secret

Privacy for this builders market

Gijs - Ertemann

Gijs - Ertemann | Developer relations

Cosmos Tech stack maximalist

Education fanatic

Background in physics and Machine learning

full-time web3 since early 2022

Privacy aficionado

Sean Conrad | Developer relations

abandoned solidity for Privacy

Video wizard

Loves the Rust compiler

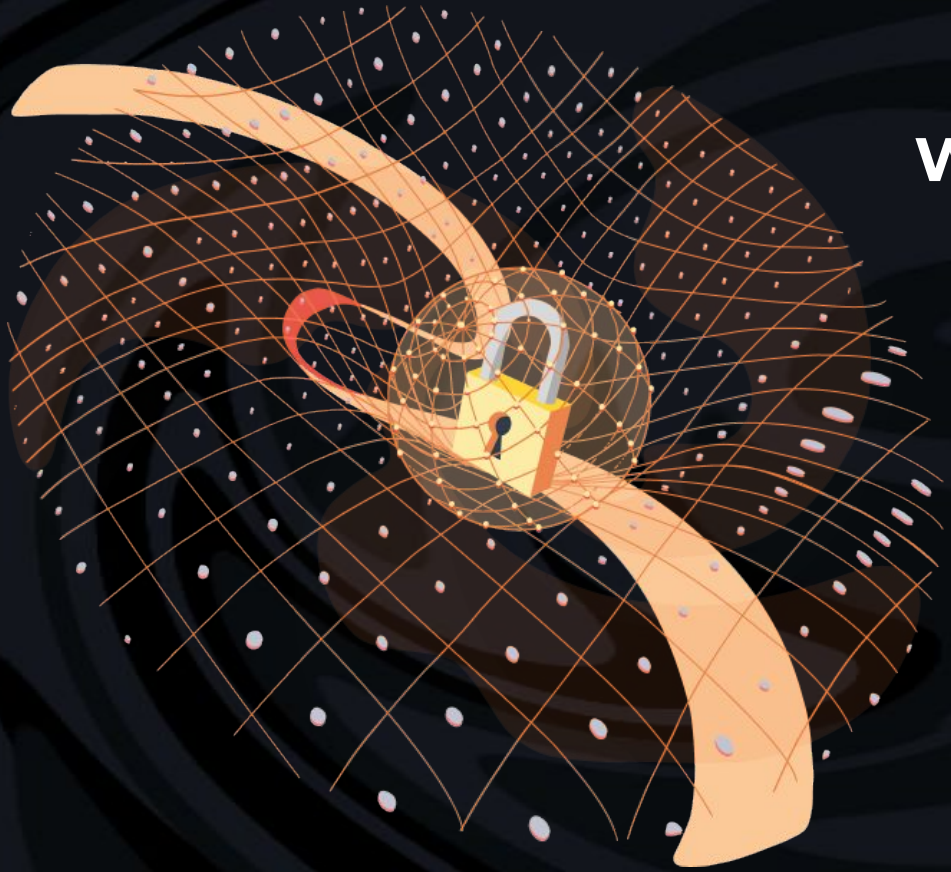
Joined Secret early 2023

Builds dApps for (grand)ma and pa

WELCOME TO SECRET NETWORK

The Data Privacy Platform For Web 3

Secret Network is the first blockchain with **data privacy by default**, allowing you to build and use applications that are both permissionless and privacy-preserving. This unique functionality protects users, secures applications, and unlocks hundreds of new use cases for Web 3.

