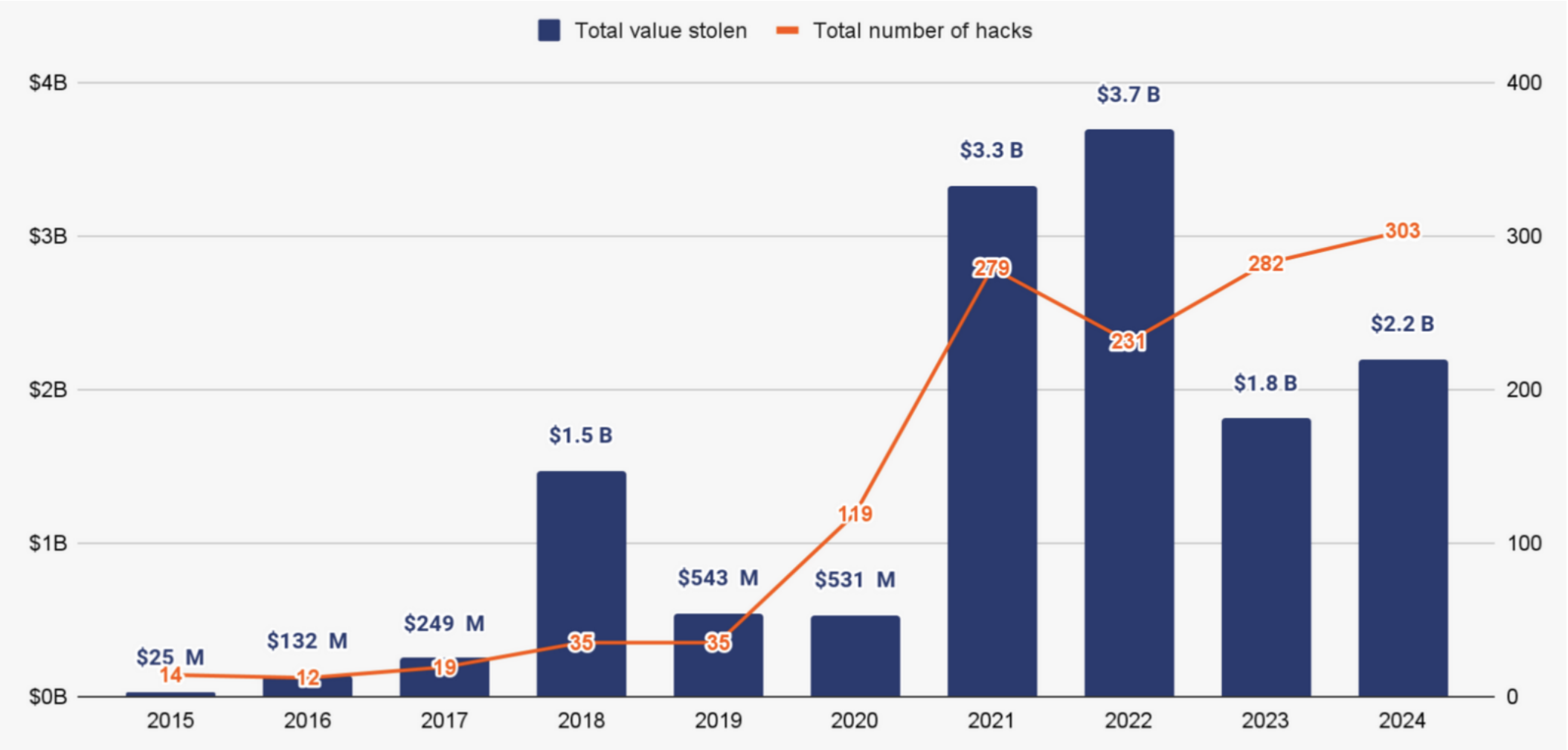
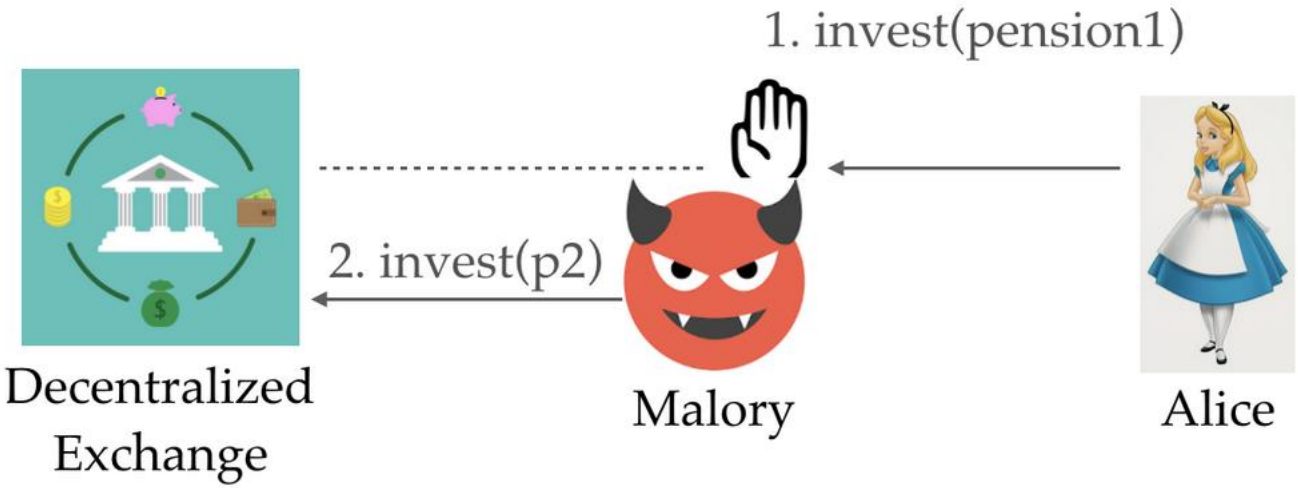
Full Privacy is Bad for You

Hacks on Blockchains



Source: https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/

Front Running Attacks



The overall losses caused by front-runners across major decentralized exchanges in 30 days, from April 24 to May 24, was $279M. It was $12M alone in the last 24 hours of this interval.

Money Laundering with Crypto

$455 million stolen by Lazarus, a North Korean government-backed hacking group, was laundered.
https://www.reuters.com/business/finance/us-scraps-sanctions-tornado-cash-crypto-mixer-accused-laundering-north-korea-2025-03-21/

Redbelly Network

Vincent Gramoli

University of Sydney

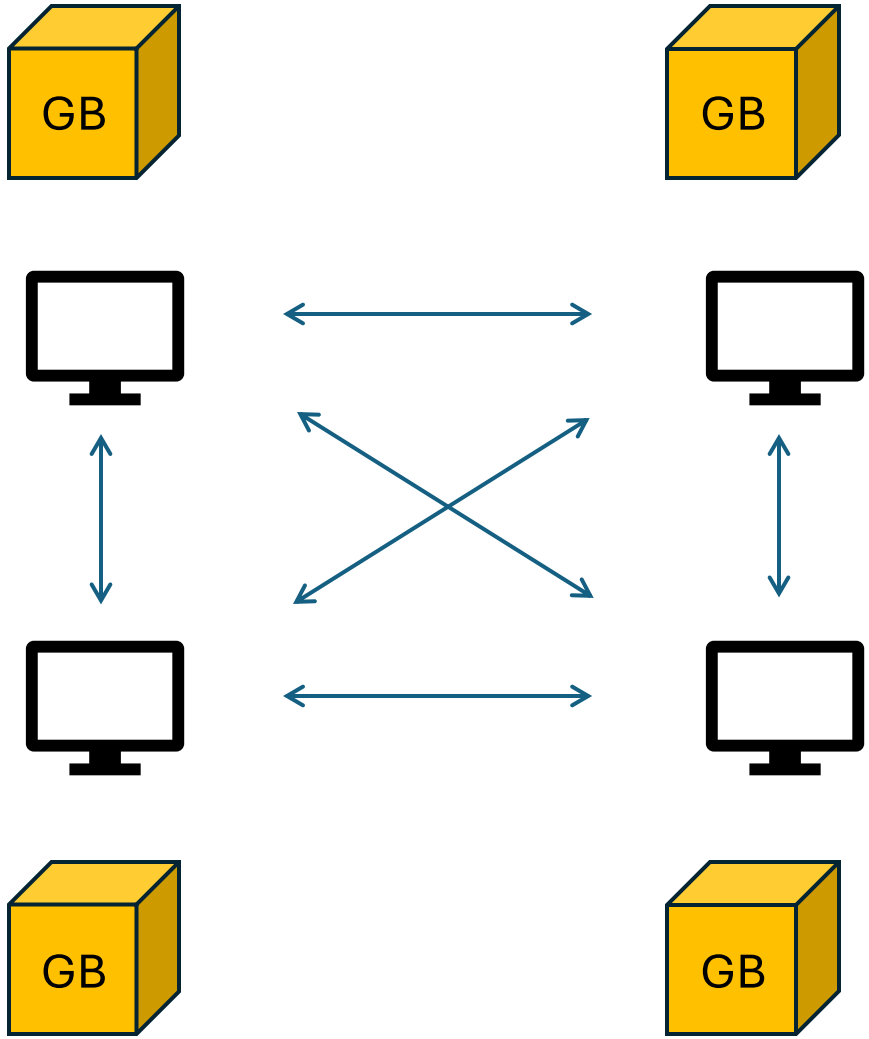
Redbelly Network

Roadmap

1. How to make blockchain more secure
2. How to make sure it is correct
3. How to make sure this is efficient
4. How to run generic applications
5. How to make sure it is reliable
6. How to mitigate front running attacks
7. How to prevent money laundering
8. Why these decisions proved us right

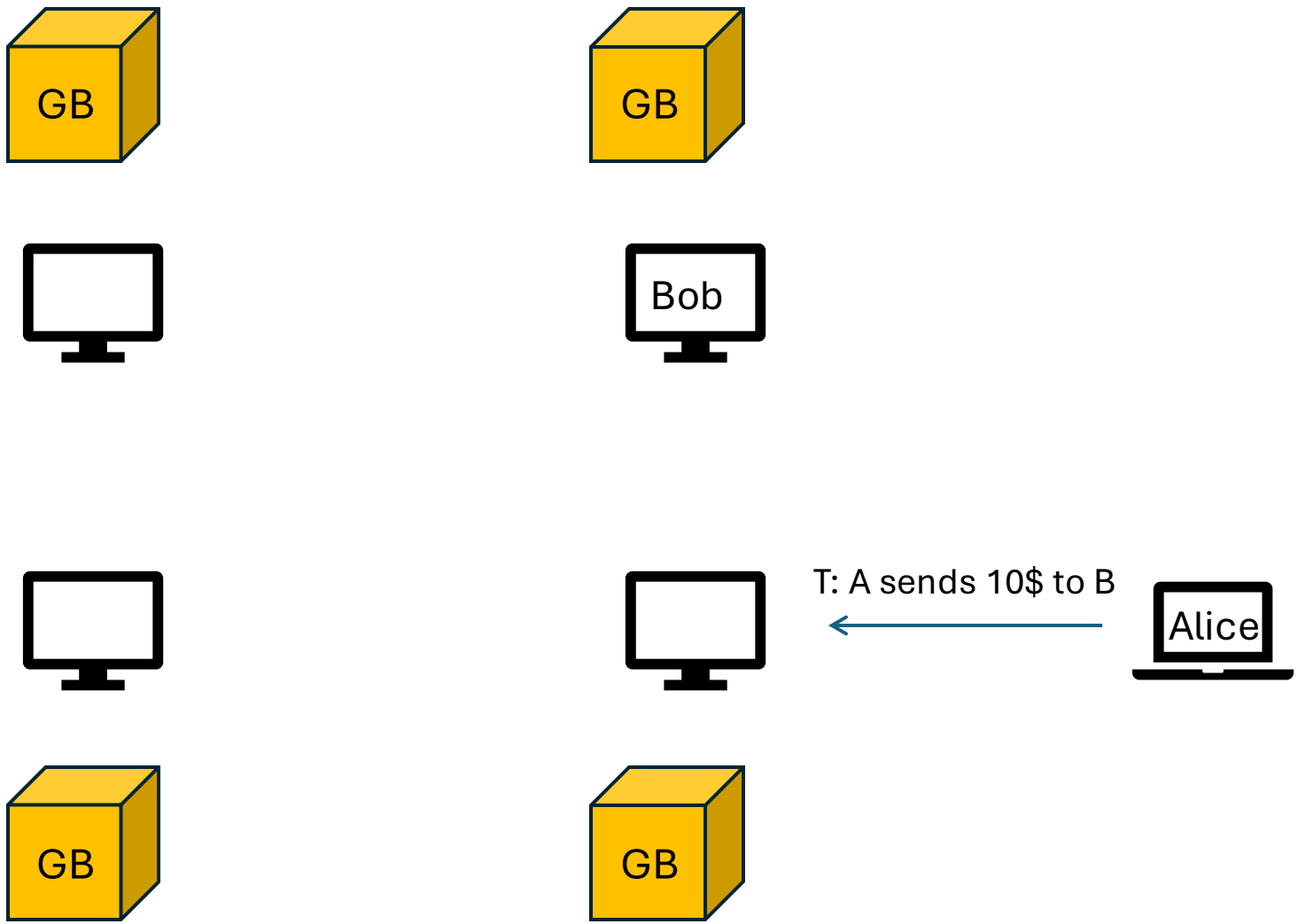
How to make Blockchain more secure

Blockchain

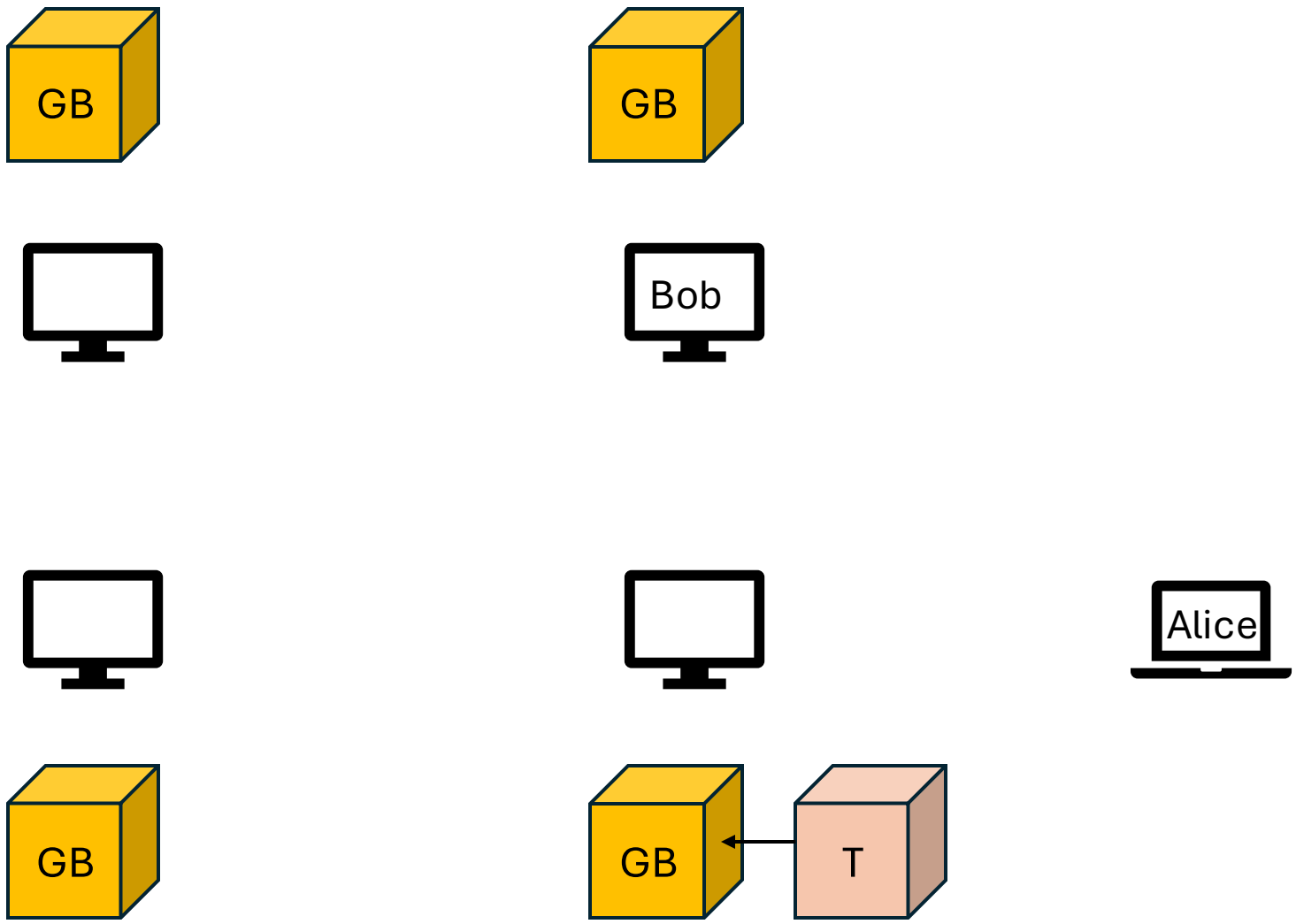


Bitcoin: A Peer-to-Peer Electronic Cash System.
S. Nakamoto, 2008.

