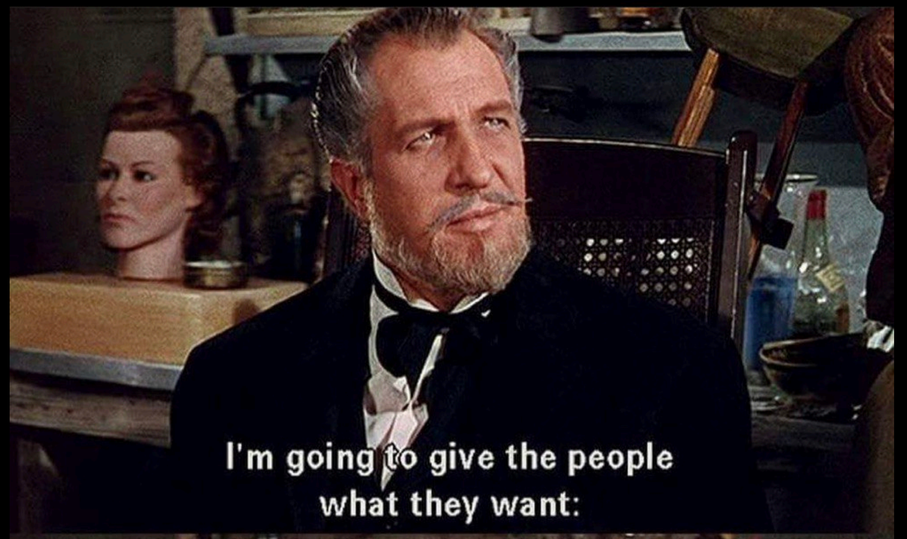
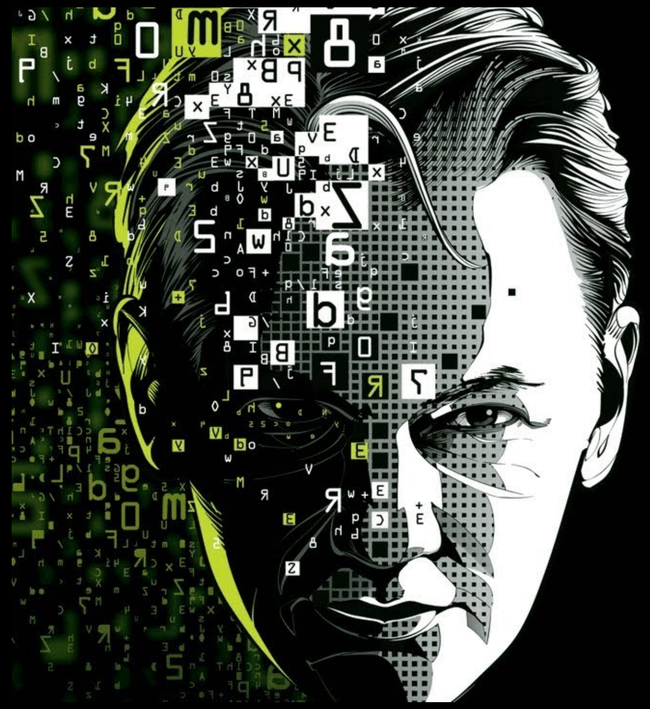
Shackled by blockchain
or
freed by client-side validation?

Olga Ukolova
LNP/BP Standards Association
Pandora Prime Inc

Disclaimer!


I'm going to give the people
what they want:


sensation, horror, shock.



The Cypherpunk Manifesto

9 March 1993

How it started

BITCOIN

A Peer-to-Peer Electronic Cash System

ABSTRACT: A purely peer-to-peer version of electronic cash would allow online payments to be sent directl
from one party to another without going through a financial institution. Digital signatures provide part of th
solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending

We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoi
chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of th
sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are n
cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadca
on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gon

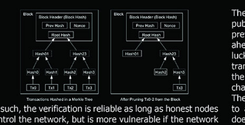
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non- reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party. What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the

majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added. To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:
1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment,

The receiver generates a new key pair and gives t
public key to the sender shortly before signing. T
prevents the sender from preparing a chain of bloc
ahead of time by working on it continuously until he
lucky enough to get far enough ahead, then executing t
transaction at that moment. Once the transaction is se
the dishonest sender starts working in secret on a para
chain containing an alternate version of his transactio
The recipient waits until the transaction has been add
to a block and z blocks have been linked after it.
doesn't know the exact amount of progress the attack
has made, but assuming the honest blocks took t
average expected time per block, the attacker's potent
progress will be a Poisson distribution with expected valu