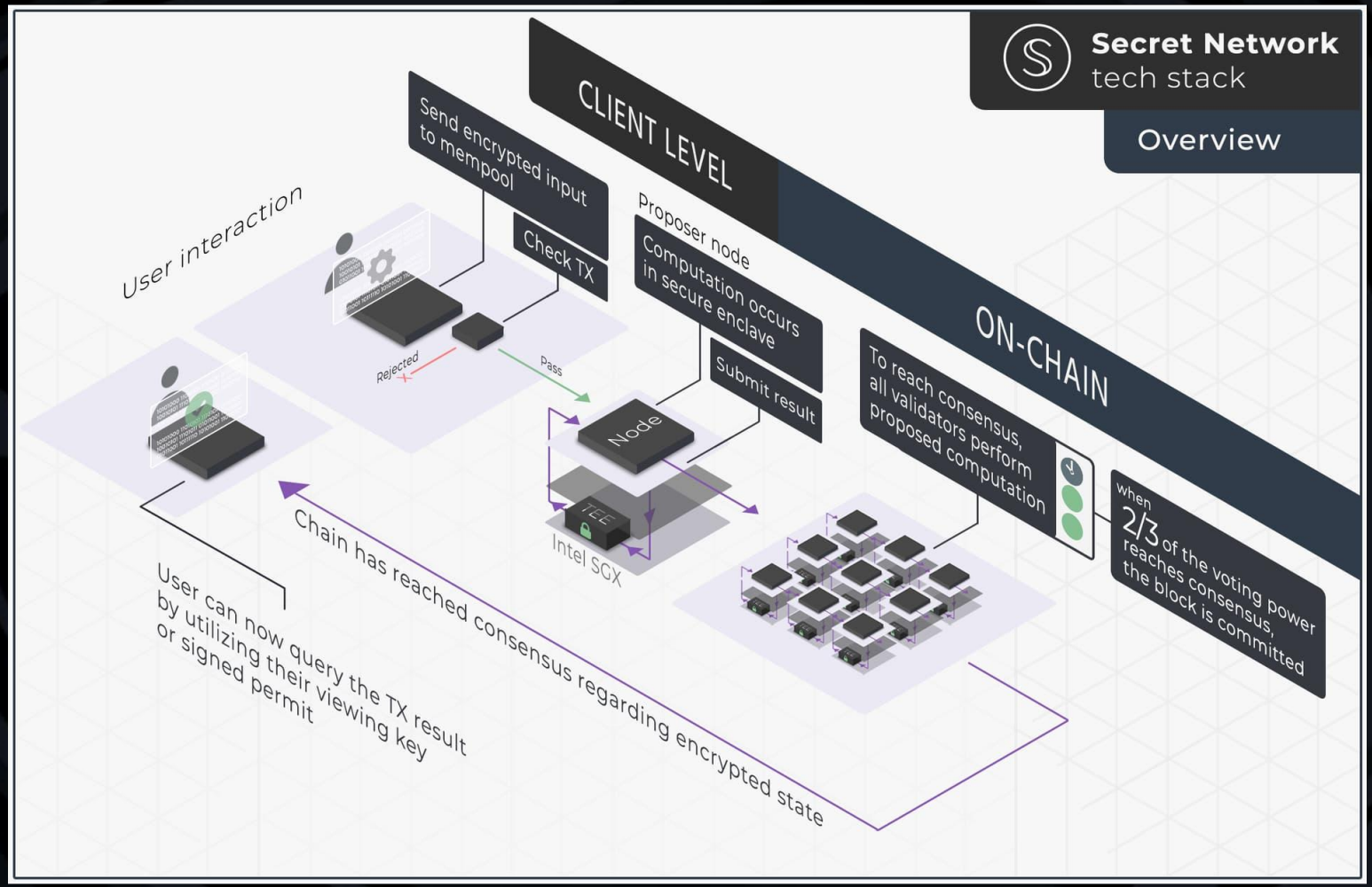


Why web3 privacy matters

- Censorship resistance
- Fungibility
- Security - removal of middleman
- True ownership
- Disconnect from action history

And most importantly:

- Feature parity - web2


Secret Network
tech stack
Overview
CLIENT LEVEL
ON-CHAIN
User interaction
Send encrypted input to mempool
Check TX
Rejected
Pass
Proposer node
Computation occurs in secure enclave
Submit result
Node
TEE
Intel SGX
To reach consensus, all validators perform proposed computation
when 2/3 of the voting power reaches consensus, the block is committed
Chain has reached consensus regarding encrypted state
User can now query the TX result by utilizing their viewing key or signed permit

