

# 隐私赛道扫盲

@andyw514



# 本次讨论希望围绕的主要问题

- 隐私是否是区块链的刚需？（近期vs. 远期）
- 哪类隐私技术符合应用/监管/用户的需求？
- 隐私赛道应该如何投资？

# 什么是隐私？

隐私有两个组成部分：

- 匿名性 (anonymity)
- 保密性 (confidentiality)

隐私放到区块链的范畴里，还需要解决“正确性 (correctness)”和“去中心化 (decentralization)”两个维度的问题

# 为什么区块链需要隐私？


- **基本人权**（大家都知道重要，但是没人愿意买单）
- **链接现实的合规需要**
- **金融/游戏博弈**
- **用户体验**
- **你懂的**

# 隐私能解决什么具体问题？

	透明公链的问题 (non-exhaustive)
合规	各国的隐私保护法 (e.g. GDPR, HIPA, Bank Secrecy Act) 要求大部分链接现实的应用需要实现用户数据保护
New 抗审查	公链的验证节点无法审查交易，因为交易节点本身无法获取mempool的信息
博弈	金融机构的杠杆爆仓点被全网追杀 (e.g. Celsius, 3AC)
	机构的Alpha交易策略被散户/机器人拷贝
	AMM交易被机器人或矿工MEV
	策略游戏 / 盲盒只能依靠线下计算，无法保证透明公正
用户体验	个人资产和交易链上透明，特别是如果和DID挂钩
	NFT功能单一且可以“右键保存”
	成为诈骗犯目标

# 比较不同的隐私解决方案

未来主要技术路线

	匿名币	混币协议	中心化/线下	ZK 公链	TEE 公链
项目例子	 		 	 	
匿名性	Y	Y	N	Y	Y
保密性	Y	N	Y (但会被中心化实体知道)	Y (支付) N (DeFi)	Y (需要trust Intel SGX芯片)
	仅限支付	仅限支付	CEX仅限交易	公链/有限隐私	公链/通用隐私



# Privacy Comparisons

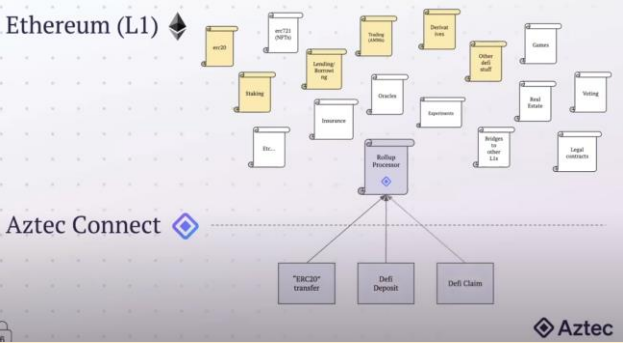
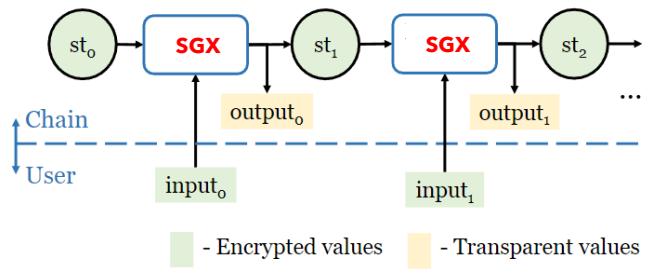


	ASSUMPTIONS	COMPUTATIONAL COST	NETWORK COST	DEVELOPMENT DIFFICULTY
Partial HE/FHE	Inapplicable	⚠️ High	Low-Medium	⚠️ High*
Threshold FHE	No collusion	⚠️ High	Low-Medium	Medium
MPC	No Collusion	Low-Medium	⚠️ High	Medium
TEEs	Secure Hardware	✅ Low	✅ Low	✅ Low
ZKPs	At Least One Party Sees All Data	Medium-High	✅ Low	⚠️ High**

\* Many applications can't be developed using these. It also requires better cryptographic understanding of the underlying primitives


\*\* Prover-verifier model requires developers to change how they think and build programs


# ZK和TEE比较

	隐私实现方式	可实现应用	优劣比较
ZK公链	 <p>用线下的复杂数学证明来验证线上的交易</p>	<b>有限的隐私功能</b> <ul style="list-style-type: none"><li>• 隐私支付</li><li>• 有限隐私的DeFi（用户batch后提交给L1应用执行）</li></ul>	<ul style="list-style-type: none"><li>+ ZK技术作为scaling solution吸引了大量的优秀开发者</li><li>+ 雄厚的VC资金支持</li><li>+ ZK技术还在早期，后面可能会有新突破</li><li>- 隐私功能比较有限，应用间无法共享state（例如AMM）</li><li>- zkEVM虽然取得进展，但是未涉及隐私，隐私应用开发周期任然很长</li></ul>
TEE公链	 <p>通过Intel的加密执行芯片（SGX）对input进行trustless保密，同时执行运算</p>	<b>可以实现所有透明公链能做到的功能</b> <ul style="list-style-type: none"><li>• 支付</li><li>• DeFi</li><li>• GameFi</li><li>• NFT（可编程）</li></ul>	<ul style="list-style-type: none"><li>+ 应用功能极具灵活性，任何ETH/Cosmos的应用均可以做隐私版本</li><li>+ 生态成熟度/多样性领先ZK</li><li>+ 通过IBC和Axelar可以实现公链间交互式隐私</li><li>- 严重依赖Intel SGX芯片</li><li>- TEE比较吃硬件，scalability还待验证</li></ul>



# ZK L2隐私举例 (Aztec) – 部分主网

 **ElementFi**

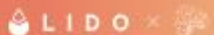
Fixed Yield 


Deposit zkDai to Element for fixed yield. Funds are locked in Element and returned at the maturity date.