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could s
catch up now, we multiply the Poisson density
each amount of progress he could have made
the probability he could catch up from that poi

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

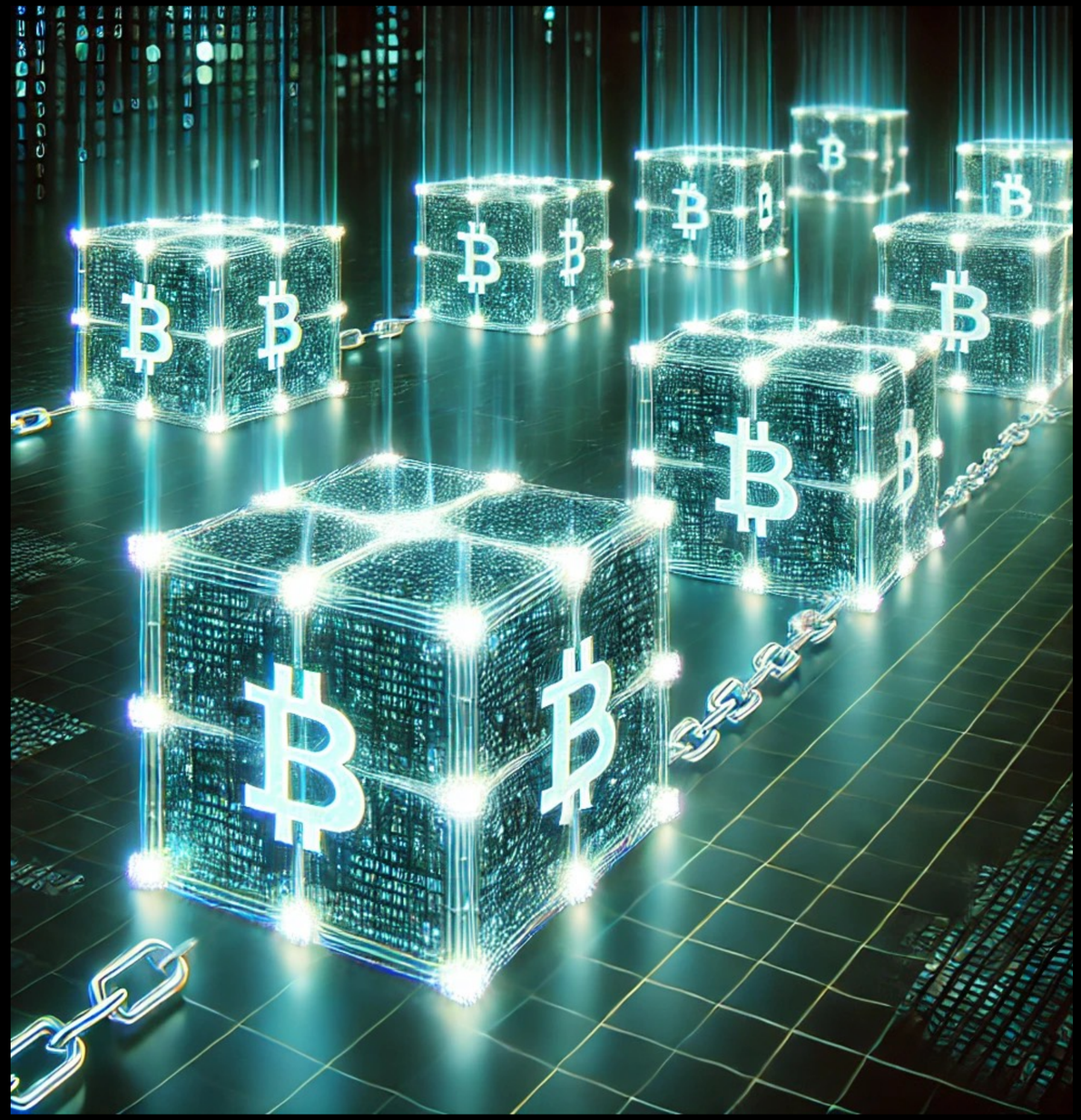
Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} (1 - (q/p)^{(z-k)})$$