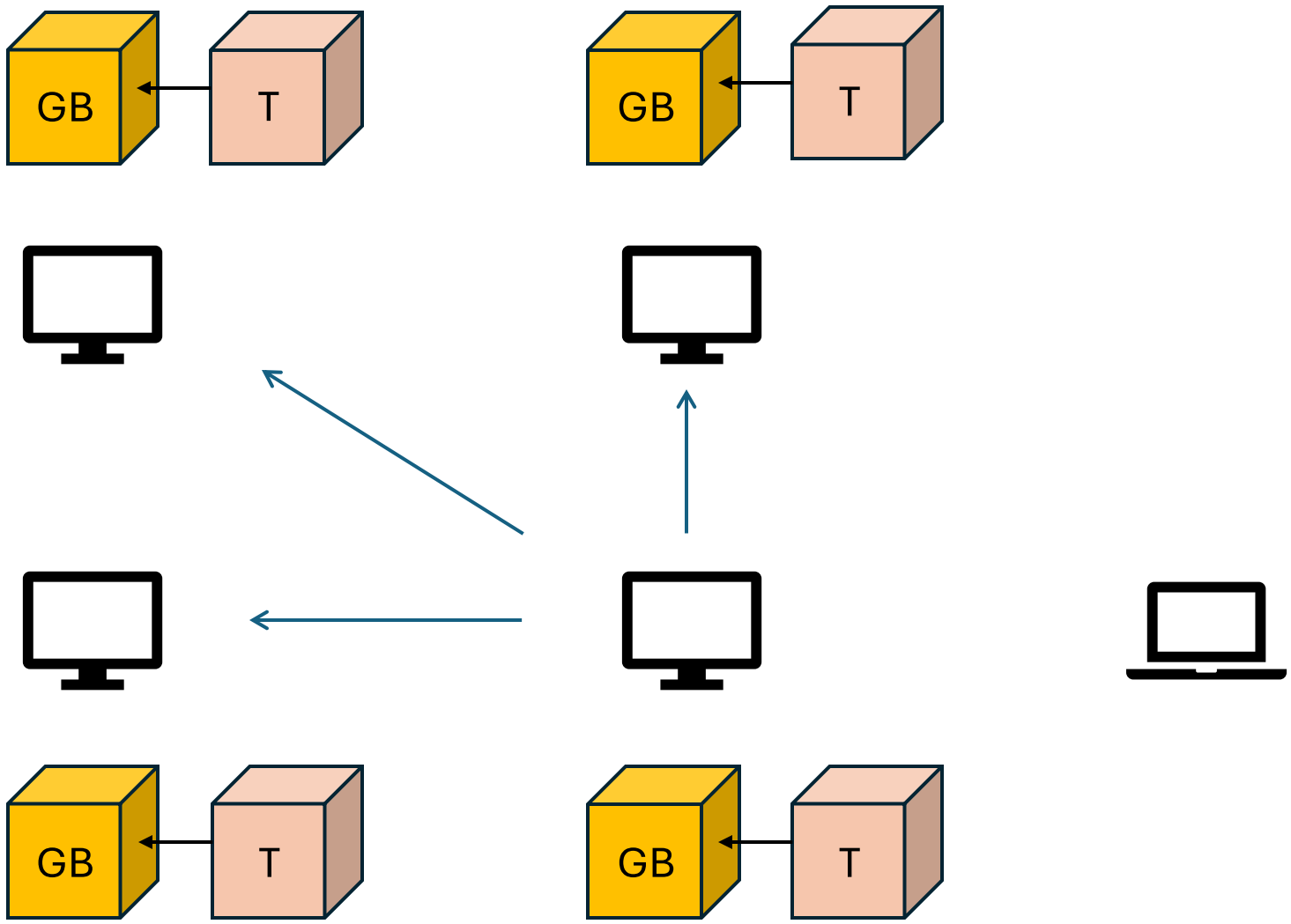
Blockchain



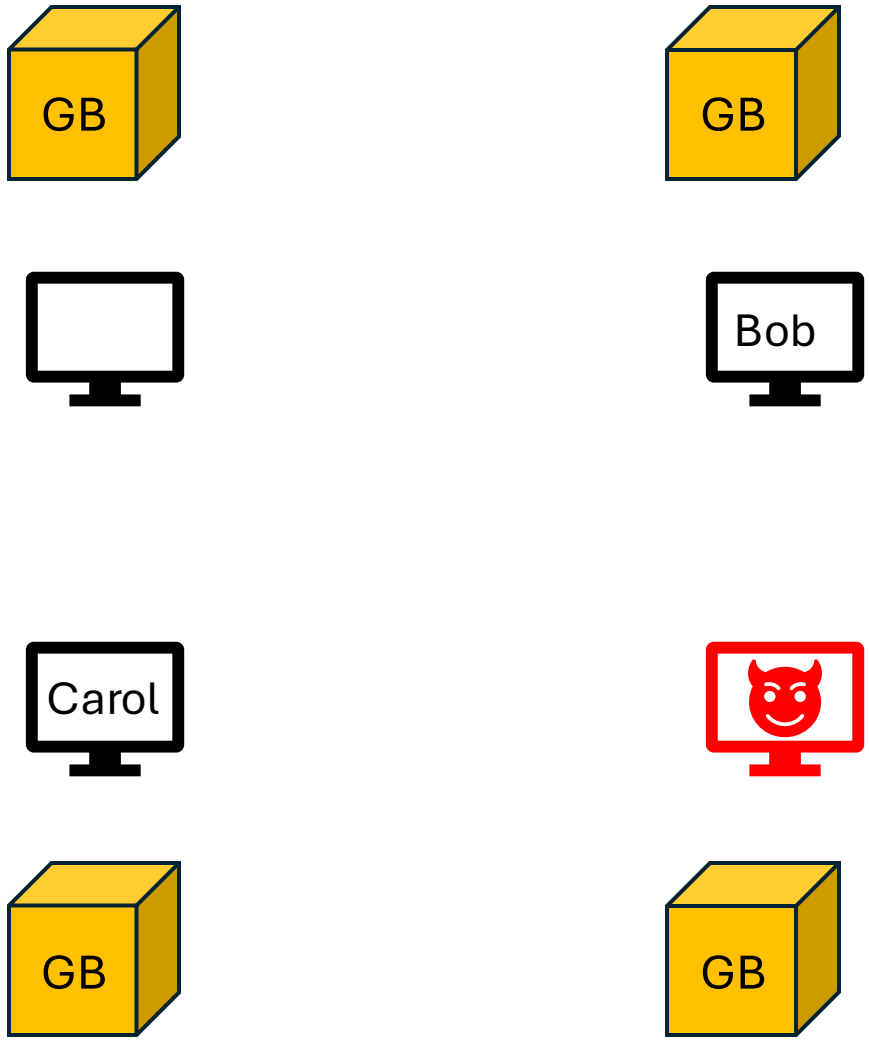
Blockchain



Blockchain

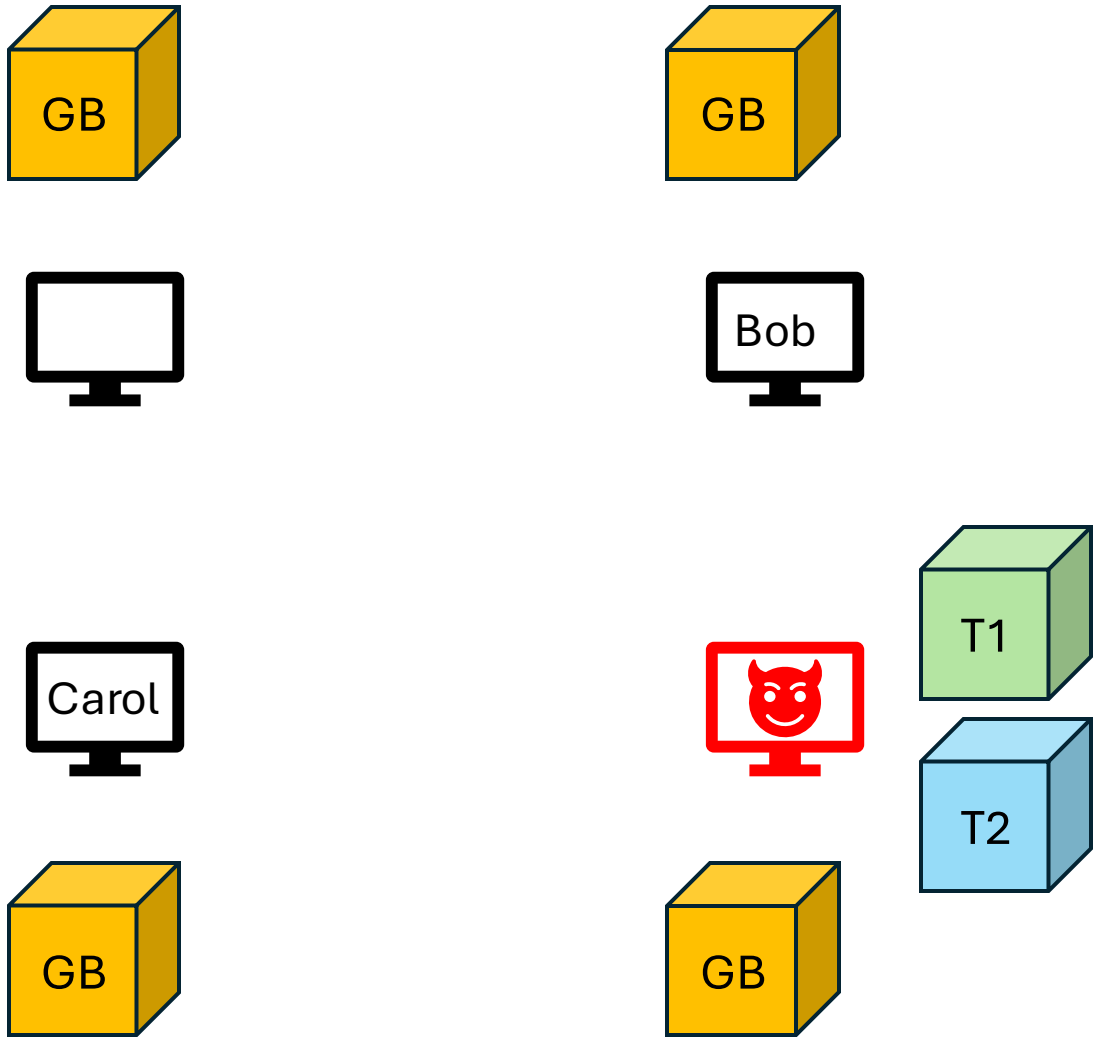


Problem: Double Spending

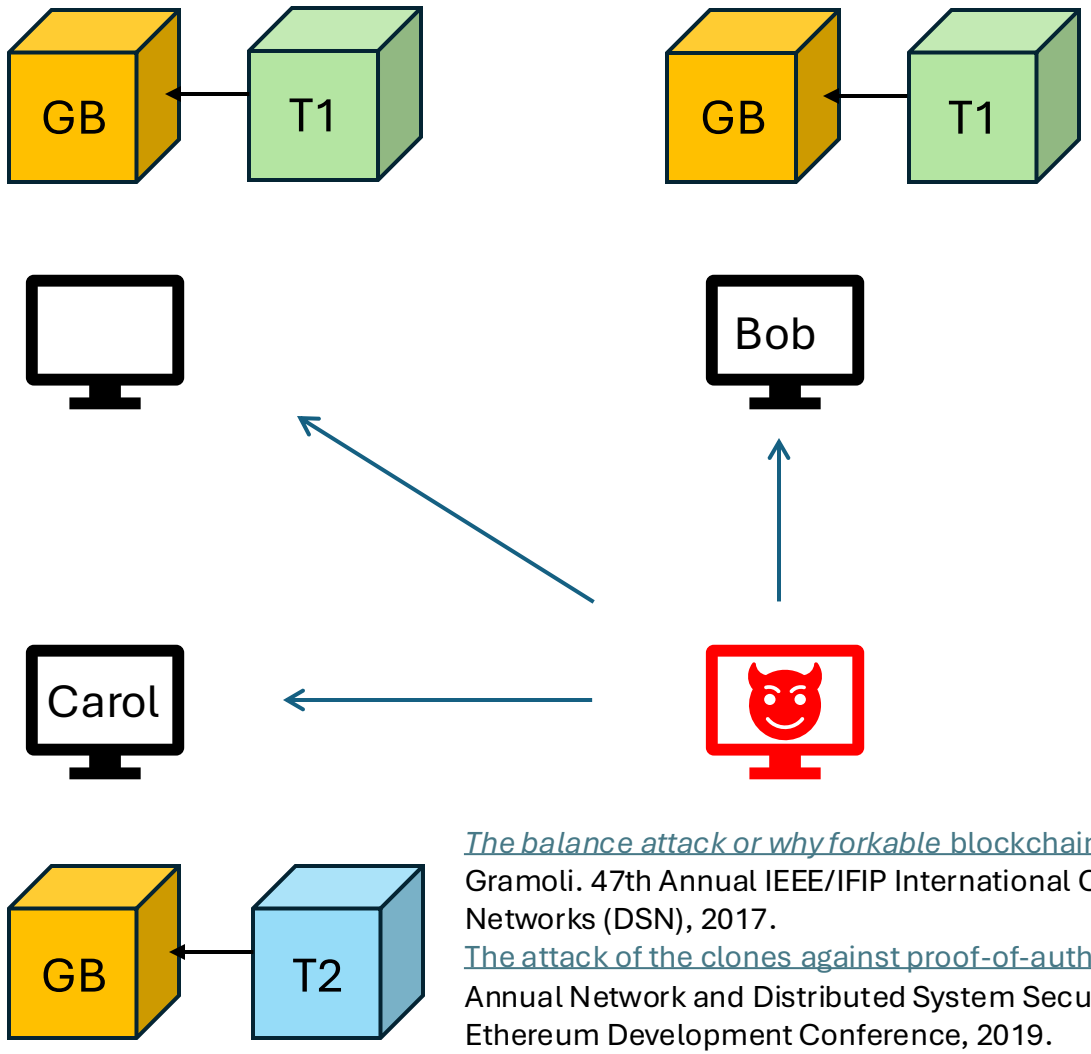


T1: M sends all her coins to B
T2: M sends all her coins to C

Problem: Double Spending



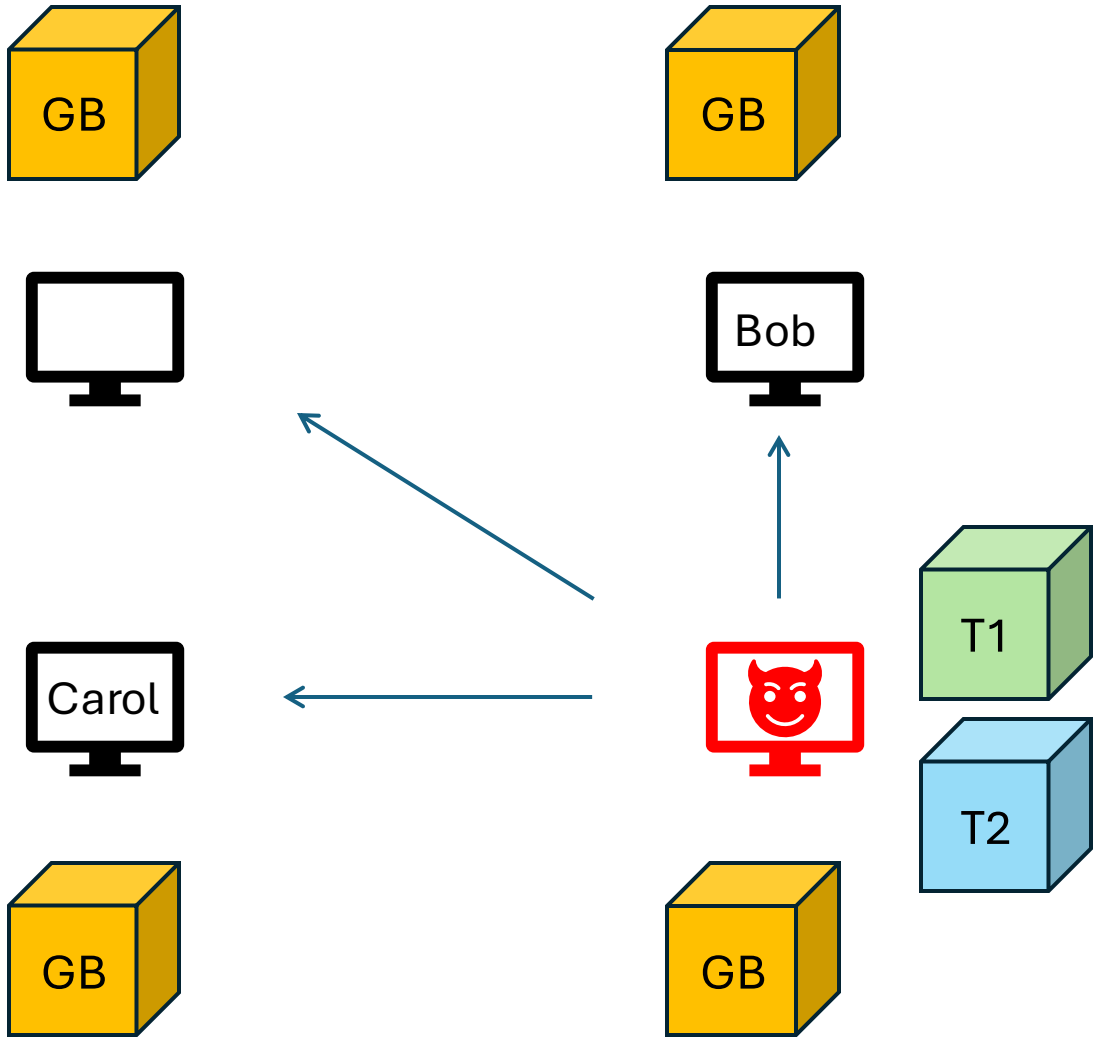
Problem: Double Spending



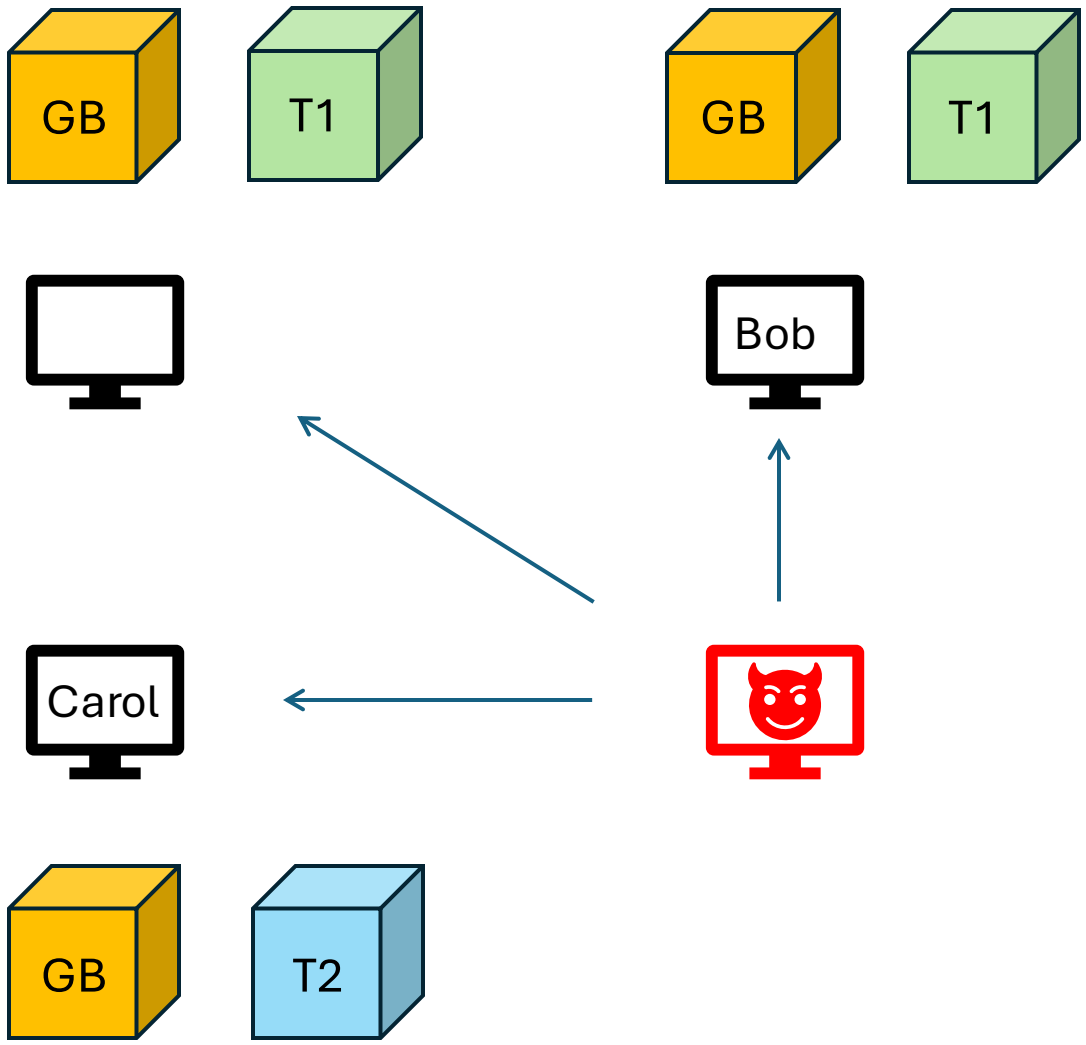
The balance attack or why forkable blockchains are ill-suited for consortium. C Natoli, V Gramoli. 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2017.

The attack of the clones against proof-of-authority. P Ekparinya, V Gramoli, G Jourjon. 27th Annual Network and Distributed System Security Symposium (NDSS), 2020. Community Ethereum Development Conference, 2019.

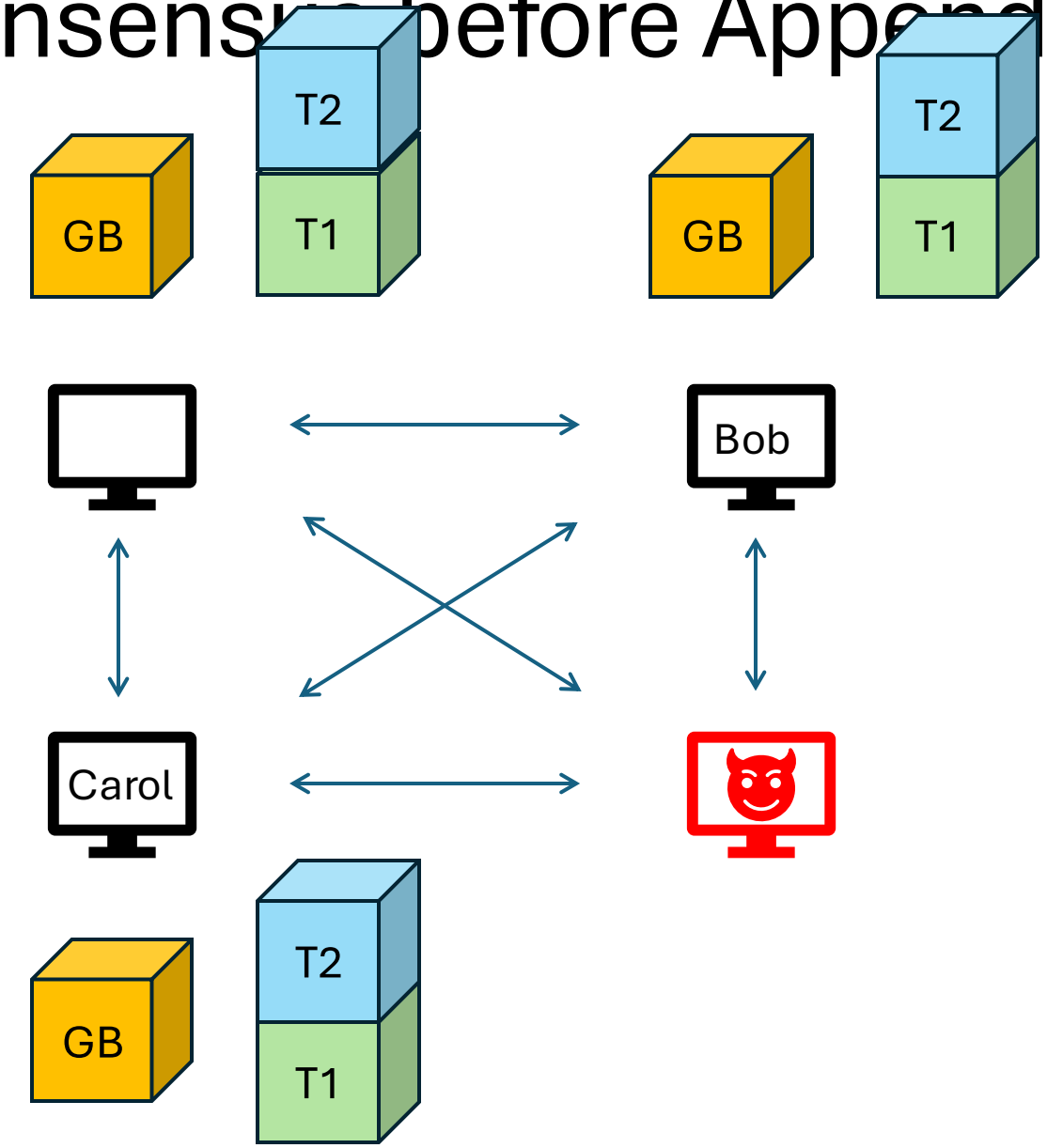
Solution: Consensus before Appending Blocks



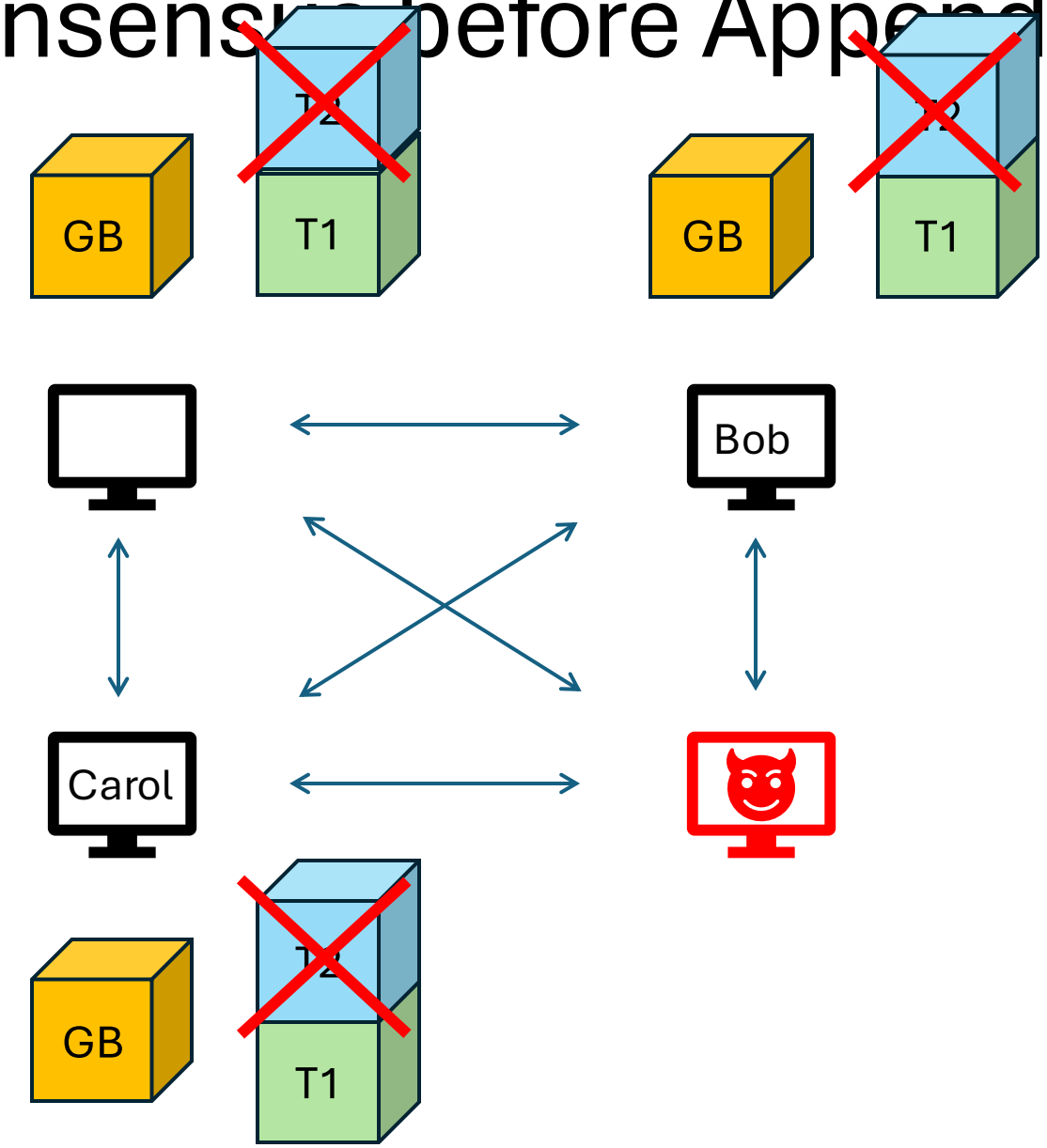
Solution: Consensus before Appending Blocks



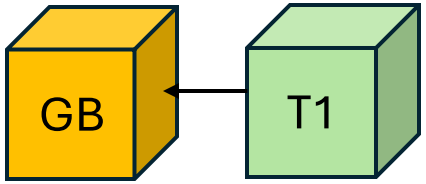
Solution: Consensus before Appending Blocks

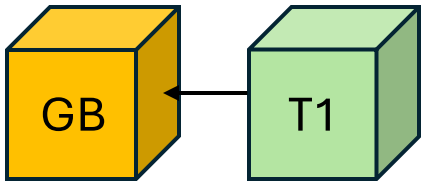


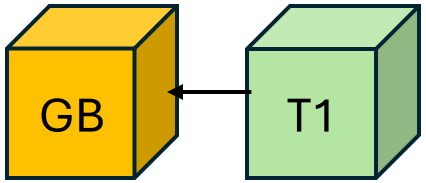
Solution: Consensus before Appending Blocks



Solution: Consensus before Appending Blocks







DBFT: Efficient Leaderless Byzantine Consensus and its Application to Blockchains. T. Crain, V. Gramoli, M. Larrea, M. Raynal. IEEE 17th Int'l Symposium on Network Computing and Applications. 2018.