CosmWasm

Cosmos SDK

Tendermint Core

IBC Protocol

2015 IEEE CS Security and Privacy Workshops

Decentralizing Privacy: Using Blockchain to Protect Personal Data

Guy Zyskind
MIT Media Lab
Cambridge, Massachusetts
Email: guyz@mit.edu

Oz Nathan
Tel-Aviv University
Tel-Aviv, Israel
Email: oznathan@gmail.com

Alex 'Sandy' Pentland
MIT Media Lab
Cambridge, Massachusetts
Email: pentland@mit.edu

***Abstract*—The recent increase in reported incidents of surveillance and security breaches compromising users' privacy call into question the current model, in which third-parties collect and control massive amounts of personal data. Bitcoin has demonstrated in the financial space that trusted, auditable computing is possible using a decentralized network of peers accompanied by a public ledger. In this paper, we describe a decentralized personal data management system that ensures users own and control their data. We implement a protocol that turns a blockchain into an automated access-control manager that does not require trust in a third party. Unlike Bitcoin, transactions in our system are not strictly financial – they are used to carry instructions, such as storing, querying and sharing data. Finally, we discuss possible future extensions to blockchains that could harness them into a well-rounded solution for trusted computing problems in society.**

***Keywords*—blockchain; privacy; bitcoin; personal data**

I. Introduction

The amount of data in our world is rapidly increasing. According to a recent report [22], it is estimated that 20% of the world's data has been collected in the past couple of years. Facebook, the largest online social-network, collected 300 petabytes of personal data since its inception [1] – a hundred times the amount the Library of Congress has collected in over 200 years [13]. In the Big Data era, data is constantly being collected and analyzed, leading to innovation and economic growth. Companies and organizations use the data they collect to personalize services, optimize the corporate decision-making process, predict future trends and more. Today, data is a valuable asset in our economy [21].

While we all reap the benefits of a data-driven society, there is a growing public concern about user privacy. Centralized organizations – both public and private, amass large quantities of personal and sensitive information. Individuals have little or autonomous deployment of a PDS which includes a mechanism for returning computations on the data, thus returning answers instead of the raw data itself [6]. Across the industry, leading companies chose to implement their own proprietary authentication software based on the OAuth protocol [19], in which they serve as centralized trusted authorities.

From a security perspective, researchers developed various techniques targeting privacy concerns focused on personal data. Data anonymization methods attempt to protect personally identifiable information. *k-anonymity*, a common property of anonymized datasets requires that sensitive information of each record is indistinguishable from at least $k-1$ other records [24]. Related extensions to *k-anonymity* include *l-diversity*, which ensures the sensitive data is represented by a diverse enough set of possible values [15]; and *t-closeness*, which looks at the distribution of sensitive data [14]. Recent research has demonstrated how anonymized datasets employing these techniques can be de-anonymized [18], [5], given even a small amount of data points or high dimensionality data. Other privacy-preserving methods include *differential privacy*, a technique that perturbs data or adds noise to the computational process prior to sharing the data [7], and encryption schemes that allow running computations and queries over encrypted data. Specifically, fully homomorphic encryption (FHE) [9] schemes allow any computation to run over encrypted data, but are currently too inefficient to be widely used in practice.

In recent years, a new class of accountable systems emerged. The first such system was Bitcoin, which allows users to transfer currency (bitcoins) securely without a centralized regulator, using a publicly verifiable open ledger (or *blockchain*). Since then, other projects (collectively referred to as *Bitcoin 2.0* [8]) demonstrated how these blockchains can serve other functions requiring trusted computing and

Enigma: Decentralized Computation Platform with Guaranteed Privacy

Guy Zyskind **Oz Nathan** **Alex 'Sandy' Pentland***

Abstract

A peer-to-peer network, enabling different parties to jointly store and run computations on data while keeping the data completely private. Enigma's computational model is based on a highly optimized version of secure multi-party computation, guaranteed by a verifiable secret-sharing scheme. For storage, we use a modified distributed hashtable for holding secret-shared data. An external blockchain is utilized as the controller of the network, manages access control, identities and serves as a tamper-proof log of events. Security deposits and fees incentivize operation, correctness and fairness of the system. Similar to Bitcoin, Enigma removes the need for a trusted third party, enabling autonomous control of personal data. For the first time, users are able to share their data with cryptographic guarantees regarding their privacy.

