

Jan 9

zkTLS

اصالت سنجی داده های web2 در web3 به کمک zkTLS

معرفی و صحبت درباره نیازهایی که از اکوسیستم ایران میتونه حل کنه

TORINO™

پول نو

Jibit

صراف

Exfinio

EFEX

مهر

کیف پول من

Mazdax
Trade Globally

excoino

NIPOTO

NOBITEX

OMPfinex

BtPh

Jan 9



TORINO™

پول نو

Jibit

صراف

Exfinio

EFEX

کیف پول من

Mazdax

excoino

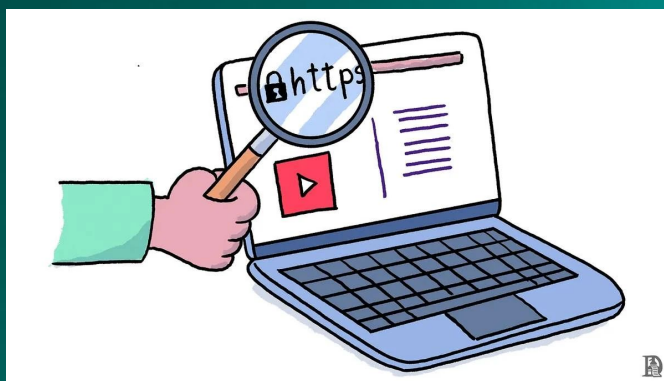
NIPOTO

NOBITEX

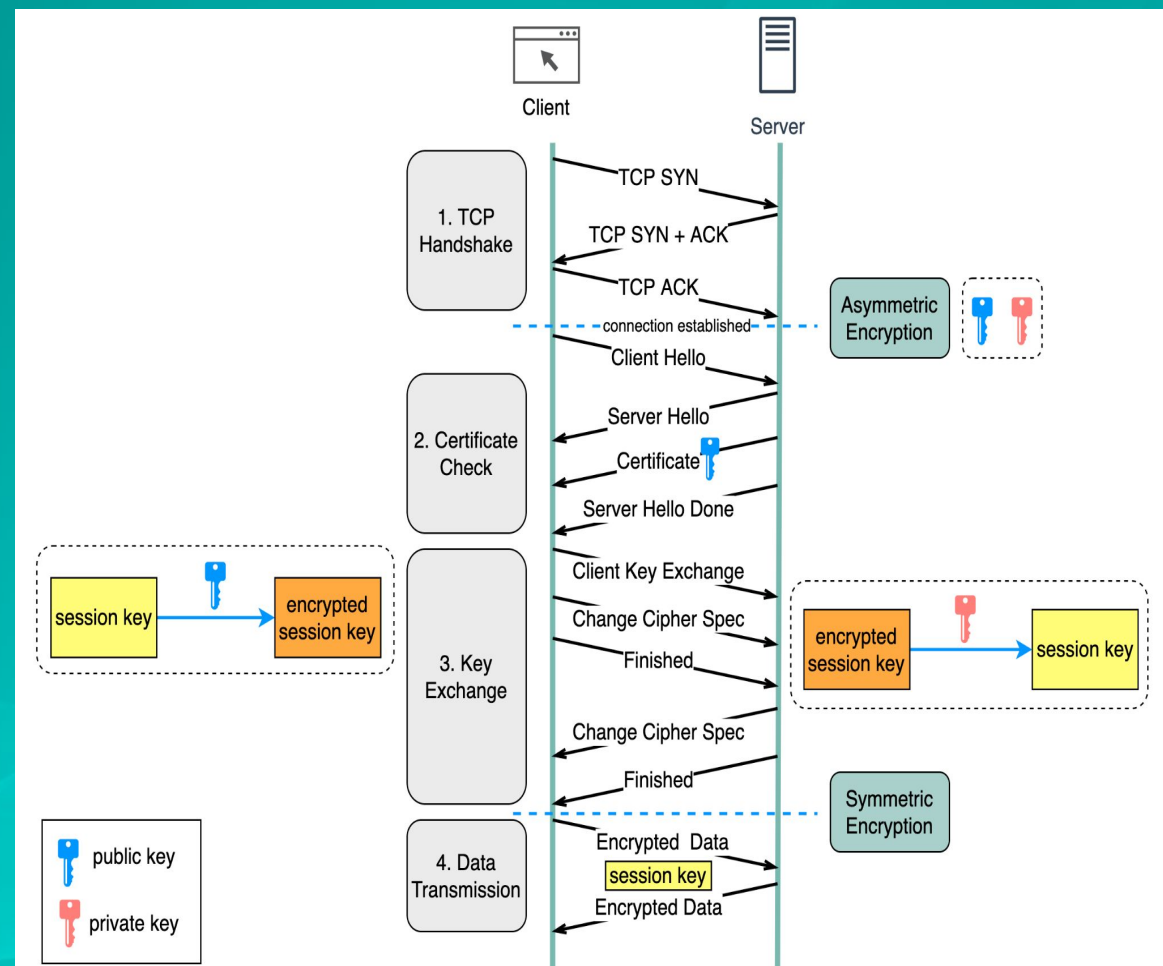
OMPfinex

BtPh

Jan 9

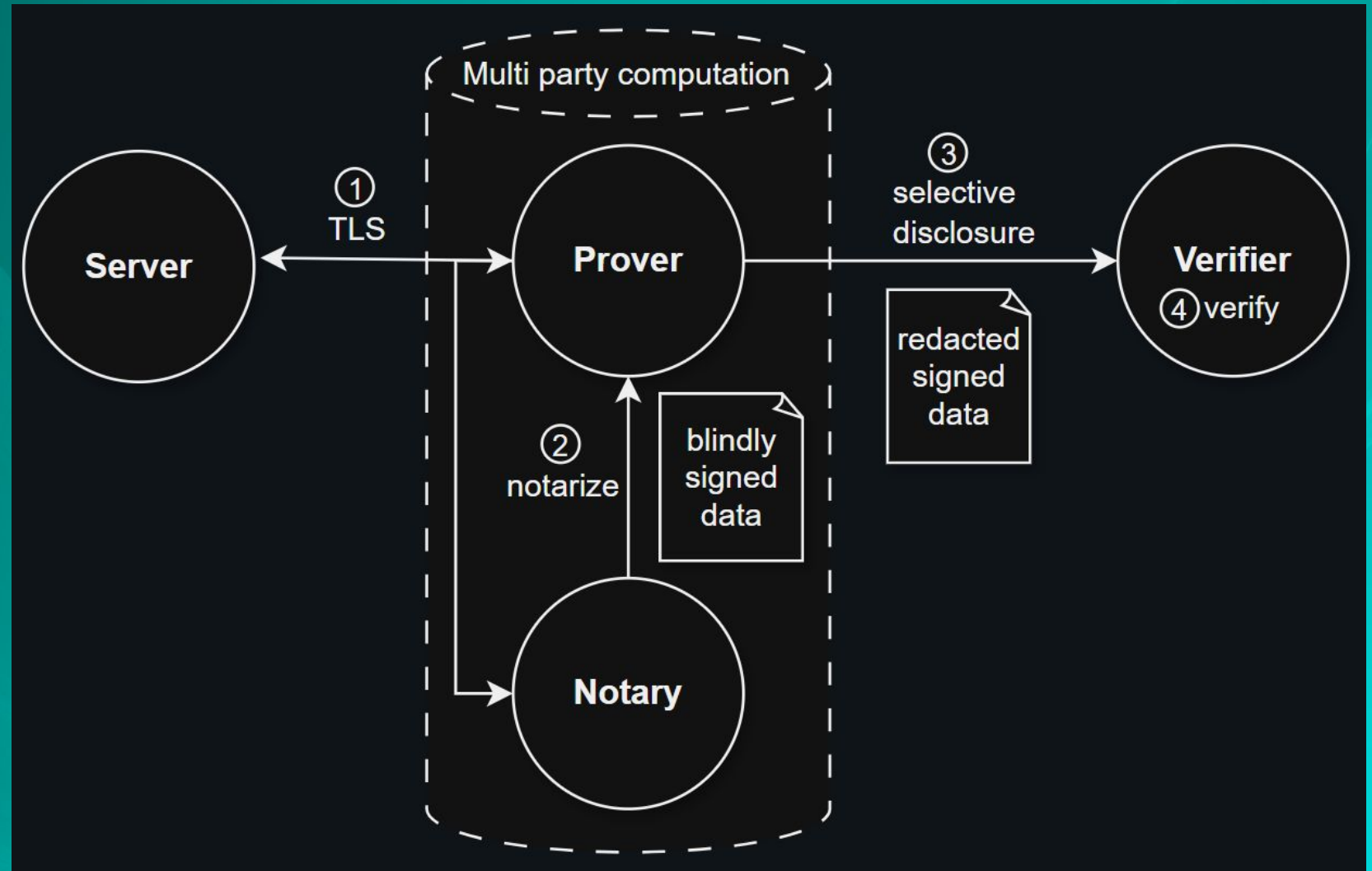


چرا TLS به تنهایی کافی نیست؟



Jan 9

1. MPC
2. TLS Handshaking
3. Communication
4. Selective Disclosure (Merkle Tree)
5. Attestation (Signed Message by Notary)