Solution: Consensus before Appending Blocks

- Uniqueness of the block at each index is key to avoid double spending
- Reaching consensus guarantees the uniqueness of this block
- But how to make sure that the consensus protocol works as expected?

How to make sure it is correct

Proving a Consensus Protocol is Insufficient

- Ripple consensus at the heart of XRP had a flaw in its proof
- Zyzzyva [ACM TOCS'07], the best paper at SOSP 2007, had a flaw in its manual proof [arXiv'17], it took 10 years to find it.

Formal Verification of Blockchain Byzantine Consensus Fault Tolerance. P. Tholoniat, V. Gramoli. 36th in Handbook on Blockchain.DOI: 10.1007/978-3-031-07535-3_12, November 2022.

Formal Verification of Blockchain Consensus

- We specified DBFT in a threshold automaton (TA)
- We exploited our fairness property to reduce the TA
- We used the Byzantine Model Checker [POPL'17]
- DBFT solves consensus in any possible execution for any system size

Holistic Verification of Blockchain Consensus *N. Bertrand, V. Gramoli, M. Lazić, I. Konnov, P. Tholoniat, J. Widder. 36th International Symposium on Distributed Computing (DISC), 2022.*

Solution: Consensus before Appending Blocks

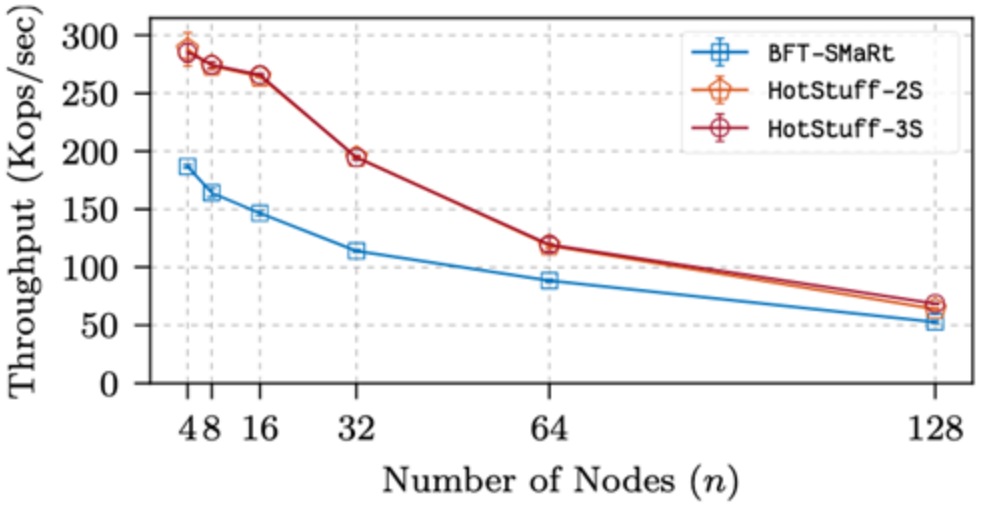
- Formal verification of the consensus protocol reduces human errors
- It becomes almost impossible for a hacker to double spend
- But is the performance overhead of this security manageable?