1 Motivation

Since early human history, centralization has been a major competitive advantage. Societies with centralized governance were able to develop more advanced technology, accumulate more resources and increase their population faster [1]. As societies evolved, the negative effects of centralization of power were revealed: corruption, inequality, preservation of the status quo and abuse of power. As it turns out, some separation of powers [2] is necessary. In modern times, we strive to find a balance between the models, maximizing output and efficiency with centralized control, guarded by checks and balances of decentralized governance.

The original narrative of the web is one of radical decentralization and freedom[3]. During the last decade, the web's incredible growth was coupled with increased centralization. Few large companies now own important junctures of the web, and consequently a lot of the data created on the web. The lack of transparency and control over these organizations reveals the negative aspects of centralization once again: manipulation [4], surveillance [5], and frequent data breaches [6].

secret ecosystem

Visit **scrt.network** for a complete overview of the Secret ecosystem.

DEFI

- AmberDAO
- Blizzard
- Btn.group
- Kado
- Poolparty
- Secret Time Capsule
- Restake
- SecretSwap 2.0
- Selenian
- Shade Protocol
- Sienna Network
- Stake Easy
- Yieldmos

COMMUNICATION

- Abakhus
- Alter
- Dibs Domains (Secret DNS)
- Fardels

NFTS

- ActiList
- AnonDao
- Bidshop
- Cover
- CertUp
- Eqoty - Music
- IBC NFTs
- Killroy Was Here
- LegendDAO
- Stashh
- Tarantino NFTs
- V-IRL
- XP Network

GAMING

- Bushi/Onenet
- DreamScape
- Lorem Ipsum
- Secret Heroes

EXHANGES

- Binance
- Bitmart
- Button Swap
- Gate.io
- Huobi
- Kraken
- KuCoin
- Kujira FIN
- Mandala
- MEXC
- OkCoin
- JunoSwap
- Osmosis
- Sienna Swap
- Sifchain
- SushiSwap
- Uniswap

DATA SECURITY

- Data Vault
- Secret Bazaar

WALLETS & EXPLORERS

- Btn.group Tools
- Citadel.One
- Cosmostation/ Mintscan
- CryptoClerk
- Fina Cash
- Keplr
- Kryptic
- Leap Wallet
- MathWallet
- MetaMask
- Secret Ledger App
- SecretNodes
- Starshell
- Secret Analytics

BRIDGES

- Axelar
- Binance Smartchain
- Ethereum
- IBC
- Monero
- Snakepath TNLS

INFASTRUCTURE

- Agora Nodes
- Baedrick
- Blockpane
- Census One
- Chain of Secrets
- Forbole
- Lavender.Five
- Mr. Robot
- Quiet Monkey Mind
- Secret Chain Girl
- Secret Nodes
- Secret Saturn
- Stake or Die
- Stashh
- Support Team
- Trivium

RELAYERS

- Autostake
- CryptoCrew
- Lavender.Five
- PFC
- Stakelab

SECURITY / TOOLING

- Blackbox
- Packs DAO
- Prifi Labs
- ScrtSybil
- Secret DAO
- Serenity Shield
- Stakely
- Yoiu Launchpad

DEVELOPER TOOLING

- Ankr
- DDT Secret-rng
- Fadroma
- Griptape.js
- Polar Arufa Research
- Secret IDE
- Secret Javascript
- Secret .Net
- Secret Python
- Secret University

SUPPORTING ORGANIZATIONS

- Secret Agency
- Secret Foundation
- SCRT Labs

stashh

EOTY

V-IRL

Secret NFTs

- Public & private metadata
- Only visible to owner
- Access control
- Private ownership
- Ticketing/ RL access
- Evolving NFTs

ALTER NETWORK

A Decentralized Mnemonic Backup System for Non-Custodial Cryptocurrency Wallets

Data & Security

- Private voting DAOs
- Wallet Inheritance
- Communication/data storage
- MPC wallets
- Improved Domain services