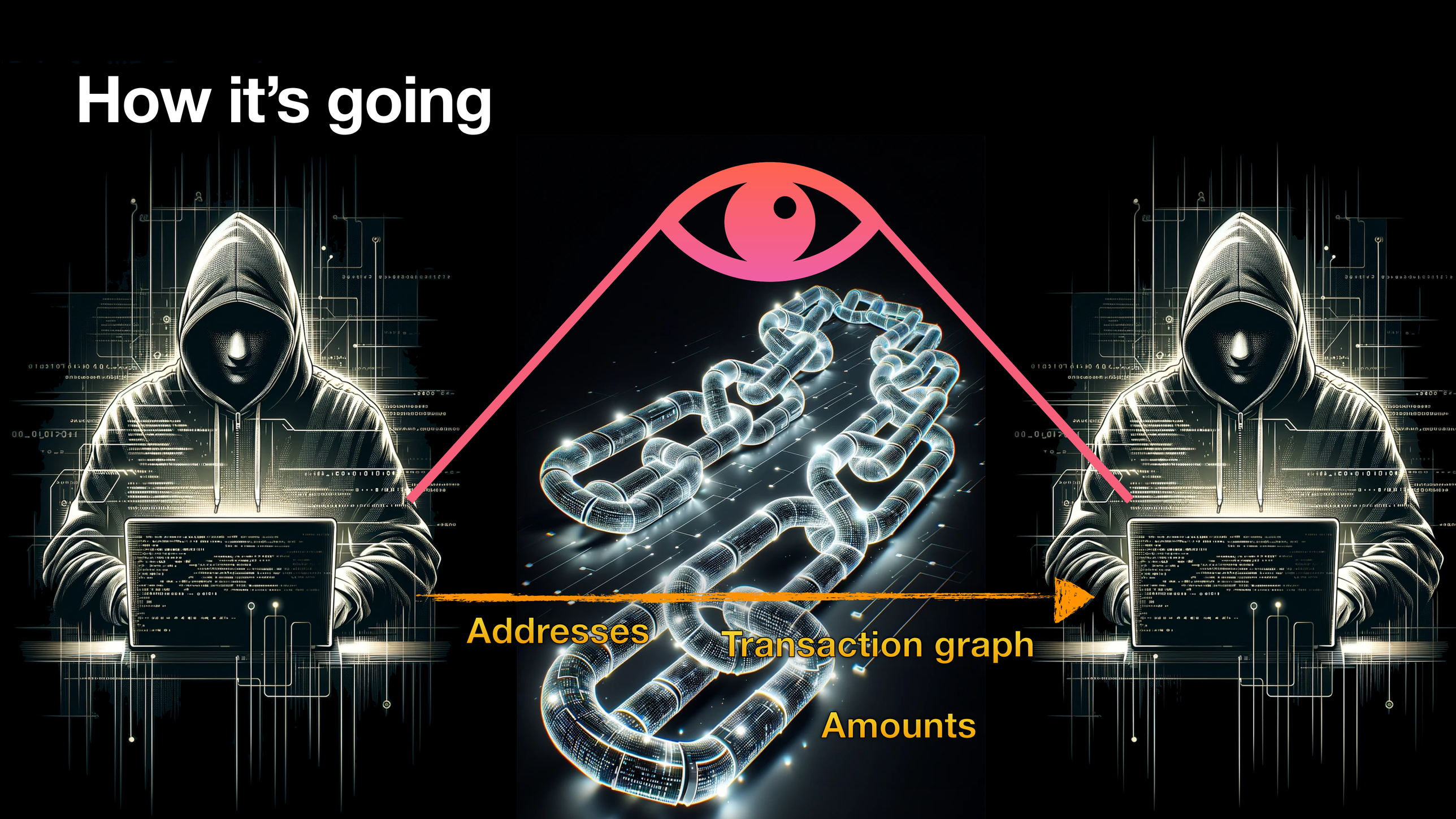
Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
```

- Blockchain
- Openness and transparency
- Freedom money
- Empowering individual
- Self-custody
- Speed of transactions
- No central authority



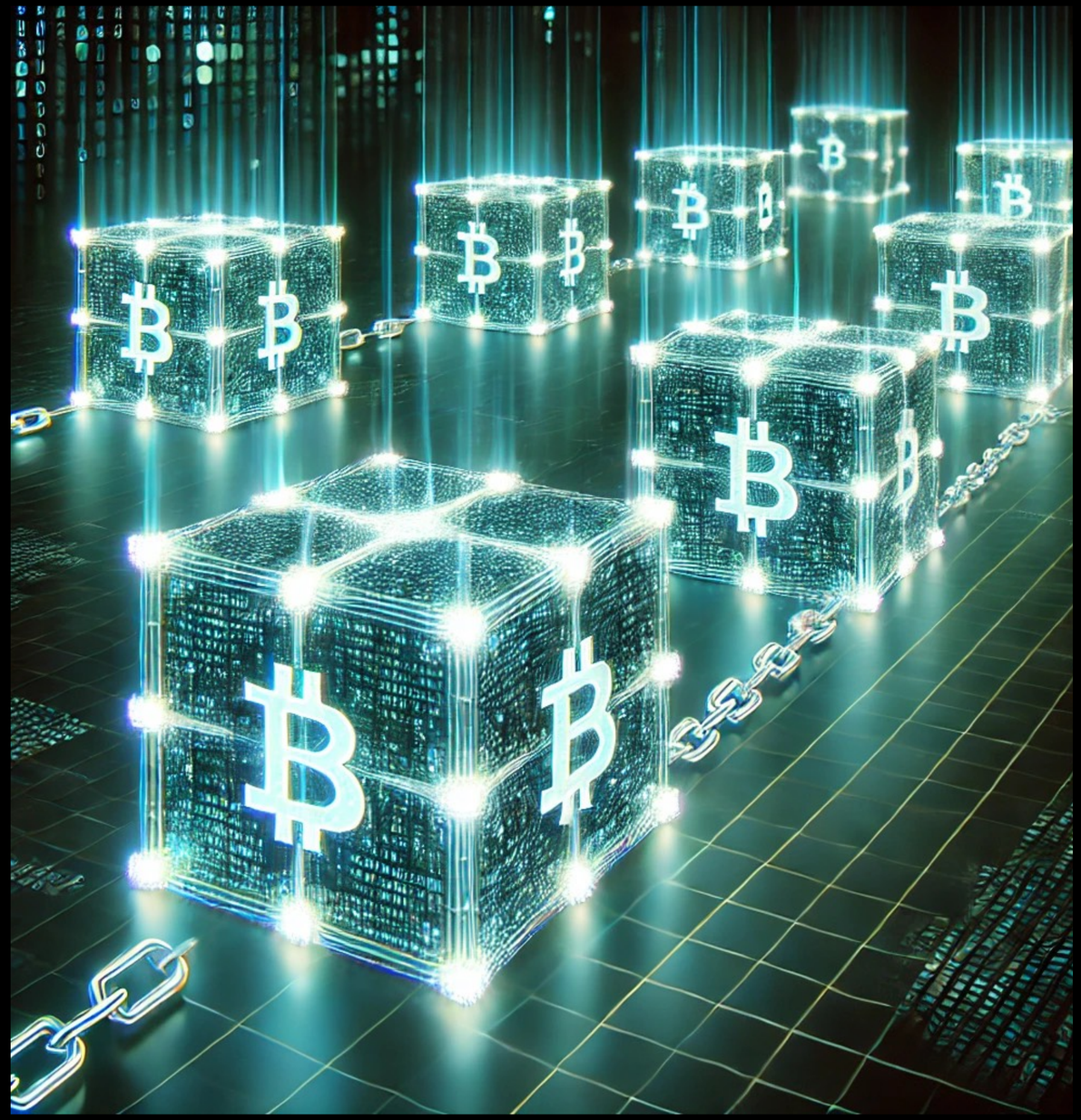
How it’s going



~~PRIVACY~~

~~PROGRAMMABILITY~~

~~SCALABILITY~~



PRIVACY

Attempts to fix this:

- Sidechans - Liquid
- Mixers/Coinjoins
- Monero/Privacy coins
- Ark/Covenants/Soft forks

Attempts to fix this:

- Sidechans - Liquid
- Mixers/Coinjoins
- Monero/Privacy coins
- Ark/Covenants/Soft forks

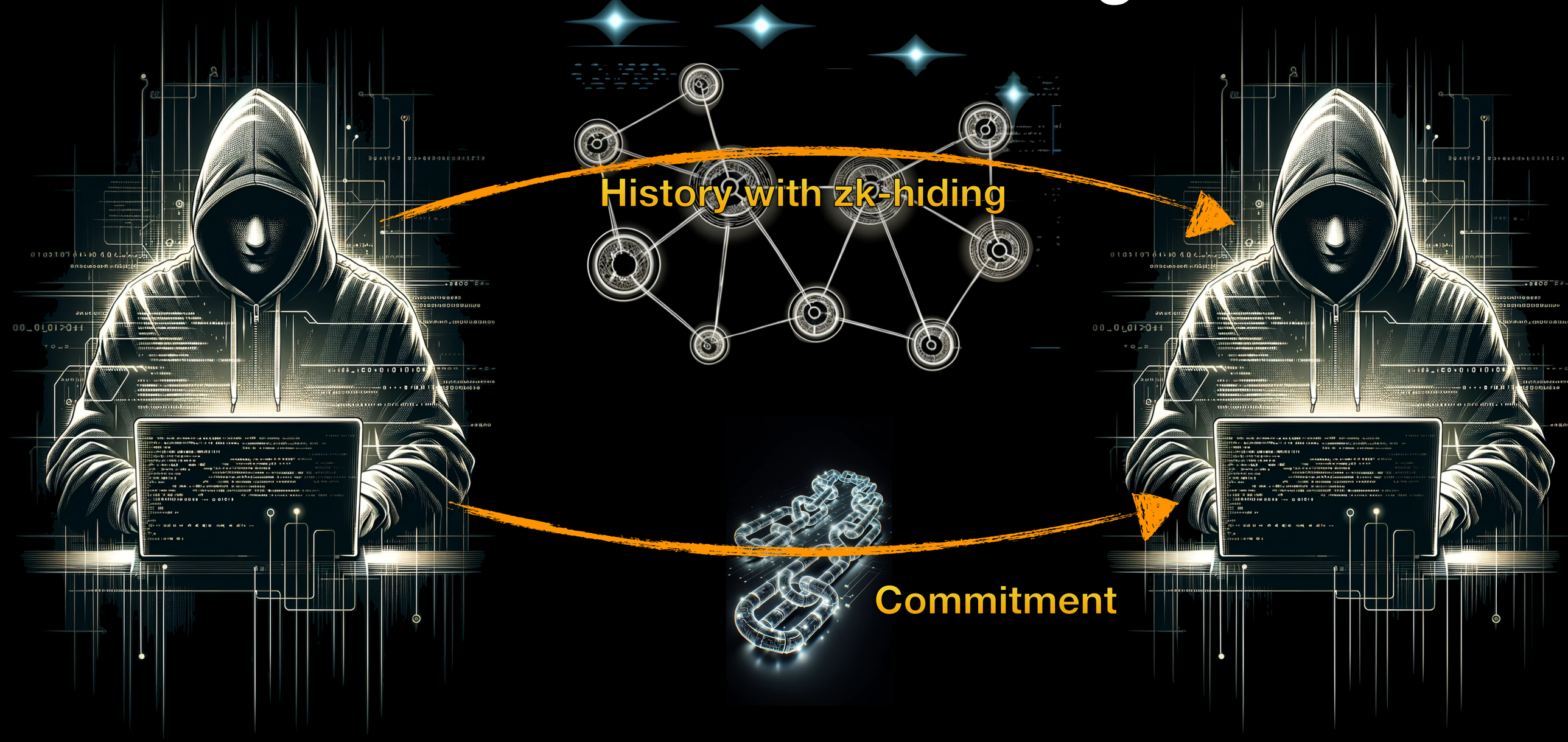
Does it help?

How things work today

Is there a solution?

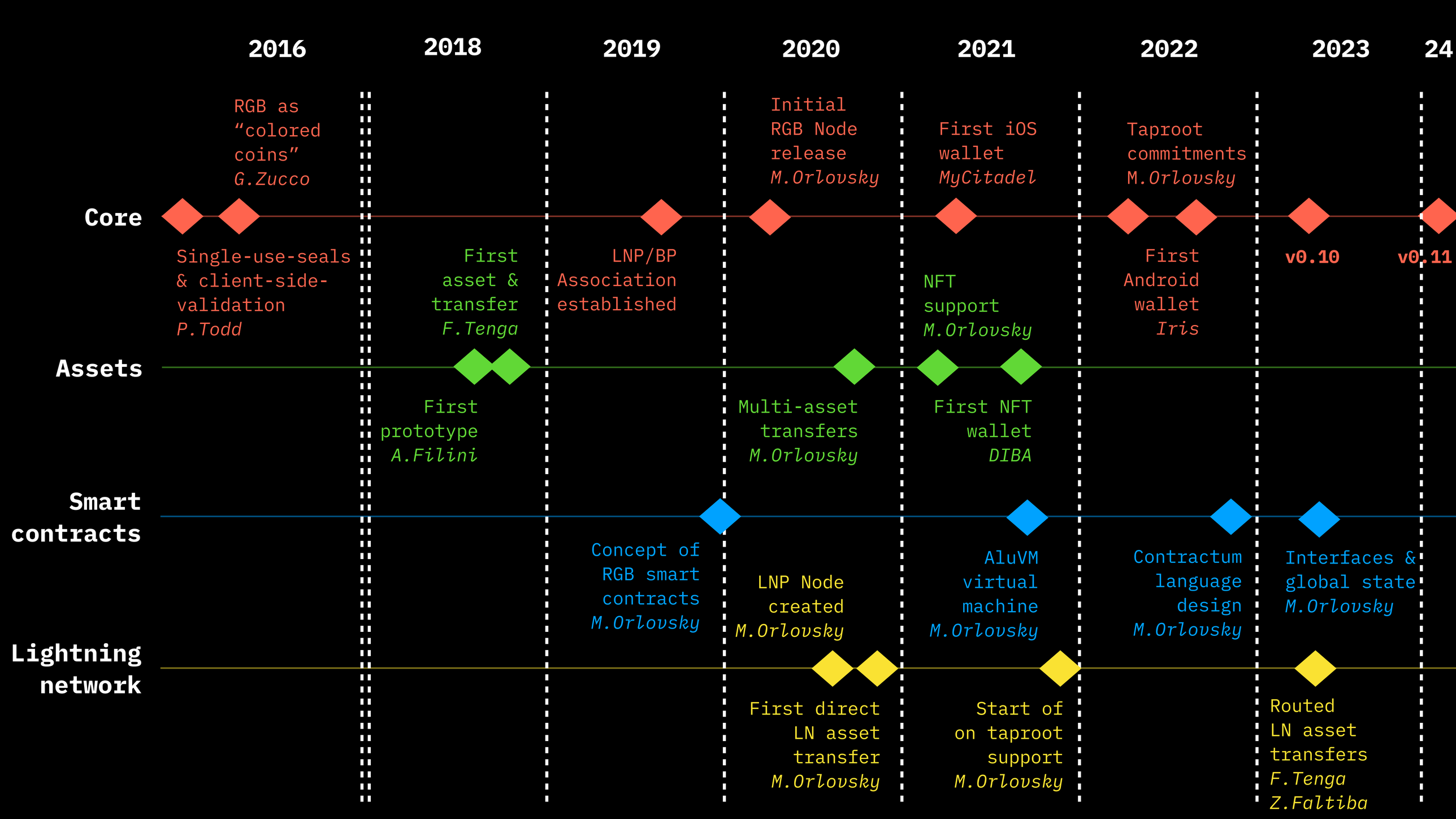
CLIENT-SIDE VALIDATION

What client-side validation changes



CLIENT-SIDE VALIDATION

- No blockchain pollution
- Privacy by design + zk-proofs
- Scalability and speed
- Verifiability without trust or central registry
- No forks


2016
2018
2019
2020
2021
2022
2023
24
Core
Assets
Smart contracts
Lightning network
RGB as “colored coins” G.Zucco
Single-use-seals & client-side-validation P.Todd
First asset & transfer F.Tenga
First prototype A.Filini
LNP/BP Association established
Initial RGB Node release M.Orlovsky