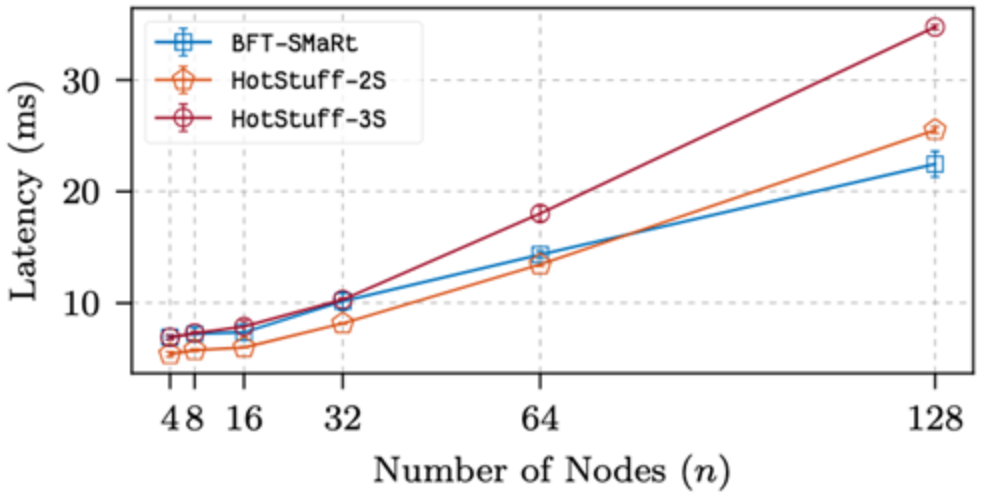
Formal Verification of Blockchain Byzantine Consensus Fault Tolerance. P. Tholoniat, V. Gramoli. 36th in Handbook on Blockchain.DOI: 10.1007/978-3-031-07535-3_12, November 2022.

How to make sure this is efficient

Byzantine Consensus never Scaled

- Practical Byzantine consensus protocols were designed for LAN
- All Byzantine consensus protocols used in blockchain are similar
  - Hotstuff, Tendermint, SBFT, IBFT, BFT-Smart
  - They are all leader-based





- Their performance drops with the system size

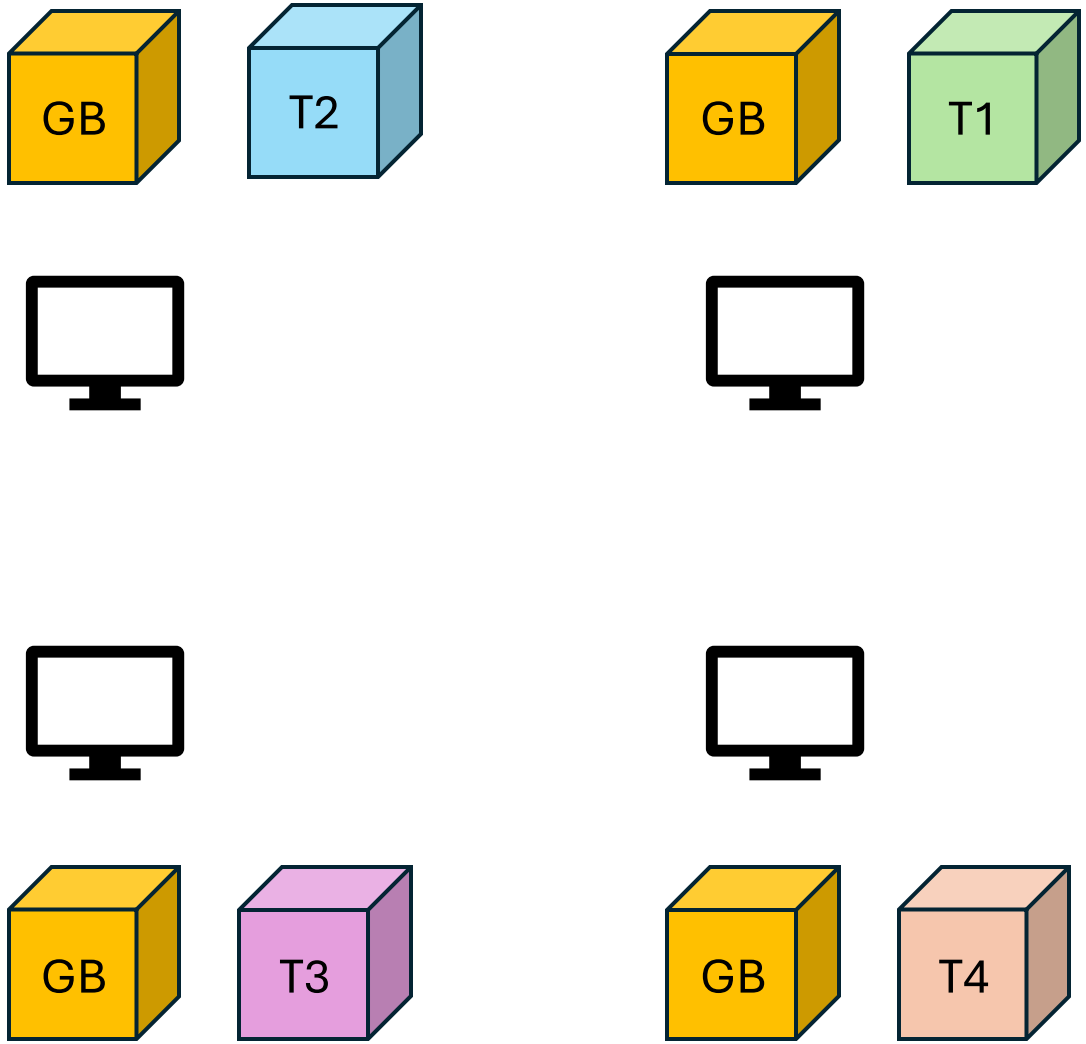
Planetary Scale Byzantine Consensus . G. Voron, V. Gramoli. ACM Workshop on Advanced tools, programming languages, and PLatforms for Implementing and Evaluating algorithms for Distributed systems (ApPLIED), 2023.

Problem: Competition in the Blockchain Network

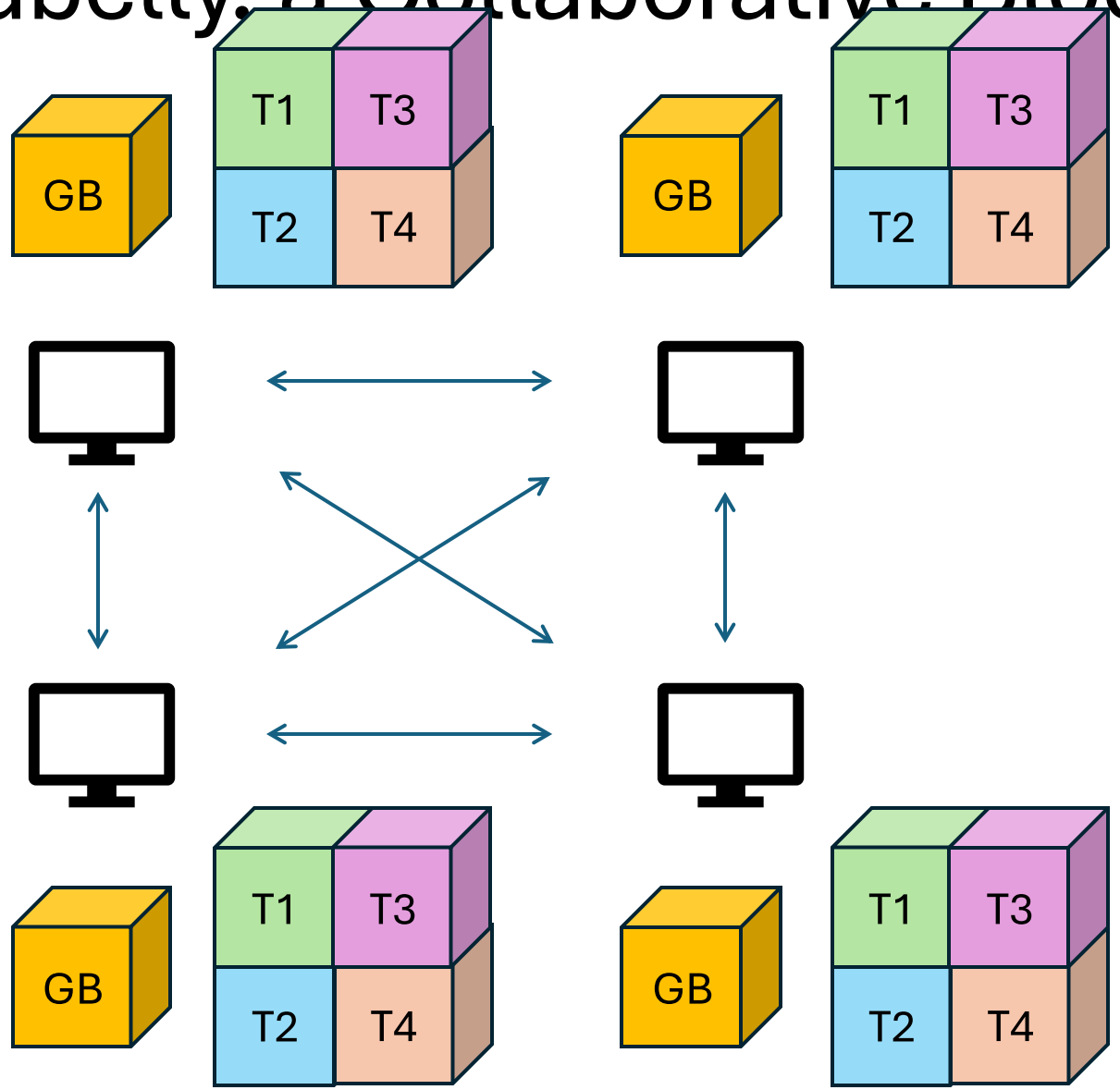
- All participants try to impose their block to the rest of the system
- This competition is a waste of efforts and resources
- Participants should collaborate and combine their blocks instead

Red Belly: A secure, fair and scalable open blockchain. T Crain, C Natoli, V Gramoli. IEEE Symposium on Security and Privacy (S&P), 466-483, 2021.

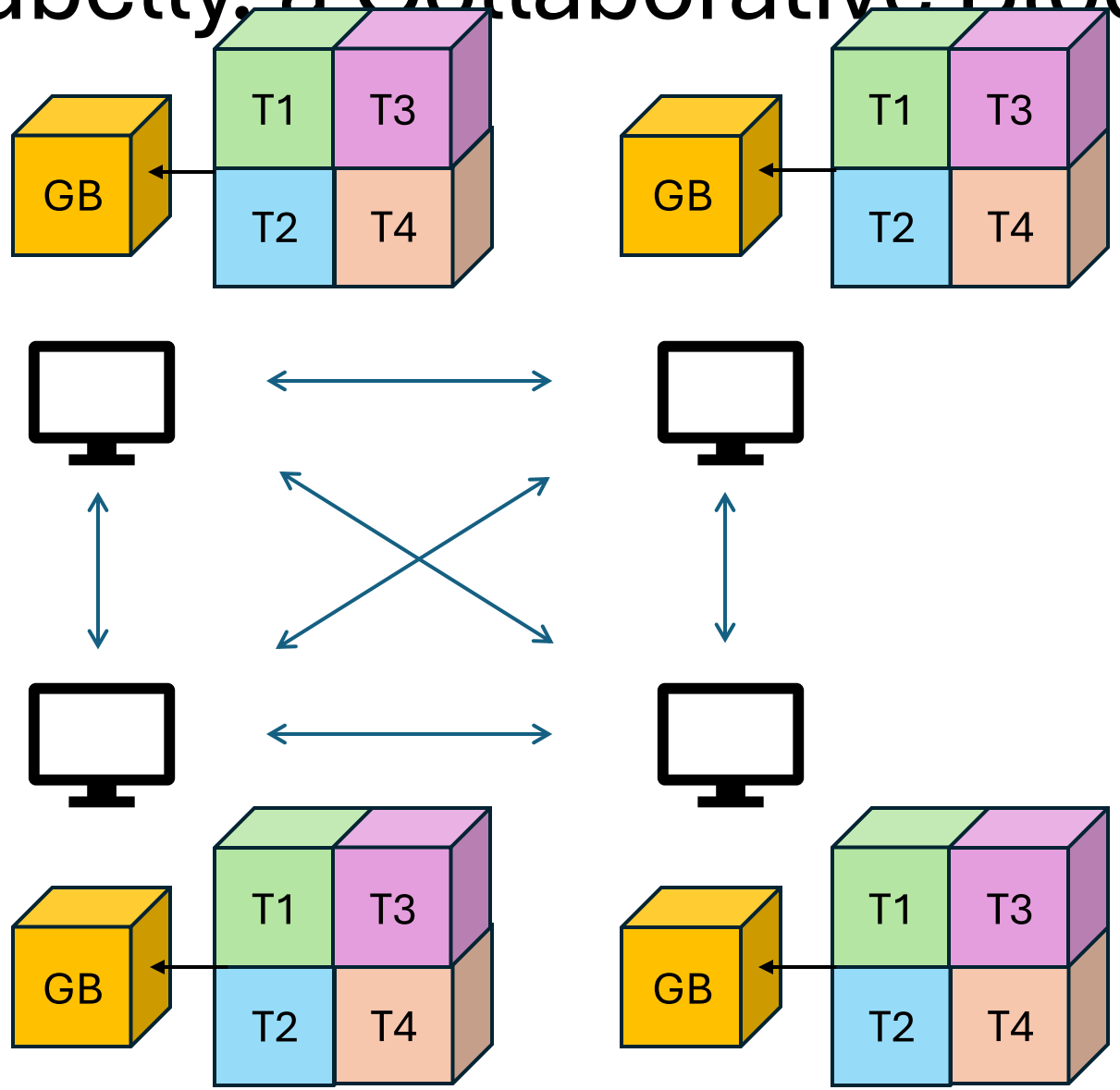
Solution: Redbelly, a Collaborative Blockchain



Solution: Redbelly, a Collaborative Blockchain

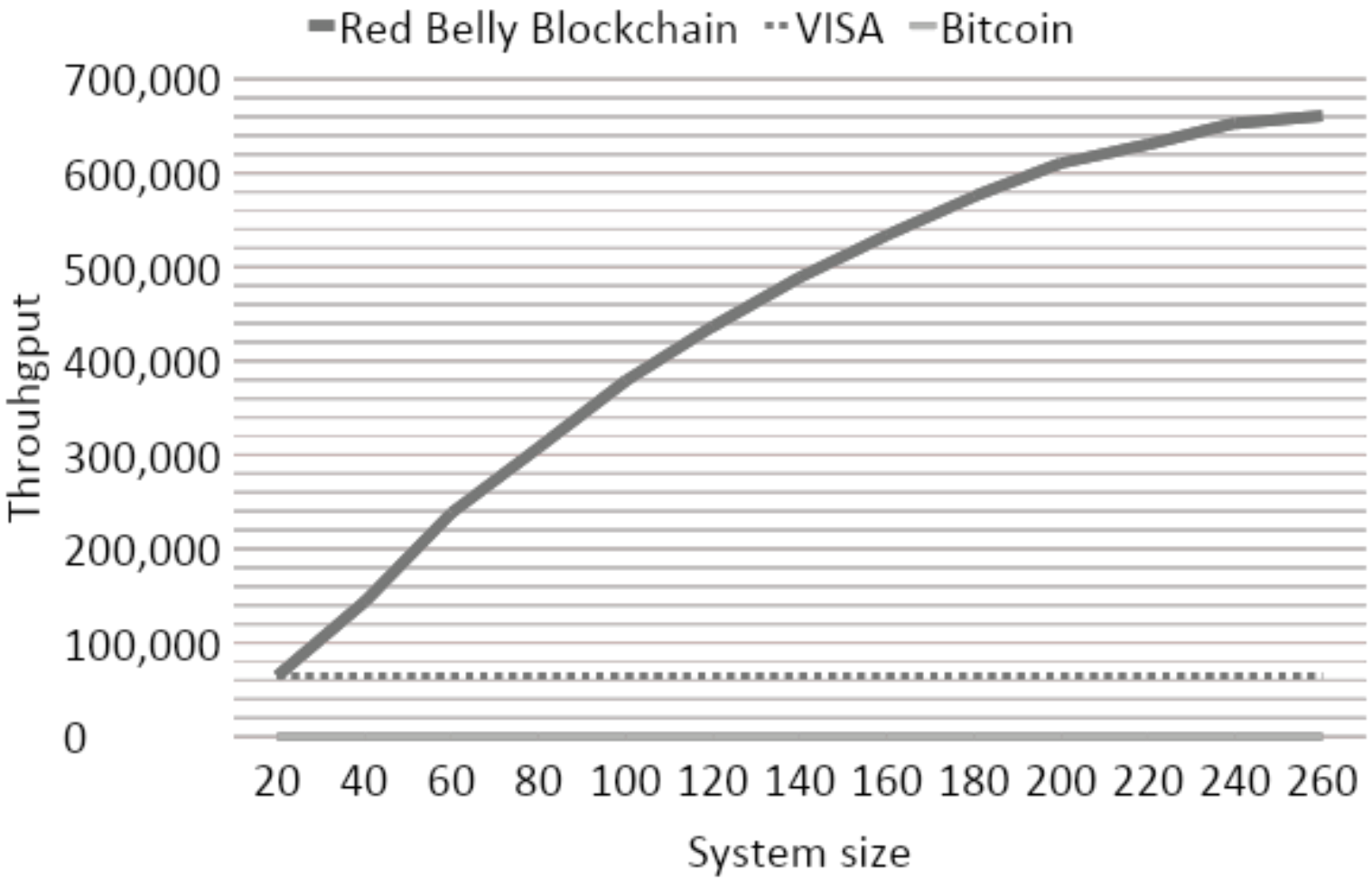


Solution: Redbelly, a Collaborative Blockchain



Solution: Redbelly, a Collaborative Blockchain

- Amazon EC2 instances
- One availability zone in US
- System size from 4 to 260
- 18 HT cores per node
- 60 GB memory
- 2 Gbps
- t=6 failures max.