BLIZZARD

Sienna

shade

Secret DeFi (PriFi)

- No front-running (encrypted mempool)
- Private holdings via Secret Tokens
- Private lending/borrowing positions
- Under Collateralized lending
- Sealed bid auctions

(Fully) Homomorphic encryption

Encrypt all data and compute over it

Slow but never lose privacy

(Secure) Multi Party Computation (MPC)

Disperse data over multiple people and they all compute part of the result

If people collude they know everything

Trusted Execution Environments

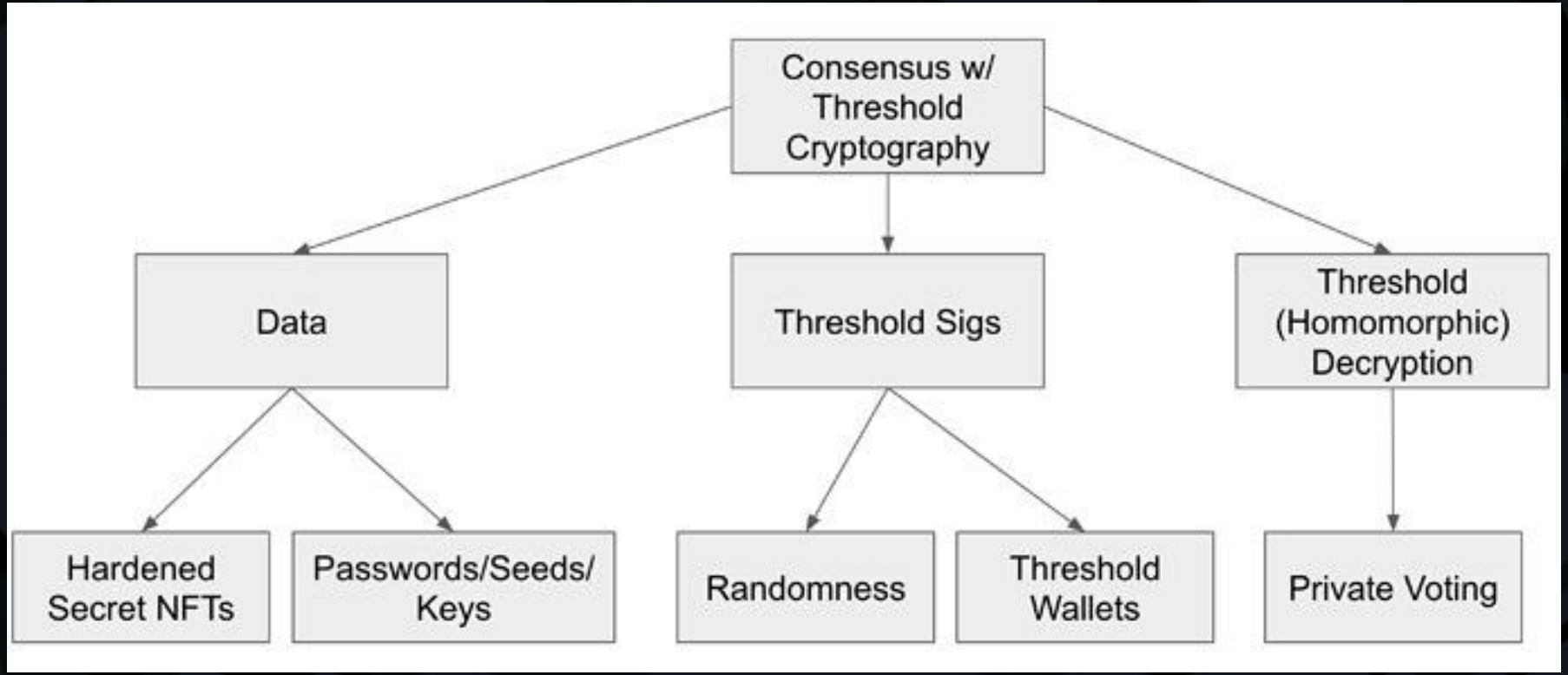
Encrypt all data pass it to a trusted section on a device, decrypt and compute