Multi-asset transfers M.Orlovsky
Concept of RGB smart contracts M.Orlovsky
LNP Node created M.Orlovsky
First direct LN asset transfer M.Orlovsky
First iOS wallet MyCitadel
NFT support M.Orlovsky
First NFT wallet DIBA
AluVM virtual machine M.Orlovsky
Start of on taproot support M.Orlovsky
Taproot commitments M.Orlovsky
First Android wallet Iris
Contractum language design M.Orlovsky
v0.10
Interfaces & global state M.Orlovsky
Routed LN asset transfers F.Tenga Z.Faltiba
v0.11

CLIENT-SIDE VALIDATION

- **RGB** Smart Contracts
- **Prime**: new non-blockchain solution for client-side validation
- **Radiant**: trustless Bitcoin bridge based on cryptoeconomic security
- **Storm**: Data availability network
- **Prometheus**: Computing and machine learning network

RGB:

post-blockchain smart contracts
for Bitcoin and Lightning Network

Storm:

Decentralized storage, messaging & search

Prometheus:

Decentralized computations

Radiant

Trustless pegout using payment channels

Prime: new layer 1 for Bitcoin made with RGB & client-side validation

[bitcoin-dev] Scaling and anonymizing Bitcoin at layer 1 with client-side validation

Dr Maxim Orlovsky orlovsky at lnp-bp.org
Thu Jun 1 17:21:39 UTC 2023