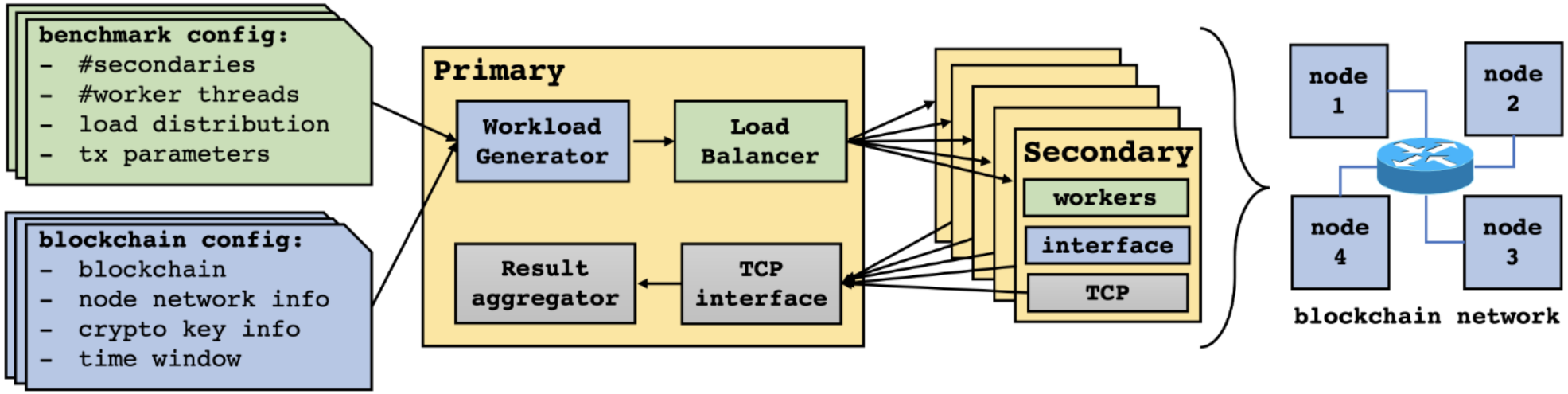
Red Belly: A secure, fair and scalable open blockchain. T Crain, C Natoli, V Gramoli. IEEE Symposium on Security and Privacy (S&P), 466-483, 2021.

Solution: Redbelly, a Collaborative Blockchain

- Collaboration allows more nodes to commit more transactions
- Redbelly executes simple transactions fast while preventing double spending
- But how would it perform executing realistic applications?

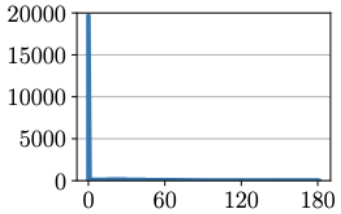
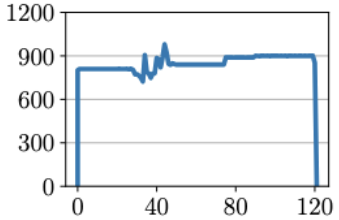
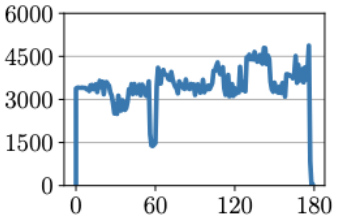
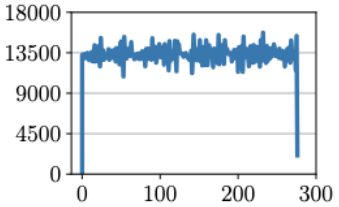
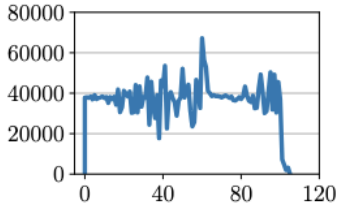
How to run generic applications

Diablo Benchmark with Real DApps



Diablo: A Benchmark Suite for Blockchains. *V. Gramoli, R. Guerraoui, A. Lebedev, C. Natoli, G. Voron. 18th ACM European Conference on Computer Systems (EuroSys), 2023*

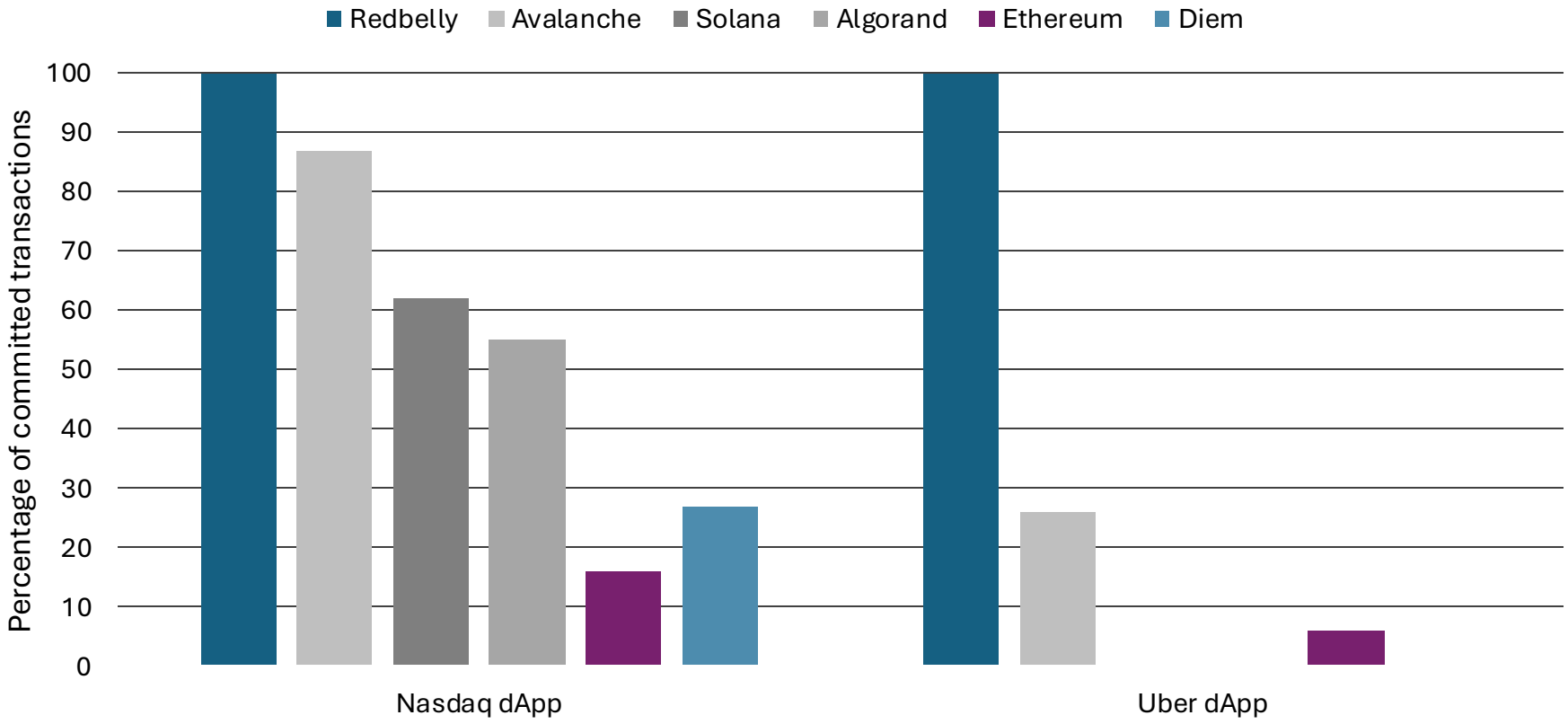
Diablo Benchmark with Real DApps

DApp	Exchange	Mobility service	Web service	Gaming	Video sharing
Workload					
Source trace	NASDAQ	Uber	FIFA	Dota 2	YouTube
Characteristics	Burst	Compute intensive	Contended	High sending rate	Very high sending rate

None of the tested blockchains (Algorand, Avalanche, Diem, Ethereum, Quorum, Solana) could commit all transactions in any of these applications!

Diablo: A Benchmark Suite for Blockchains. V. Gramoli, R. Guerraoui, A. Lebedev, C. Natoli, G. Voron. 18th ACM European Conference on Computer Systems (EuroSys), 2023

Redbelly commits all transactions



Deconstructing the Smart Redbelly Blockchain. D. Tennakoon, V. Gramoli. IEEE Transactions on Computers, DOI:10.1109/TC.2024.3475573, 2024.

Redbelly, the fastest among 50 blockchains

#	Name	Max TPS (1 block)	Max Theor. TPS	Total Transactions	Block Time	Finality	Governance
1	Redbelly New Layer 1	97,500 tx/s	666,970 tx/s	23 txns	2m 37s	0s	Council
2	Taraxa Layer 1	61,525 tx/s	50,000 tx/s	188,046 txns	3.51s	0s	Council
3	Waterfall Layer 1	30,000 tx/s	13,333 tx/s	1,312 txns	2.84s	24s	Council
4	ICP Layer 1	25,621 tx/s	209,708 tx/s	3,554,187 txns	0.48s	0s	On-chain
5	Aptos Layer 1	22,032 tx/s	160,000 tx/s	72,731 txns	0.13s	0.9s	On-chain
6	MultiversX Layer 1	13,878 tx/s	30,000 tx/s	7,840 txns	6s	6s	On-chain
7	Solana Layer 1	10,605 tx/s	65,000 tx/s	3,400,712 txns	0.4s	12.8s	Off-chain
8	NEAR Layer 1	10,380 tx/s	12,000 tx/s	303,677 txns	1.15s	2s	Council
9	Algorand Layer 1	9,079 tx/s	9,384 tx/s	48,780 txns	2.81s	0s	On-chain
10	Hedera Layer 1	8,478 tx/s	10,000 tx/s	69,470 txns	2s	7s	Council

Source: https://chainspect.app/dashboard?sort=theorTps as of 16 April 2025

Solution: Redbelly, a Collaborative Blockchain

- Redbelly can handle a high load while running complex applications
- Redbelly is fast while preventing double spending
- But how do you make sure Redbelly can be robust in case of failures?

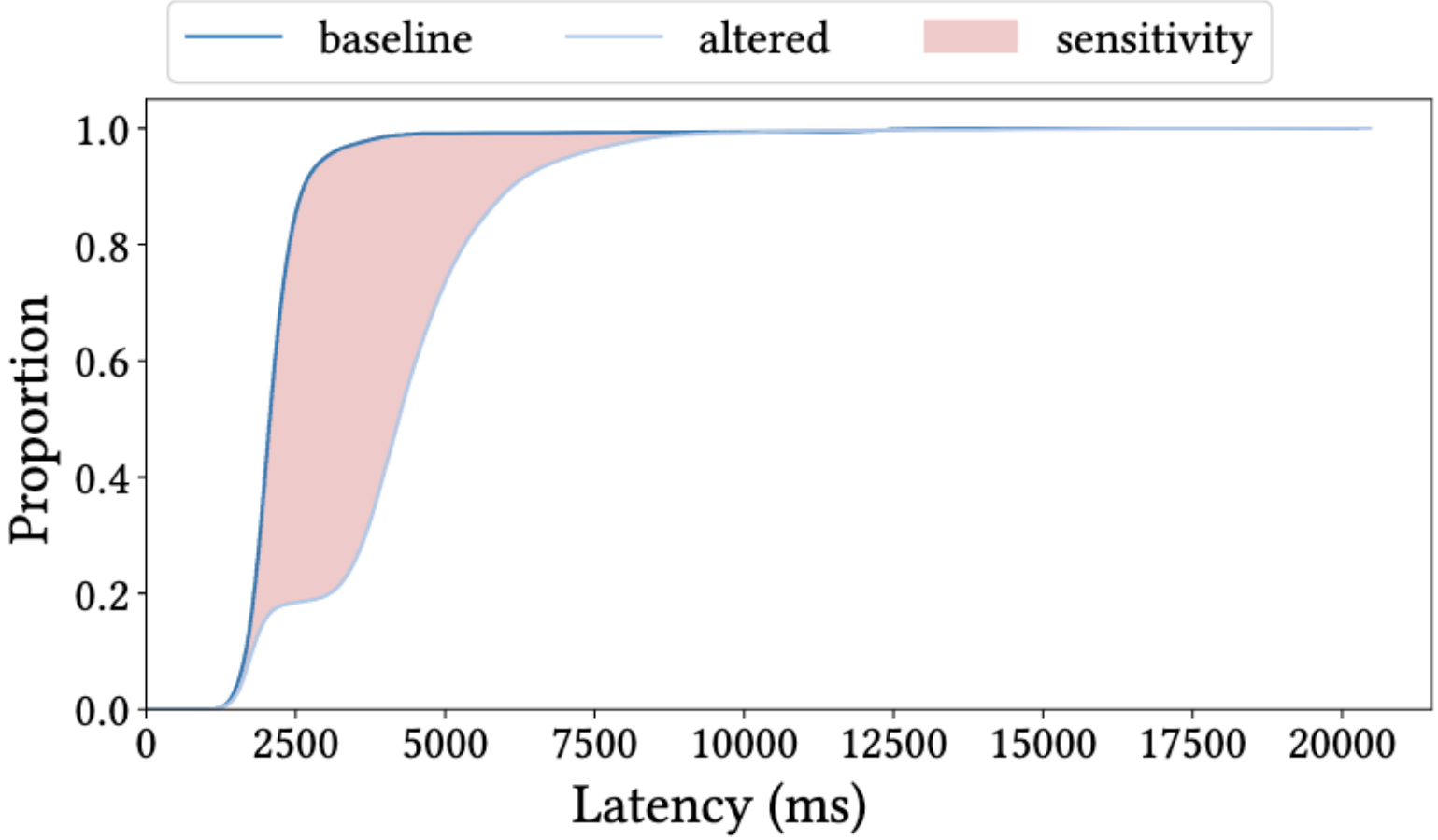
How to make sure it is reliable

Lack of Fault Tolerance in Blockchain

- Blockchain is not as available as cloud services
- In 2023, Solana experienced 154.5h of outages after 17 months.
- This translates into <99% availability
- Cloud computing services typically offer ≥99.9%.

