Five Paths

Contents

Privacy has typically underperformed in crypto, whereas it should be the primary moving feature that unlocks crypto's true potential.

My belief is this is because we haven't yet seen any true applications of privacy along this line that are exciting. Simply making payments private is not enough of a killer usecase (which is captured by Monero anyway). It requires a fullstack of apps.

DarkFi's aim is then to unlock this paradigm and take crypto to the next level. But in order to do this, we must:

1. Make lots of money so we are not resource constrained.
2. Become a cultural movement through aesthetics and propaganda.
3. Rapidly prototype MVPs that are fielded in the market.

Tech

DarkFi has:

- Its own L1 blockchain with 120s blocktimes PoW merge-mined with Monero as a distribution method. Later we can switch to a fast finality PoS with short blocktimes.
- Our own p2p layer with data availability both for rolling streamed data and static data. For example to support high throughput short lived data like chats, or for long term static data like images.
- Extensive ZK tooling and ZKVM for making anonymous applications.

In terms of apps, currently we have:

- World's first and only anonymous DAO.
- On-chain atomic swaps.
- Anonymous token issuance and payments.
- p2p anonymous chat + tasks system.
- Anonymous p2p filehosting.

Planned:

- Orderbook
- Bridges

Future apps:

- Marketplace for buy/sell goods and OTC.
- Information markets

Audience

Core audience:

- Trendy eth cypherpunks. Our video "Lunarpunk and the Dark Side of the Cycle" (rekt) brought cypherpunk forwards within Eth as a cultural force.
- Monero chads and privacy extremists.
- Incel chuddies, ancap techbros, and schizos.

Our next key target is dissident populism which is a large untapped retail market potentially.

Possible Paths

Currently our app is focused on the first usecase.

Social Media Marketplace

Our current plan is something like Telegram with apps inside such as wallets and markets. But with more emphasis on the apps rather than the chats. That is we build communities with monetization possibilities.

Facebook has its marketplace. People host pages selling goods. The idea is then through our app, you can find goods to buy/sell, or do OTC. There can even be a DEX for trading inside the app.

This plan means we focus firstly on communication and community.

Anon Stablecoin Payments

We issue our own stablecoin on DarkFi, backed with a treasury reserve with bid/put to maintain price parity.

Anonymous DEX + Orderbook

We have the pieces to construct a DEX, with the only missing pieces being the orderbook and bridges. Then people will be able to login to the app and trade anonymously.

However the orderbook offers will be public. But everything else private. You can even have private orderbooks to advertise offers.

Anonymous Auction

The advantage of auctions is that the offers remain private, however when you make a bid in an auction, your funds remain locked up for the duration of the auction.

Anonymous auctions most importantly can hide the trade volume (amount). Basically the one offering liquidity has their position hidden, and we can anonymously fill the position until it is closed.

ZK Hyperliquid with Leverage

This was the original founding vision of DarkFi, however we ended up generalizing to becoming an actual L1 with programmable smart contracts.

This would be an anonymous hyperliquid with perps and futures, and leverage. However to make this possible, we may need some kind of fast L2 sidechain.

Essentially it would be a no-KYC bitmex without frontrunning, or any positions being visible. However you would still need custodial bridges.