- Previous message: [bitcoin-dev] Full-RBF Peering Bitcoin Core v25.0 Released
- Next message: [bitcoin-dev] Scaling and anonymizing Bitcoin at layer 1 with client-side validation
- **Messages sorted by:** [date] [thread] [subject] [author]

Dear community,

Some time ago we (LNP/BP Standards Association) announced the release of RGB smart contract system [1]. In the subsequent discussion, we have referenced [2] that the introduction of client-side validation has the potential for upgrading Bitcoin layer 1 - blockchain, which has become an unnecessary limiting factor for the Bitcoin ecosystem, creating both scaling and privacy problems. While client-side validation requires consensus protocol and some layer 1 (for the proof of publication), this layer can be implemented in a more efficient way than the Bitcoin blockchain.

Today we are glad to present Prime: a proposal to upgrade Bitcoin protocol with the new scalable (up to billions of tx per minute) and fully anonymous (opaque) layer 1, moving most validation work into the client-side validation system. It leaves BTC (Bitcoin as money) and the rest of the Bitcoin ecosystem (including PoW) intact. It may be deployed without a softfork and miners upgrade, but can certainly benefit from it. It doesn't affect those users who are not willing to upgrade and doesn't require any consensus or majority for the initial deployment. It also makes Lightning Network and other layer 2 systems redundant. Finally, it will make things like BRC20, inscriptions, ordinals etc. impossible; all proper assets, NFTs etc. will be done with RGB smart contracts, not forcing non-users to store, validate and use their network bandwidth for the unpaid third-party interests.

The white paper describing the proposal can be found here:
https://github.com/LNP-BP/layer1/

As LNP/BP Standards Association we are setting a working group which will be focused on formal specification and reference implementation of this new layer - and will gladly accept everybody who wishes to cooperate on this topic. We also plan educational and workshop activities to make community understand the underlying technology better and take educated decision on its adoption.

We believe that this infrastructural effort must not be managed by a for-profit company - or a commercial group with its interests, and the only proper way of funding such an effort should be through non-profit donations. We do plan a fundraising campaign, so everyone interested in driving the Bitcoin evolution