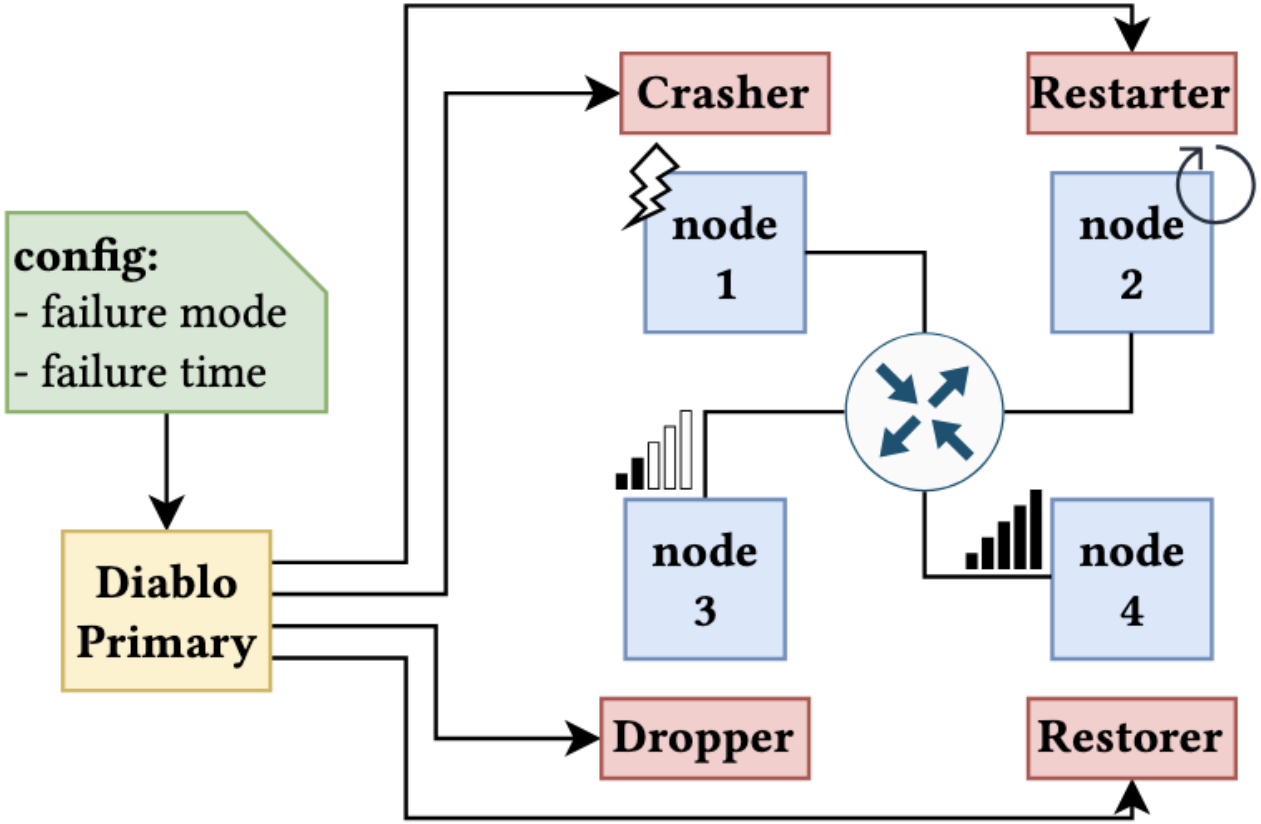
STABL: The Sensitivity of Blockchains to Failures. *V. Gramoli, R. Guerraoui, A. Lebedev, G. Voron. 26th ACM/IFIP International Middleware Conference (Middleware), 2025.*

Sensitivity to Failures



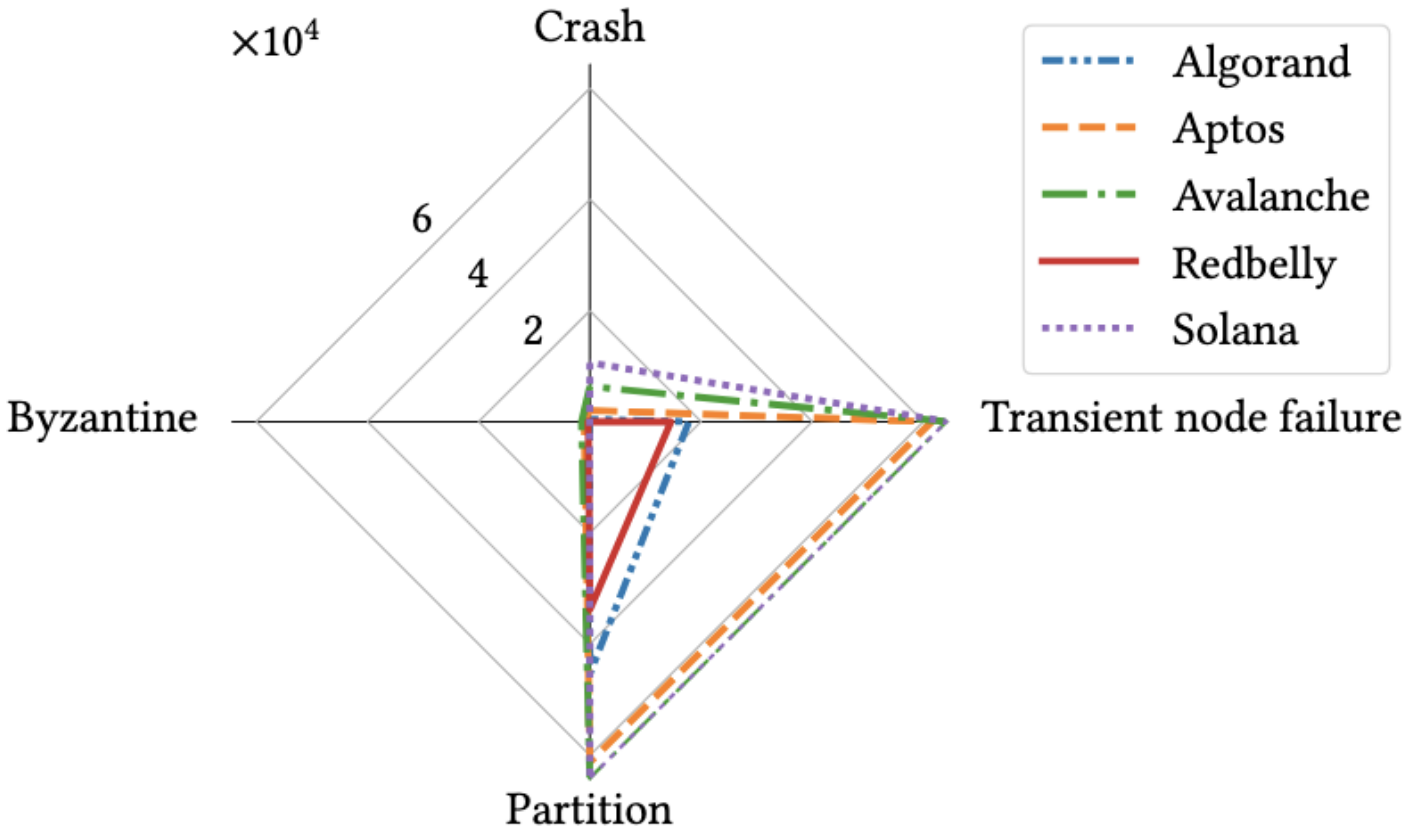
STABL: The Sensitivity of Blockchains to Failures. V. Gramoli, R. Guerraoui, A. Lebedev, G. Voron. 26th ACM/IFIP International Middleware Conference (Middleware), 2025.

Sensitivity to Failures



STABL: The Sensitivity of Blockchains to Failures. *V. Gramoli, R. Guerraoui, A. Lebedev, G. Voron. 26th ACM/IFIP International Middleware Conference (Middleware), 2025.*

Sensitivity to Failures



STABL: The Sensitivity of Blockchains to Failures. V. Gramoli, R. Guerraoui, A. Lebedev, G. Voron. 26th ACM/IFIP International Middleware Conference (Middleware), 2025.

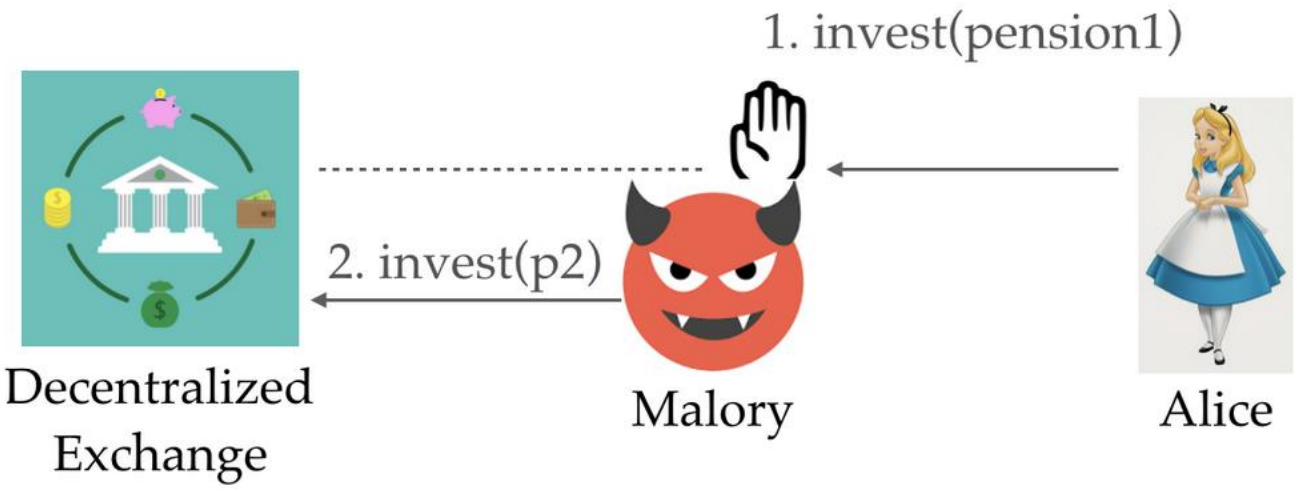
Solution: Redbelly, a Collaborative Blockchain

- Redbelly is secure and efficient
- Redbelly tolerates various failures
- But how do you prevent traders from front running honest users?

How to mitigate front running attacks

Problem: Front Running Attacks

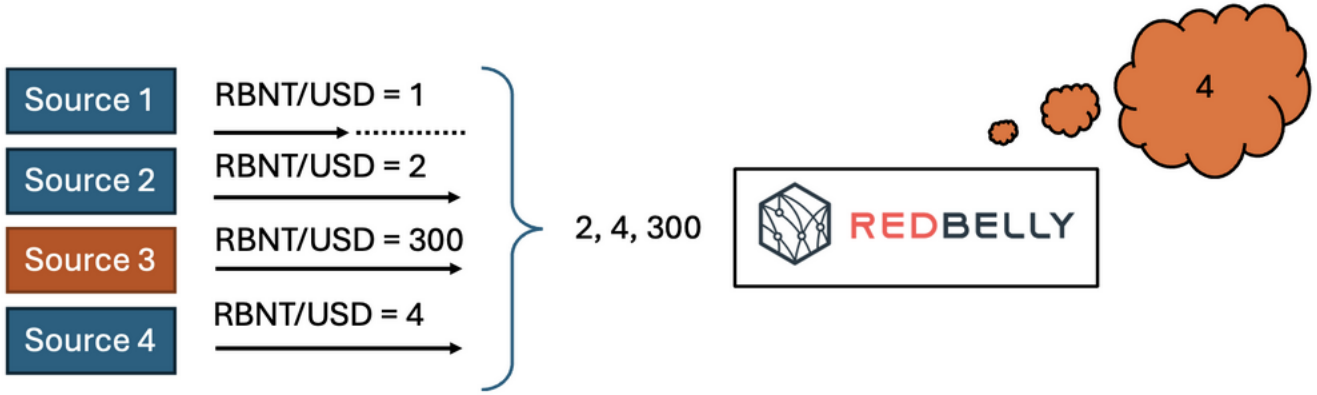
- Front running is illegal on Wall Street and happens every day on blockchains

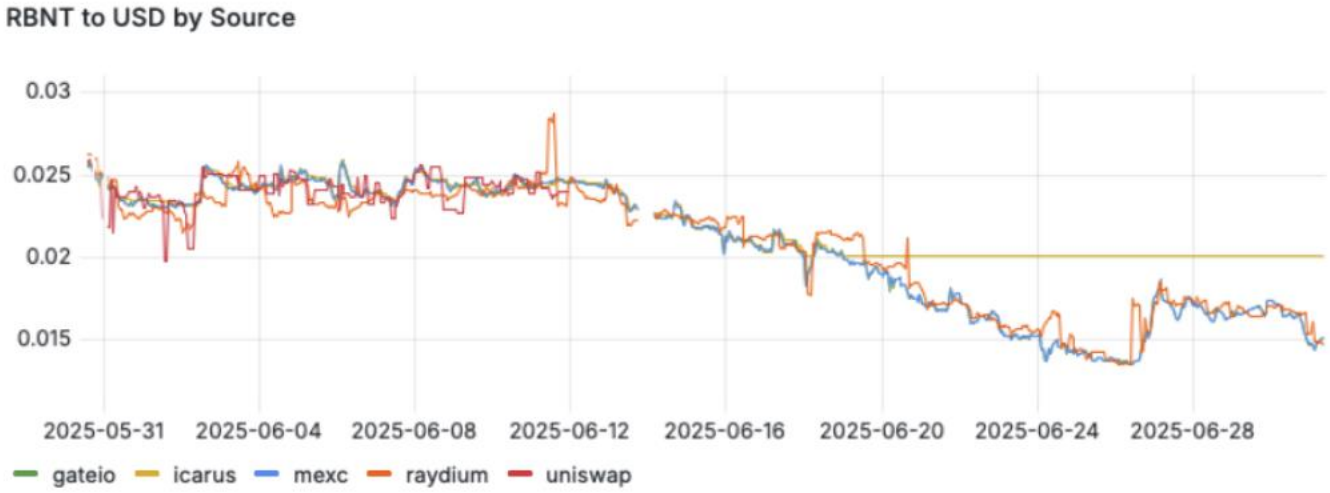


- The crux of the problem is that traders can bribe validators to prioritise their transactions over the transactions of other users

Solution 1: Oracle to fix transaction fees

- The transaction fees are fixed. More precisely, a transaction of 21,000 gas costs USD 0.01. In order to ensure this the RBNT/USD exchange rate is monitored constantly by an oracle.
- The gas price in RBNT is thus adjusted based on the current exchange rate given by multiple exchanges: the median of the values is taken as the correct one.
- When some exchange returns wrong informations, the transaction fee remains correct.





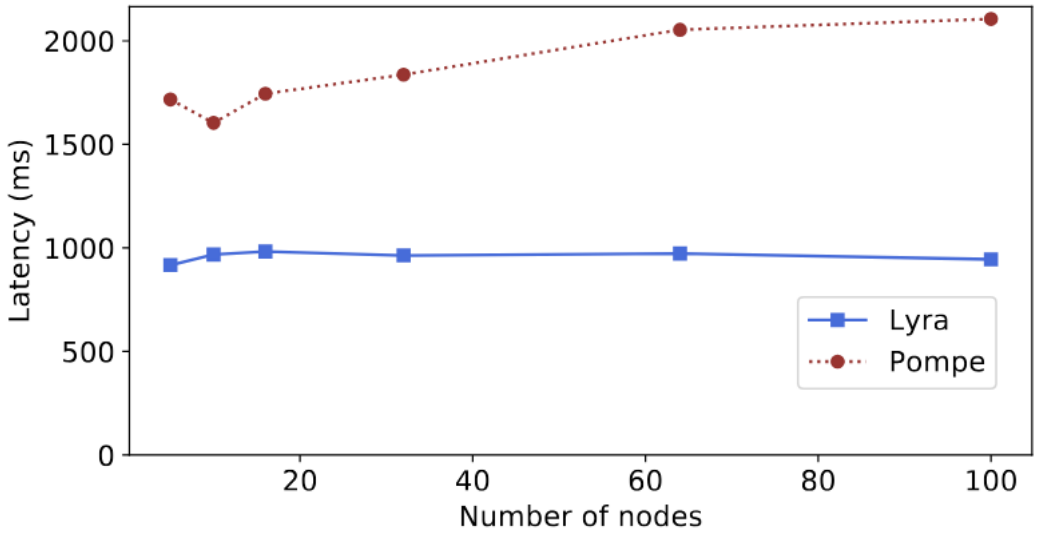
Solution 2: Lyra, enforcing the initial order

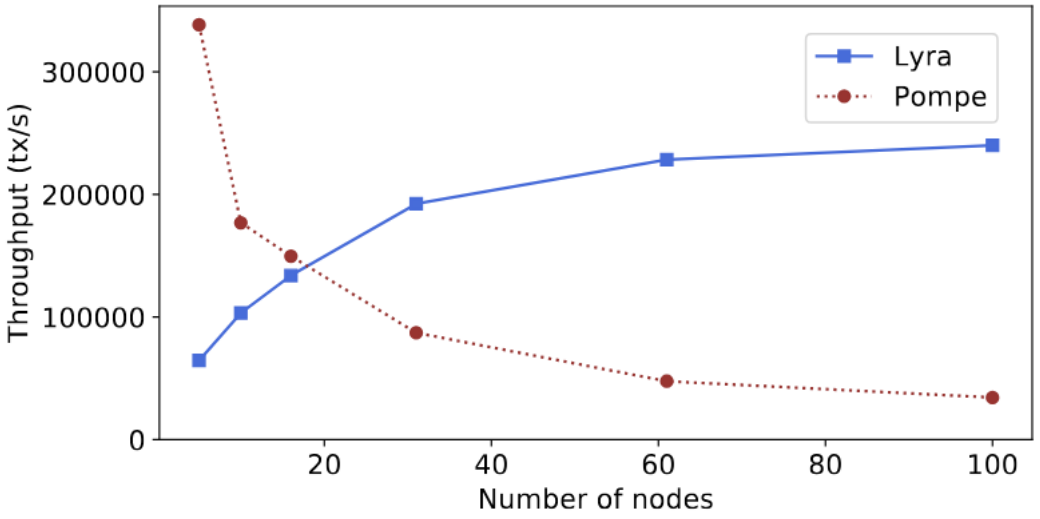
- Preserving the order of transactions slows blockchains down (9 message delays necessary to order first and reach consensus)

- We parallelised the ordering execution with the DBFT consensus execution to achieve a fast ordered consensus protocol.