APR	MATURITY	NEXT BATCH
1.74%	Sep 16, 22	~a day

USERS IN BATCH 6/40

Earn

 **LIDO x**

Staking 


Swap ETH for stETH on Curve and earn daily staking rewards. stETH is wrapped into wstETH.


APR	L1 LIQUIDITY	NEXT BATCH
4.37%	\$8.4B	~14 hours


USERS IN BATCH 35/50

Earn

More protocols coming soon!

 **AAVE**

 **Compound**

 **Liquidity**

# ZK L2隐私举例 (Dusk) – 还未主网



## Zero Knowledge Utility Token

Zero-Knowledge Utility Tokens address the industry's privacy concerns with public blockchain technology. ZK-tokens leverage zero-knowledge proof systems (ZKP) to enable anonymous user identification, a key ingredient for the Digital Identity / Self-Sovereign Identity (SSI) use case.

[QUICK VIEW](#)



## Security Token Exchange

Security token exchanges are stock exchanges that support the trading, deposit and withdrawals of security tokens, and use the blockchain in order to increase industry cooperation and bring down the cost of issuance, fundraising, and listing

[QUICK VIEW](#)



## Digital Share Registry

Digital share registries use blockchain technology in order to enhance their data, enabling automation and reconciliation by businesses and shareholders that rely on it.

[QUICK VIEW](#)



## Smart Bulletin Board

Smart Bulletin Boards can be used to indirectly match qualified buyers and sellers of security tokens. If both parties come to terms and a deal is struck, they can execute the trade *trustlessly* using the XSC-based security token contract and settle the transaction instantly on the Dusk Network blockchain.

[QUICK VIEW](#)



## Confidential Security Tokens

We've designed the 'XSC' Confidential Security Contract standard, for the creation and issuance of privacy-enabled Security Tokens. It supports permission management, and the tools needed to carry out corporate actions during the asset lifetime.

[QUICK VIEW](#)



## Proxy Voting

With the implementation of Shareholder Rights Directive II (SRD2), there is an increasing regulatory demand to encourage long term shareholder commitment. Tokenization provides a possible solution by enabling a consolidated overview of all asset holders.

[QUICK VIEW](#)



## Self-Custody

The 'XSC' Security Token Contract that governs security tokens in the Dusk Network, is designed in such a way to maximize security, and minimize risks of fraud and theft. Shareholders can choose to *self-custody* and rely on a myriad of measures

[QUICK VIEW](#)




## Decentralized Finance (DeFi)

Financial applications (such as lending, borrowing, voting and stablecoins) can be programmed as confidential smart contracts that run on the Dusk Network blockchain.

[QUICK VIEW](#)


# TEE隐私举例 (Secret Network)

## DEFI

Defi


### Shade Protocol

An array of connected privacy-preserving DeFi applications built on Secret Network.

Defi Amm

### SiennaSwap


Privacy-first & cross-chain defi platform. Privately swap, lend and convert your tokens into their private equivalent.

Defi

### Polymer


A balancer-like AMM that provides many features, competitive rates, and a zero-inflation stakeholder growth model.

## NFT / Game / Social

Communications


### Alter

A private and secure messaging app that protects your data and identity when communicating online.

NFTs


### Stashh

Mint, buy, and trade the first NFTs with native privacy and access control, known as Secret NFTs.

NFTs Games

### Legendao

A play-to-mint NFT platform that enables creators to launch their NFT projects in a unique, gamified way.

Games

### Bushi

A competitive third-person shooter that blurs the lines between traditional games, web3 gaming, and esports.

## Access Control & Enterprise Solutions

Defi

### Serenity Shield

Serenity Shield provides a tool for backing up your seed phrase and other sensitive data, allowing recovery in an emergency event.



### JACKAL

A fully decentralized yet easy-to-use cloud storage solution.

Defi Social

### Data Vault

The world's first decentralized privacy-preserving content management and data exchange protocol.

NFTs Social

### SecretDAO

SecretDAO is a DAO creation tooling platform that aims to make DAO creation simple, easy, and accessible.

NFTs

### CertUP

Revolutionising official document distribution, verification and publication through Secret NFTs.

# 隐私赛道投资策略和关注点

## Guiding principle:

- 这是个还未跨过鸿沟的赛道，风险/收益比相当高，*不建议大仓位*
- 隐私起来的前提是web3走出DeFi，只有和现实应用链接起来隐私才有意义
- ZK和TEE两大分支，类似于过去VHS和Betamax制式之争，技术和adoption需要齐头并进（目前还未知胜负）

重点关注项目：Secret Network (TEE), Obscuro (TEE), Aztec (ZK), Manta Network (ZK), Dusk Network (ZK)