fun.xyz

About fun.xyz

Fun.xyz builds a product ecosystem that leverages cross-chain decentralized wallets on the Odsy blockchain. All products either decentralize multi-chain interoperability or decentralize core web2 account services (teams, roles, account recovery, permissioning, etc.).

The Problem

In web3 today, multi-chain interoperability and basic account services are only possible with an equal serving of centralization.

Vectors of centralization go against the ethos of blockchain technology, which strives for a completely trustless and permissionless future. These vectors of centralization are only successful as long as there are no suitable decentralized alternatives. When decentralized competitors arise, it is often the case that they quickly overtake their centralized counterparts. We have seen this series of events play out many times throughout the short-lived history of crypto. For example, cryptocurrency exchanges were initially exclusively built in centralized ways, however, with their success came the incentive to build decentralized alternatives. Now DEXs account for 50% of on-chain volume as well as allow for long tail token offerings unavailable in centralized, permissioned exchanges.

It often makes sense to build new features in a centralized manner, as the system design is more straightforward and there are scaling efficiencies. However, if history is any guide, for every centralized solution that pops up, you can count on there being a decentralized alternative that will one day be ready to eat its lunch.

We have identified 2 areas in the blockchain space where

© 2022 The Fun Group, Inc.

centralization is still pervasive and ready for disruption: multi-chain interoperability and basic account services.

Multi-Chain Interoperability

At this stage in the blockchain experiment, it is becoming clear that the future is increasingly multi-chain: Bitcoin is great at monetary policy but can't handle the expressive needs of DeFi and NFTs. Ethereum is great at providing a secure and decentralized Turing-complete settlement layer but is bound by the limits of the EVM. Solana has incredible transaction throughput but achieves it by compromising on decentralization. Whatever blockchain you choose, there will be pros and cons, tradeoffs which make it excel at one task but underperform on another. In order to take advantage of everything that blockchain technology has to offer, there is no doubt that the future will be multi-chain.

There is a reason why people refer to the "Multi-chain future" as opposed to the "Multi-chain present". Although there are ways for independent blockchains to talk to each other today, the messaging is done in suboptimal ways which leverage centralization. According to Chainalysis, cross-chain bridge hacks have to-date resulted in over $2B of compromised user funds. This is because centralized solutions are often accompanied by centralized points of failure. We believe this is an area which is ripe for decentralized disruption.

Core Web2 Account Services

The centralized crypto custodians of the world have added all the functionality that comes with a traditional web2 account, including 2-factor authentication, account recovery via password reset as well as

© 2022 The Fun Group, Inc.

intuitive user interfaces. On top of this base web2 account functionality, centralized custodians have also begun to add more crypto-native functionality to their user's accounts, including staking, lending and borrowing as well as MPC for added security. While the crypto-native functionality offered by centralized custodians faces very real competition from decentralized alternatives, the traditional web2 account functionality is something that dApps have struggled to compete on and is the primary reason why centralized custodians retain their market share.

In order for trustless and permissionless blockchain technology to fully go mainstream and onboard the next 8 billion users, it will have to be accompanied by all of the base web2 functionality which users have come to expect from software service providers. We believe this is an area which is ripe for decentralized disruption.

The Technology

Decentralized wallets, or dWallets for short, have a set of native improvements over legacy account types. First, there is no single point of failure, as secret shares are distributed. Next, they are natively multi-chain while still being turing-complete, which allows for expressive Access Control Schemas. Finally, they allow for trustless account transferability

Because of these improvements, dWallets will become a fundamental piece of blockchain infrastructure. These new account types are being engineered by a team of world-class cryptographers at Odsy, with a founding team including the former founder & CEO of a $1B+ cybersecurity company and the ex-CEO of the Algorand Foundation. They will give blockchain developers access to a new primitive

© 2022 The Fun Group, Inc.

building block, the dWallet, which will allow for never-before-possible decentralized use-cases to be built. The use-cases we are most excited about are those which enable the decentralized revolutions mentioned in the preceding section: Multi-Chain Interoperability and Basic Account Services, we will get more into the details on how we leverage dWallets to solve these problems in the next section.

The team at Odsy makes all this possible by combining the powers of blockchain technology and multi party computation (MPC) to sign transactions for other target blockchains, for example, Ethereum, Solana or Bitcoin. This works by having the private key corresponding to the target blockchain accounts stored via MPC. MPC “breaks-up” a private key into multiple “secret-shares”; when a threshold of secret-share holders partially sign a message on top of eachother, this is equivalent to the original private key having signed the message. Odsy gives the creator of a dWallet a secret share accounting for 50% of the signing weight and distributes the rest of the secret shares, comprising the other 50% of the signing weight, to the blockchain validators. When a user wants to perform a transaction on a target blockchain via their dWallet, they first partially sign the transaction, then send it to the Odsy blockchain which will complete the transaction signing by coordinating the relevant nodes to partially sign the message. The system is built in such a way that no compromise of the network secret shares would ever compromise the user’s accounts on any blockchain.

Our Role

We are excited to be an early partner of Odsy, with plans to build out the application layer on top of dWallets. For the short term, our roadmap is focused on fun.xyz lab projects which we believe will have

© 2022 The Fun Group, Inc.

a huge impact on the ecosystem while themselves being relatively straightforward to implement. Our longer term vision includes projects which will be comparable in terms of impact but will require longer research and development timelines.

© 2022 The Fun Group, Inc.