Byzantine Ordered Consensus without Byzantine Oligarchy. *Y. Zhang, S. Setty, Q. Cheng, L. Zhou, L. Alvisi. USENIX OSDI 2020.*

Solution 2: Lyra, enforcing the initial order





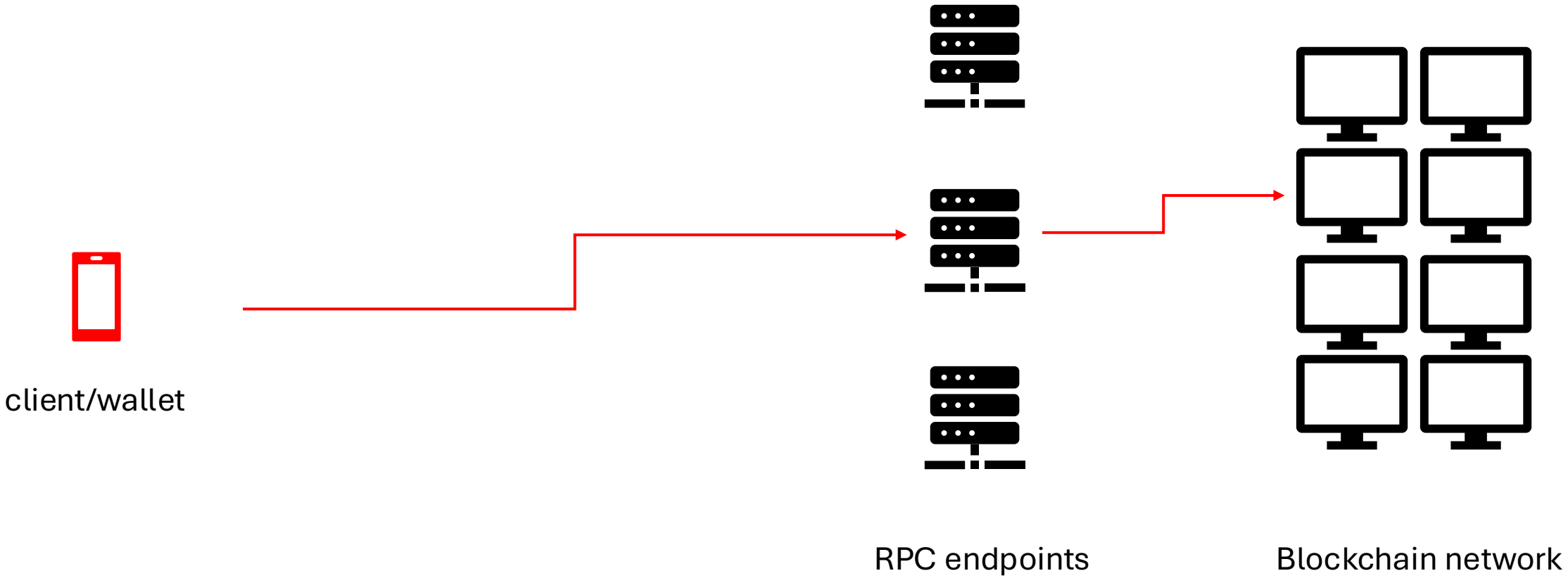
Lyra: Fast and Scalable Resilience to Reordering Attacks in Blockchains. *P. Zarbafian, V. Gramoli. 37th IEEE International Parallel & Distributed Processing Symposium (IPDPS), 2023.*

Solutions: Fixed Fees and Ordered Consensus

- Fixing the transaction fees prevent someone from bribing a validator
- And ordering consensus prevents validators from front running
- But how do you eradicate money laundering then?