Fast but trusts the hardware

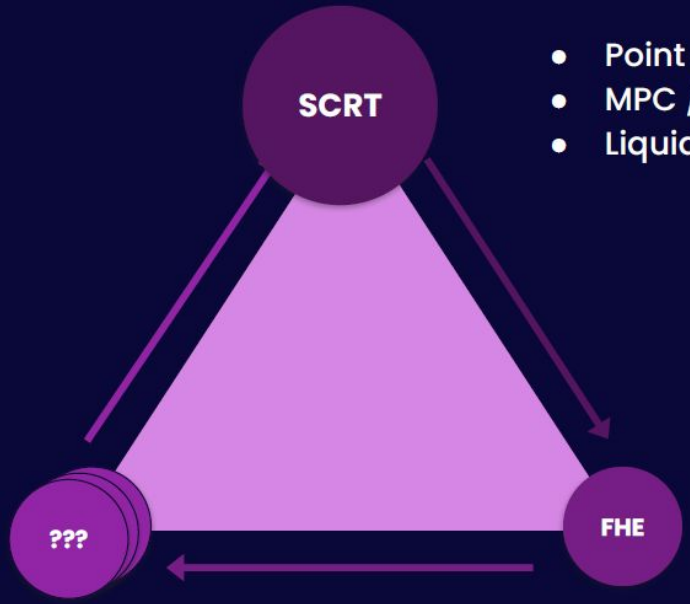
Zero-Knowledge proofs

Do computation yourself and prove you do it correctly

Fast and secure but hard to combine data


Consensus w/ Threshold Cryptography
Data
Threshold Sigs
Threshold (Homomorphic) Decryption
Hardened Secret NFTs
Passwords/Seeds/ Keys
Randomness
Threshold Wallets
Private Voting

Towards a **Constellation** of Chains



- Point of Origin
- MPC / Threshold Cryptography
- Liquidity hub for Privacy projects

- UberSCRT
- Testbed chain for public-private apps (AKA Open)
- Partner chains!

- Advancing the frontiers of Private Compute
- Interconnected with **$SCRT** (WIP)
  - ICS-like model to allocate to $SCRT Stakers
  - Liquidity sharing
  - Cross-development

Tooling and learning

Rust

Secret Tokens

Find out how Secret Tokens let you make any token privacy-preserving.

Secret Contract Development Toolkit

- Ankr
- DDT Secret-rng
- Fadroma
- Griptape.js
- Polar Arufa Research
- Secret IDE
- Secret Javascript
- Secret .Net
- Secret Python
- Secret University

What to build - Defi 2.0

(LSD) arbitrage vaults

Margin trading via Money markets

Limit orders that Execute on pools

One-click UX (for ex: Delta neutral interest arbitrage)

Flashloans

On-chain Options - Price betting

Stablecoin/Defi insurance

Mixed LP token aggregate strategies

LSD arbitrage - Vaults

1. Commit sSCRT, stkd-SCRT, SeSCRT, bSCRt, stSCRT etc. into Vault (imbalanced - Fee is lower if contributing the required assets)
2. Disperse Vault LP tokens - represents aggregate of staking derivatives
3. Vault executes arbitrage trades between staking derivatives cross-dex
4. Arbitrage revenue is compounded by retaining the LSD SCRT revenue
5. Vault LP token can be used as collateral in DeFi (looping, borrowing, self repaying loans etc)
6. Contract owner or DAO can take a fee for own revenue
7. Contract can also arbitrage its own Vault LP token as revenue source

Margin Trading

1. Create a contract that can collect Margin positions to be taken
2. Contract finds pools to use on available money market for respective pair
3. Contract loans


secret
Get Hacking
April 17th Monday
14:00 UTC
https://github.com/HackSecret/Spring-2023

Want to see more demos?

- contract: https://github.com/scrtlabs/rps
- UI: https://github.com/scrtlabs/rps-ui
- RPS deployed on testnet: https://rps.scrtlabs.com/