Jan 9

TLS guarantees:

- ✓ data origin
- ✓ data integrity

but not:

- ✗ data portability
- ✗ data verifiability

zkTLS guarantees:

- ✓ data origin
- ✓ data integrity
- ✓ data portability
- ✓ data verifiability

MPC-TLS do **NOT**
result in zk-proof (SNARK, STARK, ...)

but

- signed attestation

پس چجوری توی قرارداد
هوشمند ها میتونیم استفاده
کنیم ازش؟

ZKP, TEE, etc

Jan 9

کاربرد ها

- Identity Verification: verify your name, age, or citizenship from online government services
- Reputation Verification: verify user experience or trustworthiness on platforms like Snapp, Digikala, Tapsi
- Account Ownership Verification: confirm control over online accounts (e.g. Google, Nobitex, Twitter, etc)
- Financial Verification: verify your financial standing or prove financial dealings from your bank or other service
- User Restriction Verification: confirm if a user is barred from accessing specific applications or services

TORINO™

پول نو

Jibit

صراف

Exfinilo

EFEX

کریپتو پول نو

کیف پول من

Mazdax
Trade Globally

excoino

NIPOTO

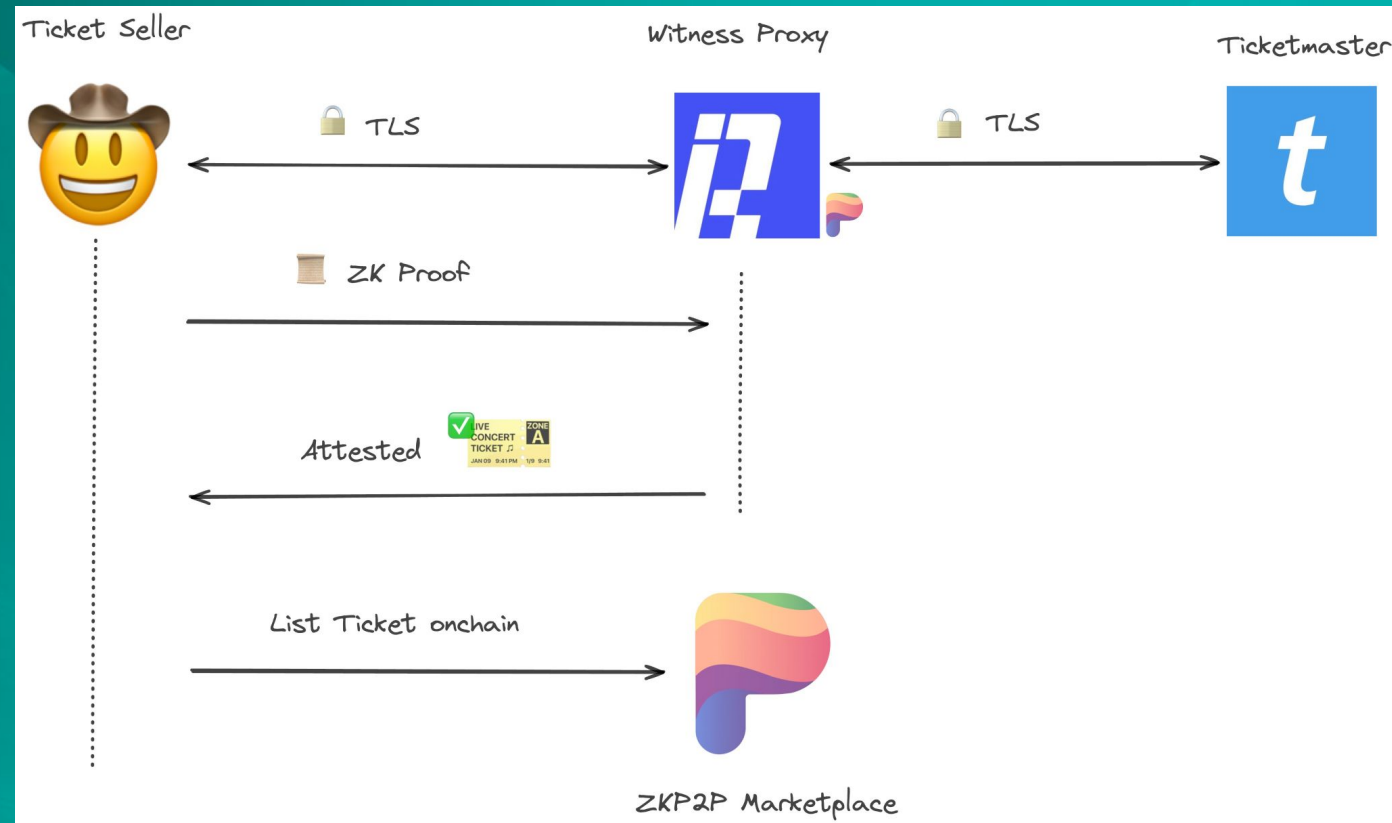
NOBITEX

OMPfinex

BtPh

Jan 9

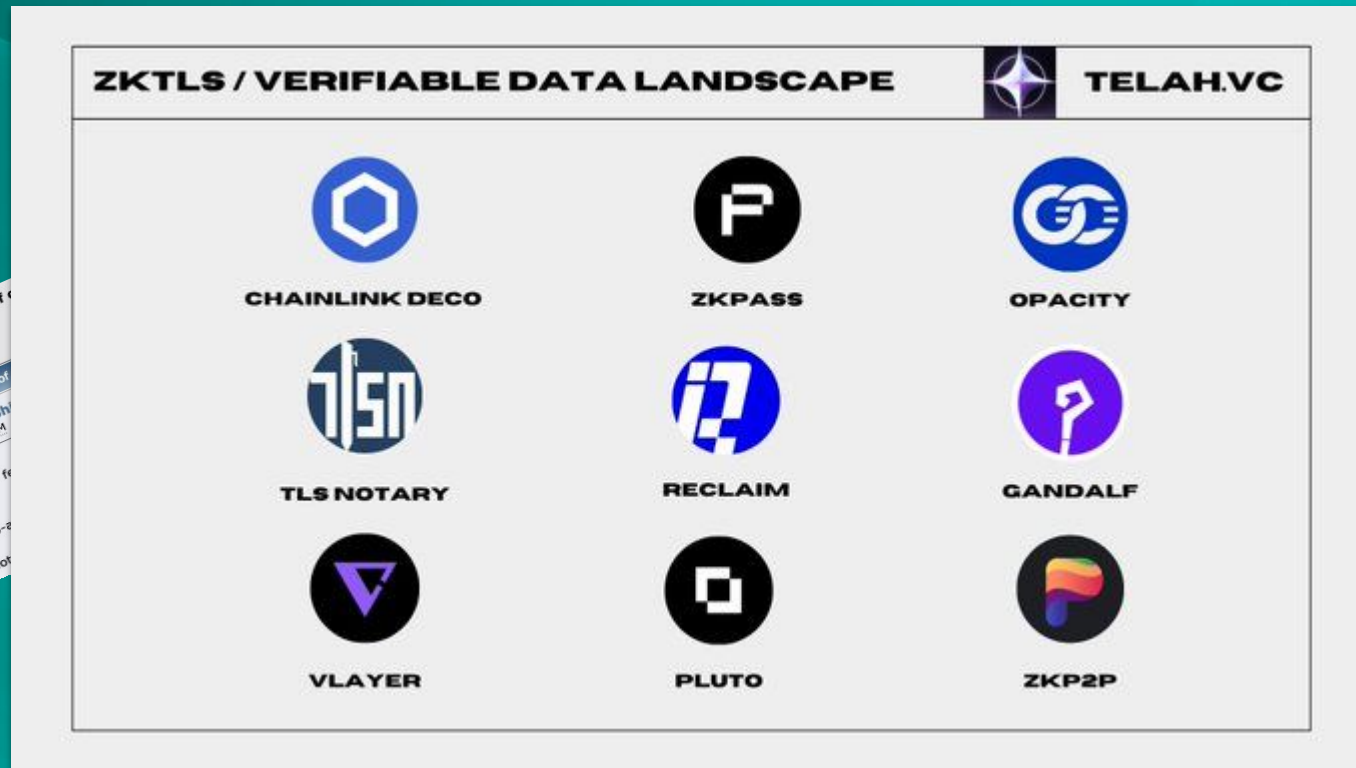
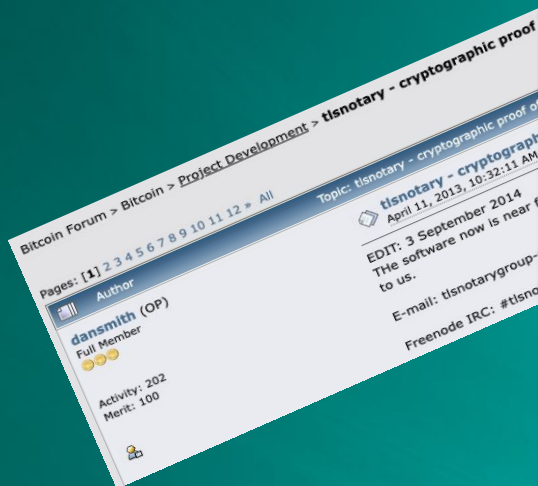
Vampire attacking Web2 Marketplaces with zkTLS



