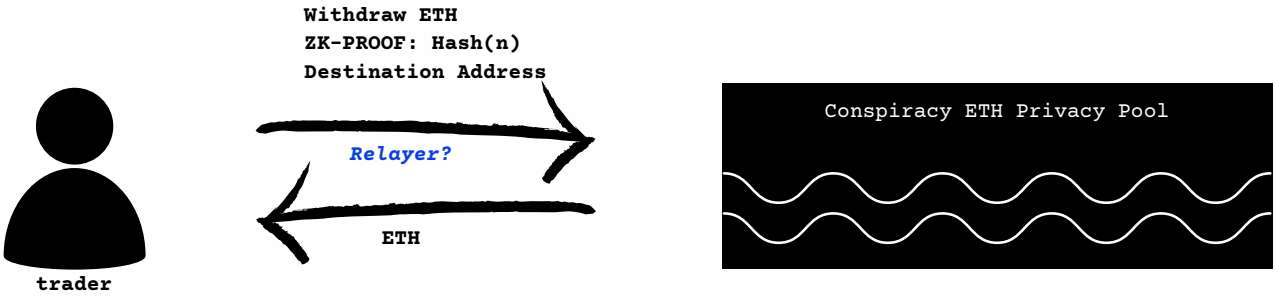
When we first began digressing the under-the-hood mechanics of Conspiracy to The Collective, we drew close comparisons to Tornado Cash and for good reason. Conspiracy works in a similar way, more specifically to Tornado Nova.

ETH is the primary currency utilised for LP pairings on DEXes like Uniswap. Likewise, Conspiracy will have an ETH pool where users can deposit arbitrary amounts of ETH along with a commitment - hash(secret, nullifier). This hash is the encrypted computation of two random numbers (secret and nullifier), of which a record is stored on-chain in a merkle tree which is made up of multiple commitments. The secret and nullifier are composed of key information such as the depositors public key, from which Conspiracy is aware that a user has rights to shielded ETH when logged in to Conspiracy. While within the pool, a user can perform shielded swaps with any token deposited into the pool that has ETH liquidity assigned to it (LP also deposits with a commitment to prove they are the LP).

Deposit:



Withdrawal:



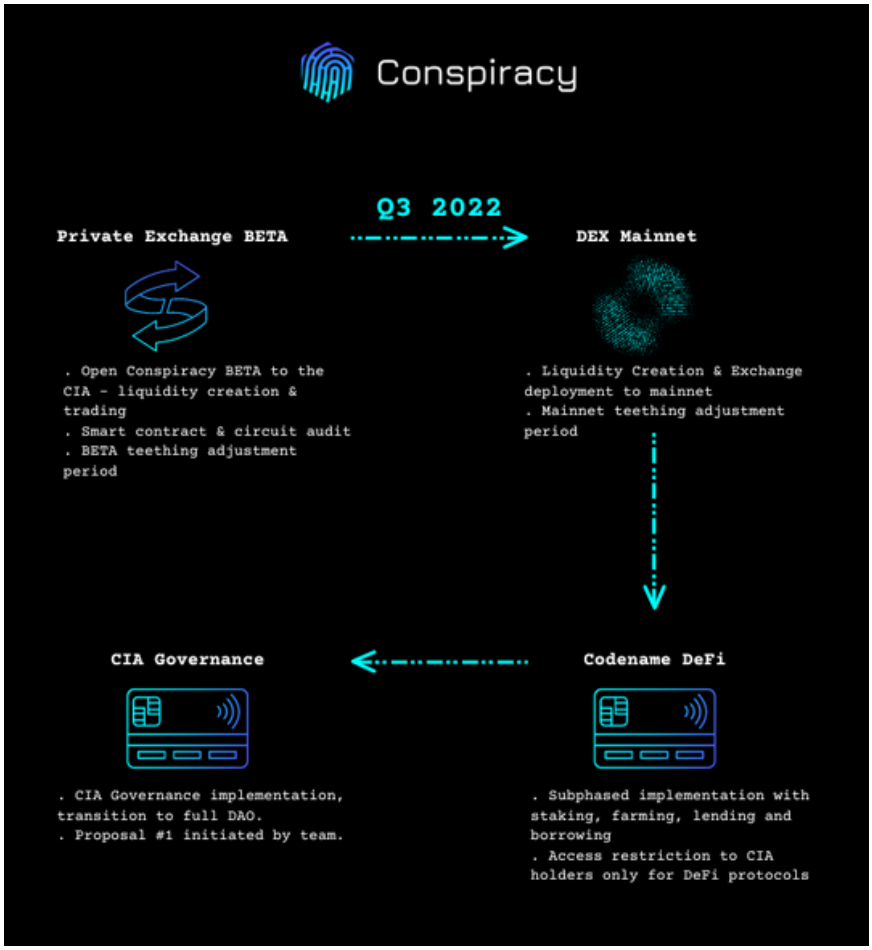
Relayers are an optional withdrawal method. They are not needed to break the link between a source and destination address, however they are needed to ensure (New) address anonymity retains. This is called the gas fee dilemma. In order to withdraw ETH from a Conspiracy Privacy Pool (or execute any wr- transaction on Ethereum for that matter) a gas fee must be paid. If a relayer was not used, then the destination address needs ETH to pay the gas fee. The gas fee dilemma is - the source of the ETH funded to the wallet, perhaps from a CEX, could lead to personal identification. However, unless you're doing something illegal - there's no reason for the ETH source (e.g. a CEX) to divulge the personal information linked to your wallet to anybody.