forward please contact us at ukolova [at] lnp-bp.org. For-profit organizations can also become members of the Association [3] and get to the committees defining the shape of the future Bitcoin technologies.

Dr Maxim Orlovsky
on behalf of LNP/BP Standards Association
https://lnp-bp.org/
GitHub: github.com/LNP-BP
Twitter: @lnp_bp
Nostr: npub13mhg7ksq9efna8ullmc5cufa53yuy06k73q4u7v425s8tgpdr5msk5mnym

[1]: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2023-April/021554.html
[2]: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2023-April/021577.html
[3]: https://www.lnp-bp.org/membership
-------------- next part --------------
An HTML attachment was scrubbed...
URL: <http://lists.linuxfoundation.org/pipermail/bitcoin-dev/attachments/20230601/3ede4035/attachment.html>

CLIENT-SIDE VALIDATION

- **RGB** Smart Contracts
- **Prime**: new non-blockchain solution for client-side validation
- **Radiant**: trustless Bitcoin bridge based on cryptoeconomic security
- **Storm**: Data availability network
- **Prometheus**: Computing and machine learning network

Bonus slide:


WEN MAINNET?

Olga Ukolova

Twitter @dr_ukolova

- Co-author of #FreeAI Manifesto
- Board member at LNP/BP Standards Association
- Founder @Pandora Prime