- Trustless version of LocalBitcoins on web3
- Private Communities
- etc

Jan 9

برخی از پروژه ها و ابزار ها



Jan 9

نیازهایی که از اکوسیستم ایران میتونه حل کنه

Naser Hakimi @NaucerHakimi

اعتبارسنجی در ایران باید به سمت ایجاد زنجیره‌های اطمینان حرکت کند. به این معنی که اعتبار شخصی همانند پول سیال و قابل انتقال شود.

Translate post

3:27 PM · Nov 28, 2024 · 2,471 Views

8 1 46

Post your reply Reply

Hamid @n3wbateni · Nov 28, 2024

روی این میشه به ایده استارت‌آپی ساخت

مسئله اعتبارسنجی رو با ترکیب `tlsnotary` میتونیم این شکلی شکل بدیم

که فرد ثابت می‌کنه توی صرافی‌های مختلف یک مقدار کریپتو با ارزش ریالی فلان داره یا مجموع خریدهای ماهانه‌اش از دیجی کالا فلان مقدار ثابت بوده

۱/۲



اعتبارسنجی و صحت‌سنجی داده‌ها بدون نیاز به جمع‌آوری دیتا

Jan 9

github.com/irnb



Hamid Bateni

irnb

Edit profile

104 followers · 39 following

@txfusion @vianetwork

https://bateni.xyz

Achievements



Highlights

PRO

Organizations



irnb / README.md

Hi there 🙌

This is Hamid

- Software Engineer, Blockchain Researcher, EIP-7503 Author
- Areas of Interest:** Ethereum Core Development, Censorship Resistance, Privacy, Layer 2, ZKP, DeFi
- Contact:** hamid@europe.com, [Telegram](#)
- Website:** bateni.xyz shiryakhat.net

Current Occupation

- Bitcoin Layer 2:**
 - Serving as a Protocol Architect and Rust Engineer in **txFusion**, working on creating a Layer 2 solution on Bitcoin based on zkSync-Era.

Previous Experience

- Ethereum Protocol Fellowship:**
 - Working on the implementation of [Inclusion List with Plausible Deniability](#) on Reth and Lighthouse as fellow in [Ethereum Protocol Fellowship](#) program.
 - Direct integration (non-http) of Lighthouse-Reth ([Link](#)).
- Enterprise Wallet Systems**
 - Worked as Software Engineer & Blockchain Integration Engineer for 3 years in a high-scale crypto exchanges environment, focusing on on-chain privacy, key security, MPC, HSM, and utilizing smartcontracts for optimizing the management of large-scale asset operations on EVM-based chains.
 - Led the integration of various new blockchains and tokens into the system.
- Applied ZKP Projects**
 - EIP-7503** ❤️: Contributed to the EIP-7503, which can be reviewed [here](#).
 - Private Proof of Solvency** 🧑‍🔬: Design Private Proof of Solvency protocol, with the research paper available [here](#).
- OrderBook Based DEX**
 - Contributed to the development of an on-chain order book for decentralized exchanges, with details available in the [whitepaper](#).

TORINO™

پول نو

Jibit

صراف

Exfinilo

EFEX

میرا

کیف پول من

Mazdax
Trade Globally

excoino

NIPOTO

NOBITEX

OMPfinex

BitPh