For these reasons, we won't be using relayers in our first release of Conspiracy. Note however that relayers can be implemented and even made the default withdrawal solution should the community pass a vote on it in governance.

NOTE: The beauty of deposits with arbitrary amounts into Conspiracy is that trading (most probably) always results in a different balance post trade. To maintain anonymity, a user should always deposit and withdraw with both different addresses and also different amounts to avoid detection. This is one of many tips that can be used to maximise anonymity, read further on to learn others.

Roadmap

Conspiracy is set to enter an ALPHA deployment state on Rinkeby testnet. While the dApp will be in an alpha state, this will essentially be the BETA phase for ***The Collectives*** first privacy centric implentation on Ethereum. **Dark** times!



This roadmap is partially conditional. Due to recent events and with our ever evolving nature as a team, **Codename DeFi** is now a conditional implementation. It is conditional upon the adoption (and therefore success) of Conspiracy as an isolated decentralised exchange, absent of 'extra' DeFi. Governance however will be shipped with mainnet release to ensure protocol perpetuity.

Fees apply two-fold in Conspiracy.

On the 'zk level' - ETH deposits are subject to a 0.5% fee, which are rewarded proportionally to CIA stakers. On the 'DEX level', a 0.5% fee is applied to swaps, rewarded proportionally to liquidity providers. Many will notice this is a slightly higher fee than *most other DEXes in the market yet is probably not considered substantial when applied to arbitrary amounts. A price must be paid to harvest the wonders of a private DEX, and it is **The CIA Collective** and liquidity providers which shall reap the rewards.

NOTE: Fee structure modification has renounced the founding team from receiving any operational reward due to potential legal implications.

DISCLAIMER: While Conspiracy will increase the anonymity of a DEX user, it/we cannot guarantee absolute untraceability or anonymity. To massively increase your chances of detection, we recommend the following additional tips:

- Deploy your own UI mirror of Conspiracy on IPFS (code will be open source and instructions equipped).
- Use a VPN service like Proton.
- Use a private browser such as Tor, or make sure to block cookies and 3rd party trackers.
- Clear your browser cookies.
- Run your own Ethereum node to avoid routing through centrally owned nodes such as Infura and Alchemy.
- Wait sufficient time between deposit and withdrawal (or as an extra measure participate when pools are high in velocity).
- Ensure deposit and withdrawal amounts are very different.
- Ensure deposit and withdrawal addresses are different.

Decentralised **Governance**

Governance is what forms our cohesion on-chain. We are able to procure upgrades, make changes and add enhancements should we collectively decide to do so. $CIA will forever remain the asset that drives our collective governance, ultimately driving our success in eradicating centralised autocracy and implementing privacy preserving protocols on Ethereum and beyond.

We earlier mentioned a change in fee structure. Yes - CIA stakers will be proportionally distributed a 0.5% of all ETH deposits into the ETH Conspiracy Privacy Pool; a small price to pay for the freedom of privacy. We recently removed founder fees from the DEX in order to preserve our long term anonymity for legality and traceability purposes. $CIA holders are now the only players with the power and the keys to the universe.

Stakers will also be issued an equivelent amount of $dCIA (**dark CIA**) which will provide voting power to all, and in alignment - proposal power to those holding over the 1.5b (1.5% total supply) minimum threshold.

NOTE: (for the inevitable profiteers) Staking $CIA will effectively take supply out of circulation and in return, provide ETH rewards and right to governance.

On-chain variables upgradeable by $dCIA holders:

- Fees (both deposit and swap)

Arbitrary proposal ideas (relatively unlimited):

- Implement relayers
- Make relayers default
- Alt chain deployment

IMPORTANT: Any privacy protocol implemented by ***The Collective*** in the future through internal technical contributions or via outsource MUST adopt the same $CIA governance principles to maintain the decentralised power balance.

A **Dark** [REDACTED] Future

As founders we will take unprecedented steps to solidify the perpetuity of Conspiracy and $CIA - we must never be taken offline. Steps will be taken to preserve all $CIA artefacts, both open source code and non-technical documentation (such as this manifesto) must sustain. It is the duty of ALL of us to participate in these survival activities if we **truly** want privacy for all.

Here's what we will do as founders:

- Maintain personal anonymity.
- Increase online $CIA related privacy measures.
- Upload mirrors of all founding documentation and code to IPFS.

Here's what you can do:

- Download, and re-upload all documentation and code to IPFS.
- Take snapshots of $CIA social accounts and open source code using web.archive.org.
- Maintain your own personal anonymity.
- Protect $CIA at all costs!

Once governance kicks in with mainnet operations, we will **all** equally responsible for $CIA operations. As founders we are just facilitators, but we are $CIA contributors same as you. At this stage, operations become the core responsibility of the $CIA holder and contributor. We must continue to talk about $CIA.

Potential Developments

$CIA must not stop at Conspiracy to bring privacy to the Ethereum world; this is merely a first implementation from us all as a single agenda. The Tornado Cash atrocity has awoken many to the persecution that the most innocent of us face. Privacy is **not** a crime.

Privacy != Criminality

A zk cross-chain bridge would be a logical evolution for a second privacy installation on Ethereum. This would be a relatively simple implementation, working just like a mixer.

Stay frosty anon.