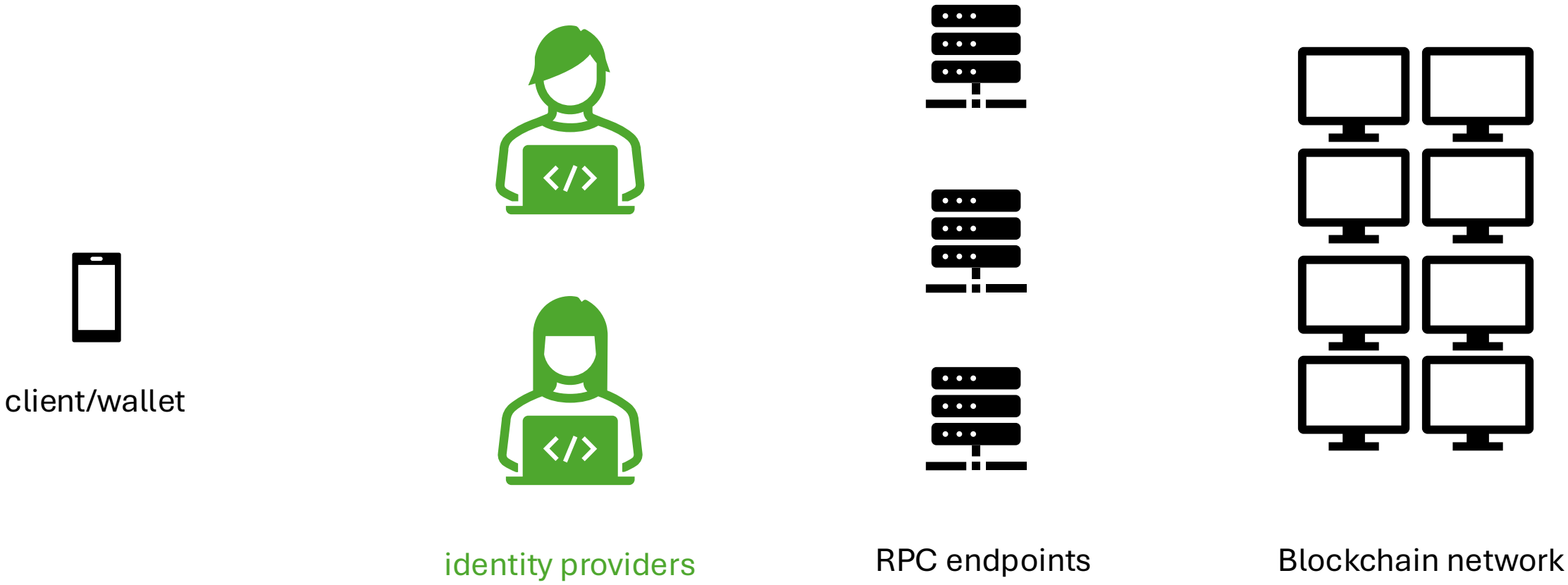
How to prevent money laundering

Problem: Blockchain is Pseudo(/Ano)-nymous

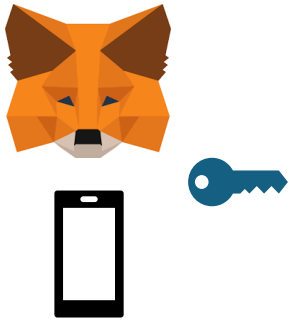


There is no accountability: hackers and terrorists can get away with anything

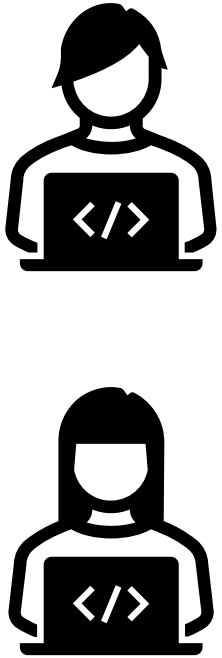
Solution: Offchain Identification



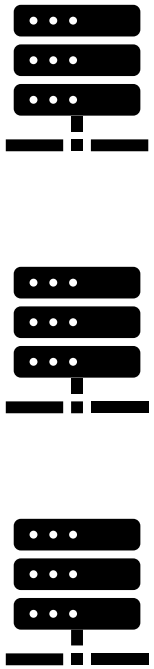
Solution: Offchain Identification



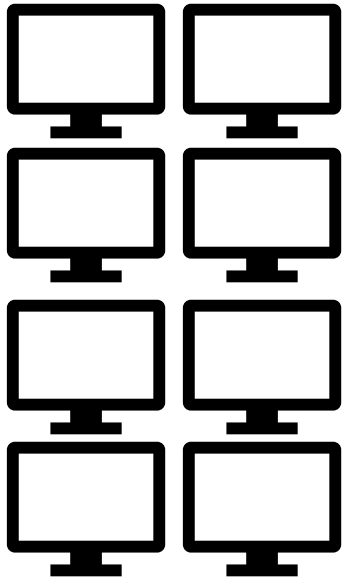
client/wallet



identity providers

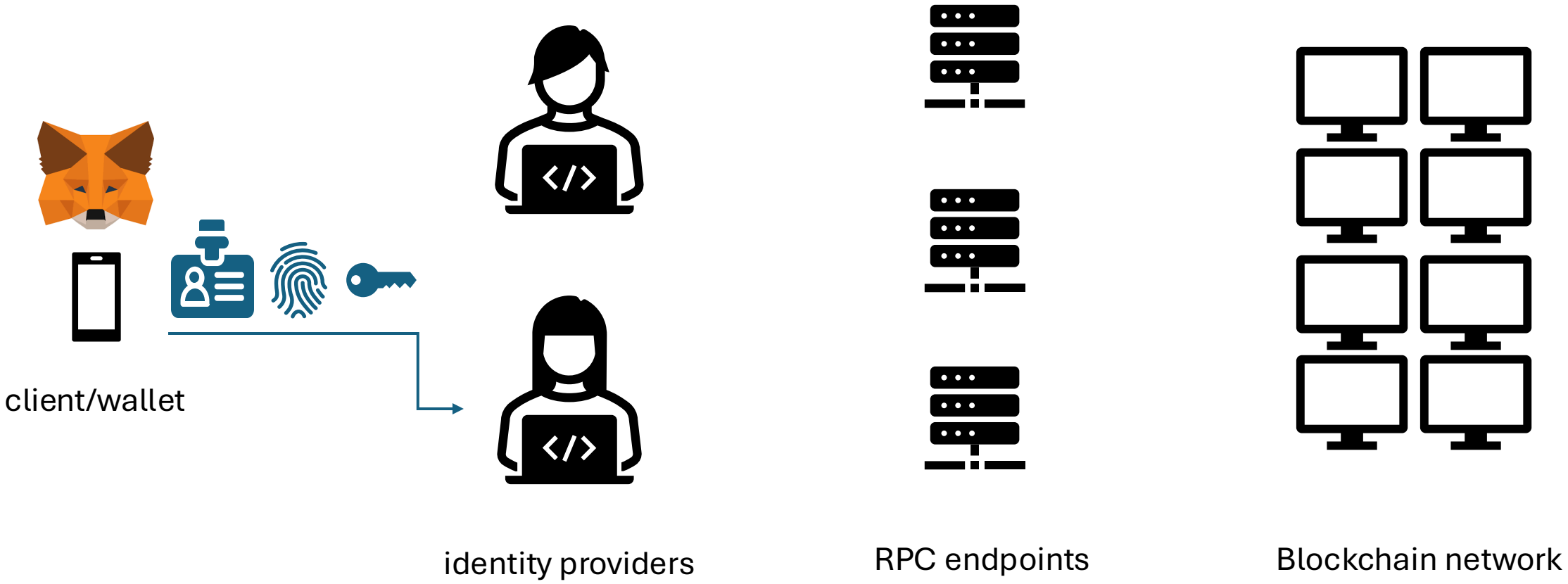


RPC endpoints



Blockchain network

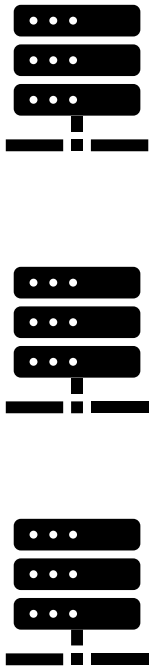
Solution: Offchain Identification



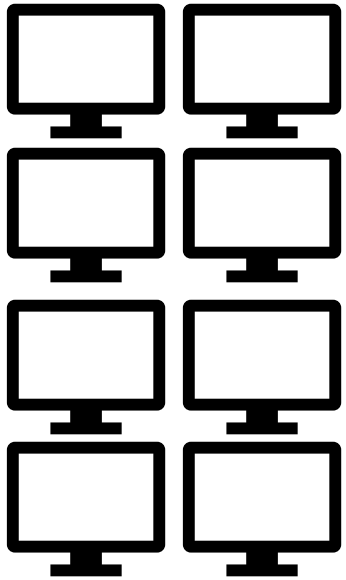
Solution: Offchain Identification

client/wallet

identity providers



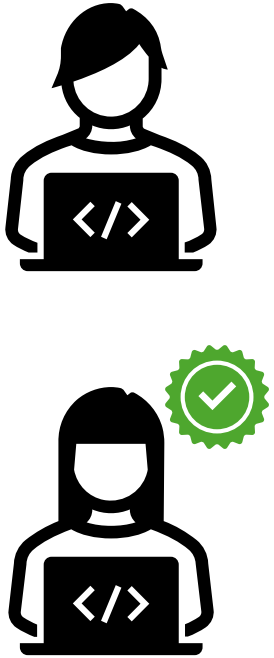
RPC endpoints



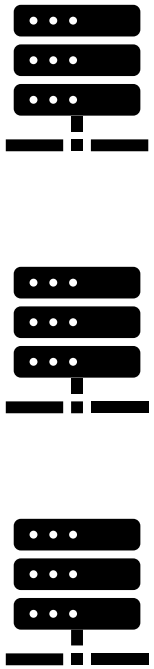
Blockchain network

Solution: Offchain Identification

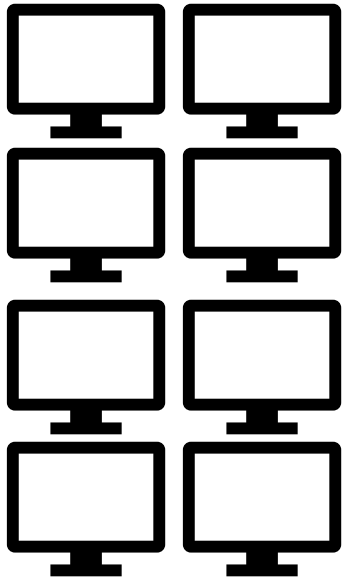
client/wallet



identity providers

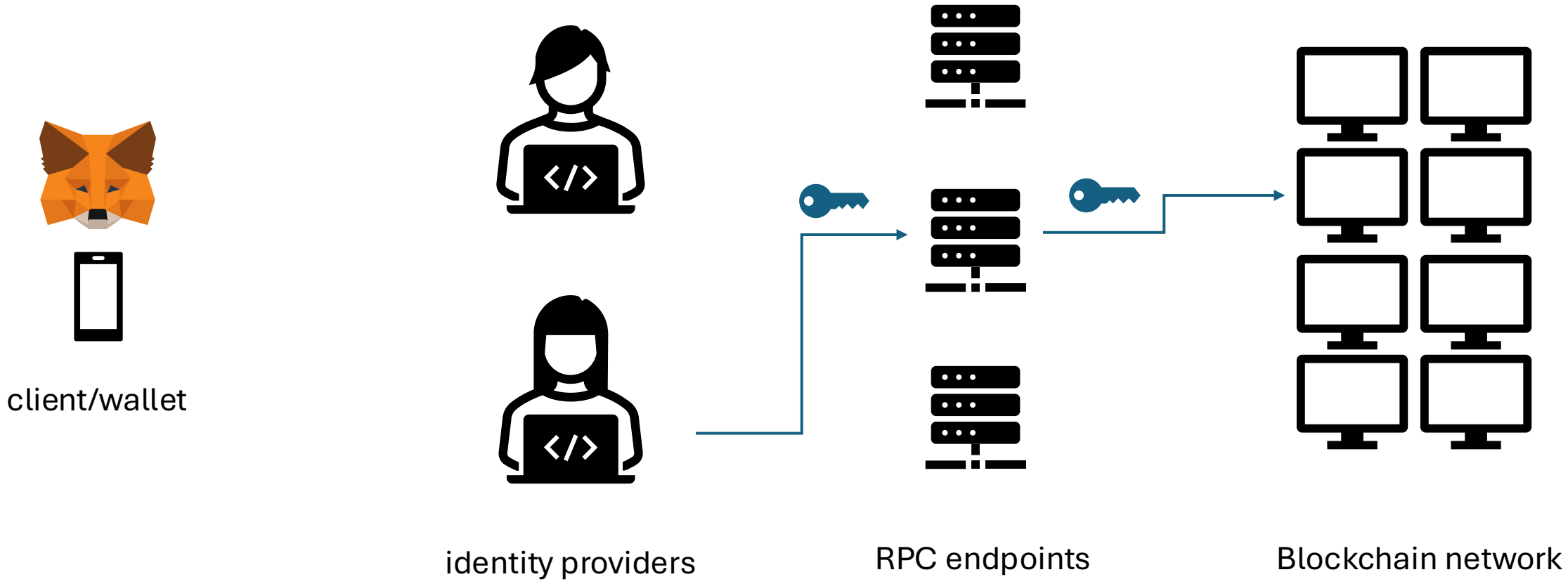


RPC endpoints

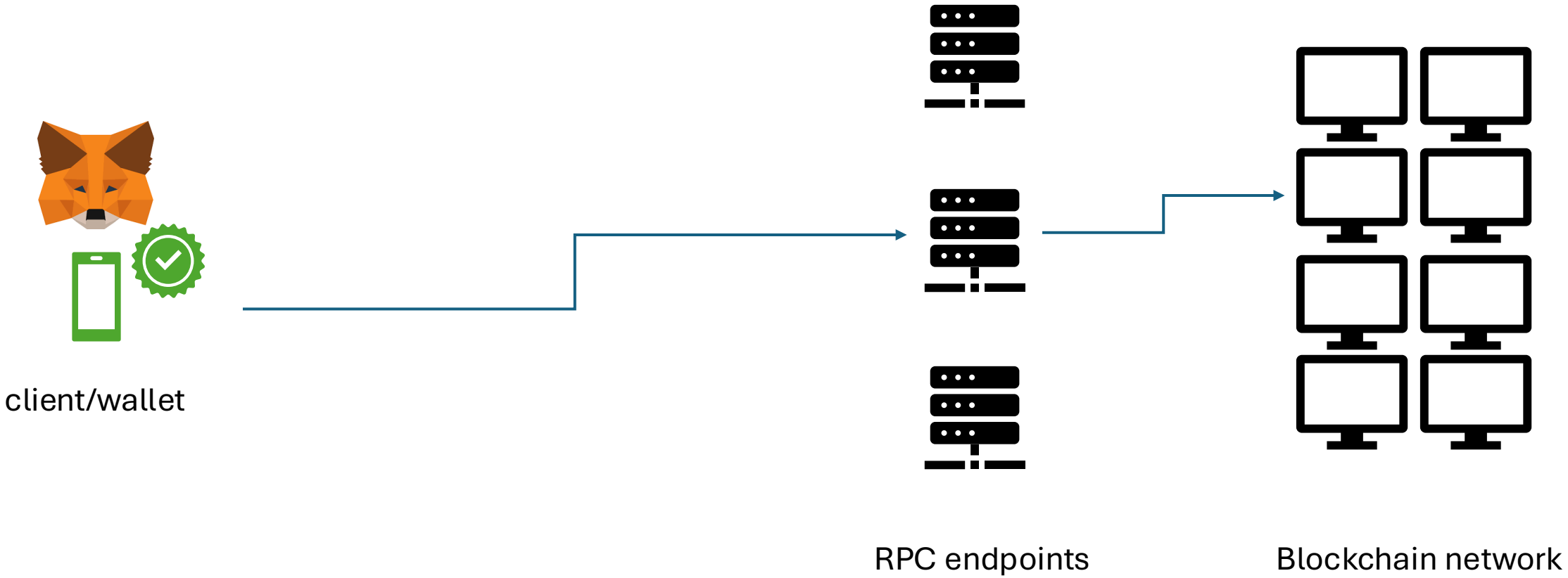


Blockchain network

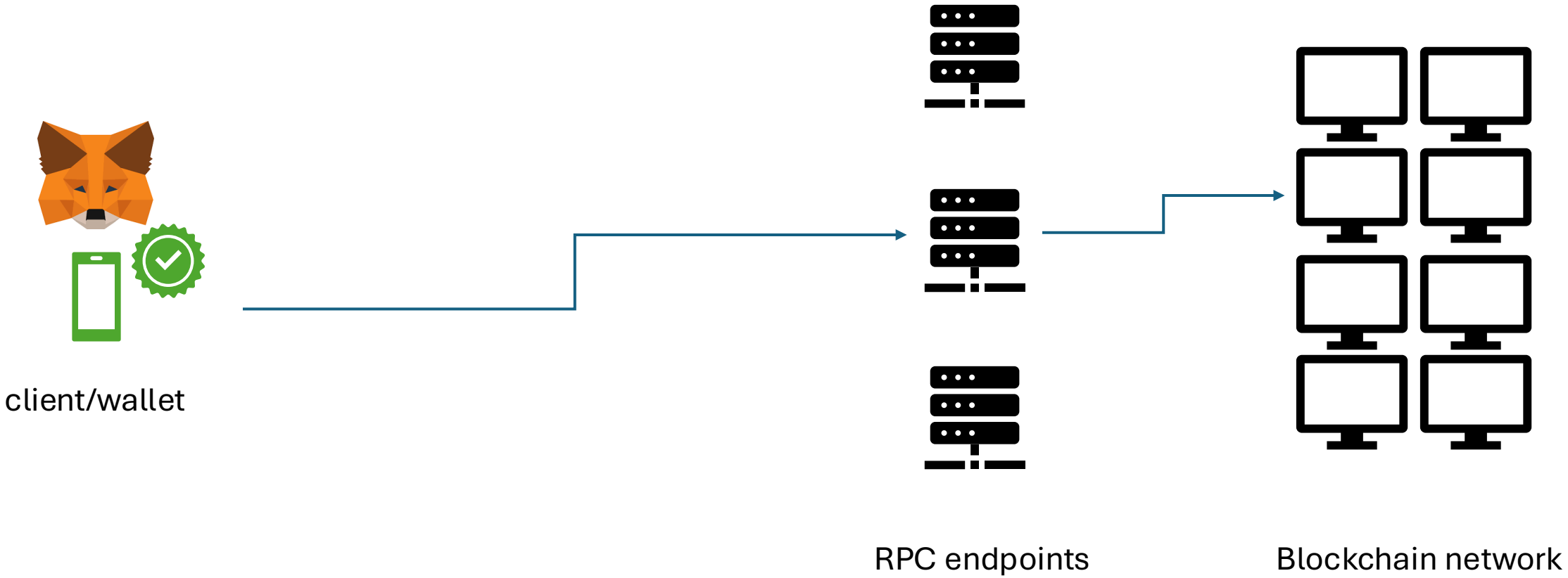
Solution: Offchain Identification



Solution: Offchain Identification



Solution: Offchain Identification

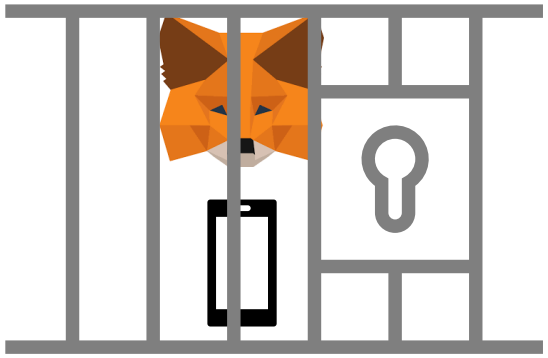


Privacy is preserved: No personal identifiable information (PII) is stored on the blockchain!

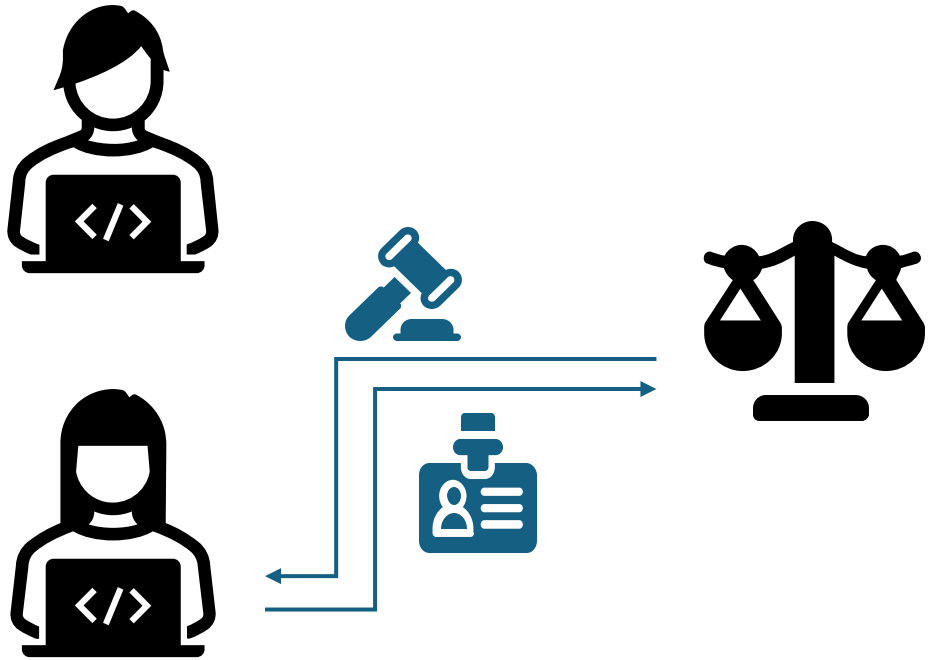
Accessing Redbelly Network

- Download wallet compatible with WalletConnect (i.e., Metamask)
- Get your identity document (i.e., passport)
- Get your phone camera to compare your photograph to your face
- Visit https://access.redbelly.network

Solution: Enforcing Accountability



client/wallet



identity providers

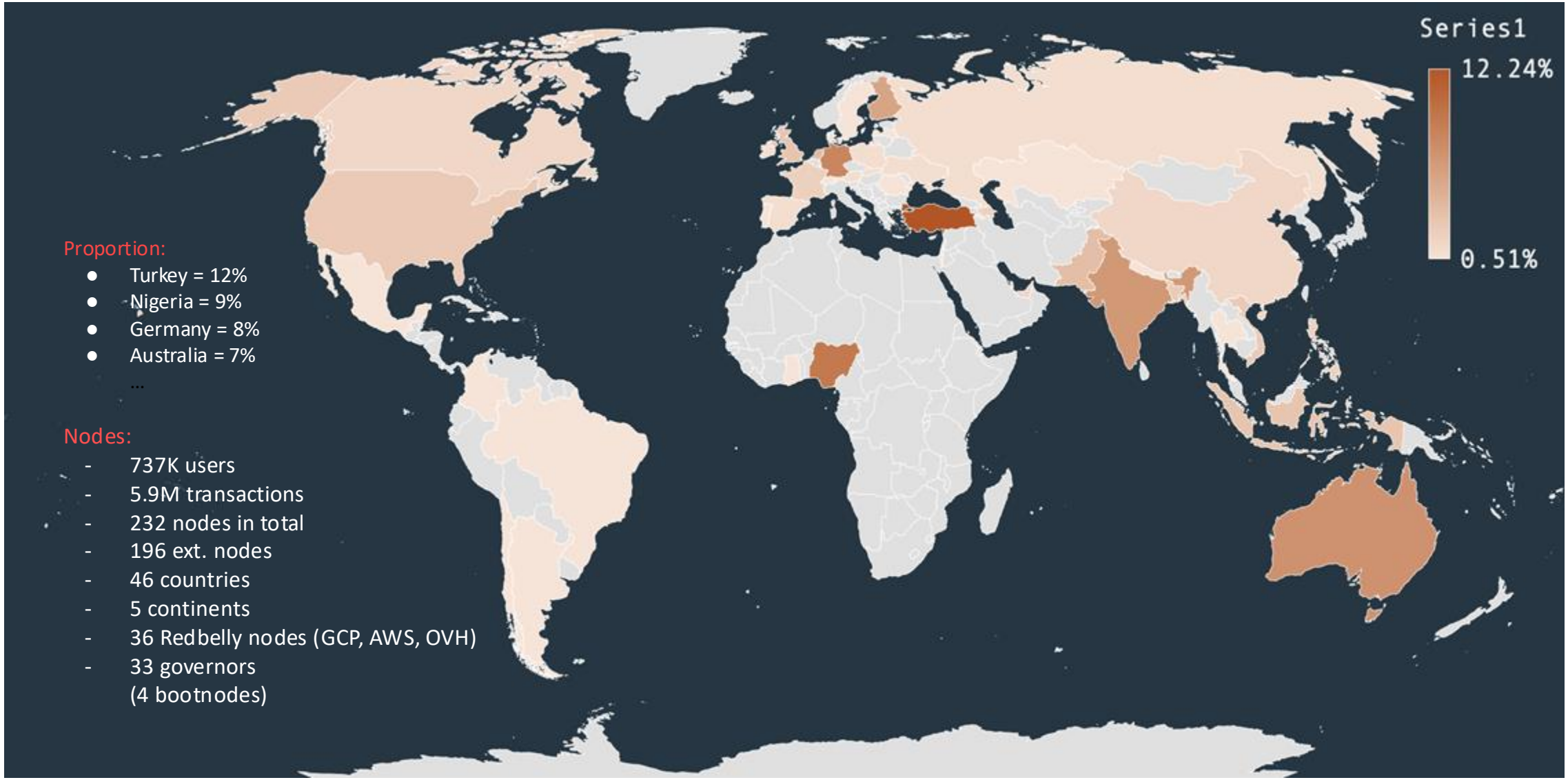
Just like in traditional finance, if a transaction is deemed illegal the authorities can ask the identity provider the identity of the culprit, but this is done outside the blockchain

Solution: Identification Outside Blockchain

- By identifying users, they become accountable
- We can restrict access to human adults and forbid AI agents
- But is Redbelly implemented and used in production?

Why these decisions proved us right

Redbelly Network in Production Today



Proportion:

- Turkey = 12%
- Nigeria = 9%
- Germany = 8%
- Australia = 7%

…

Nodes:

- 737K users
- 5.9M transactions
- 232 nodes in total
- 196 ext. nodes
- 46 countries
- 5 continents
- 36 Redbelly nodes (GCP, AWS, OVH)
- 33 governors
  (4 bootnodes)

Node Operator Program

Requirements:

8 hardware threads

16 GB memory RAM

1 TB storage space

Ubuntu 24.04.1

Signup bonus (currently):

250,000 RBNTs, including

150,000 vested over 4 years

and 100,000 RBNTs staked

Real World Assets (RWAs)

Redbelly Coin Staking Contract
RBNT Verified

Category	Staking
Price per Token	$0.015
Total Value Tokenized	$3.1M

0x43A1dc10...c5bd2817

Project of Cerrado and Amazonia ...
CH7

Category	Carbon Credits
Price per Token	$73
Total Value Tokenized	$25.2B

0xC2375752...2DB2C740

Domus Nova
DONO

Category	Real Estate
Price per Token	$110
Total Value Tokenized	$877.6K

0x3c6F30B0...3Df2e022

Buckhorn Mine
AV20 Verified

Category	Carbon Credits
Price per Token	$73
Total Value Tokenized	$28.7B

0x0DB762E2...d589A023

FeTi70
FETI70

Category	Commodities
Price per Token	$100
Total Value Tokenized	$420.0K

0xDA601f48...5c7D64A2

Hutly Shadow
SHUT Verified

Category	Equities
Price per Token	$0.629
Total Value Tokenized	$226.7M

0x93239eBE...F947Ea84

Liquidise ORD Shares
ORD Verified

Category	Company Shares
Price per Token	$2.78
Total Value Tokenized	$10.0M

0x57C9d8a5...F7C0e3DE

Joe Brown Well #5
AV21 Verified

Category	Carbon Credits
Price per Token	$72
Total Value Tokenized	$12.1M

0xDB762E27...589A023C

Joe Brown Well #9
AV22 Verified

Category	Carbon Credits
Price per Token	$72
Total Value Tokenized	$11.0M

0xDB762E27...589A023C

Source: https://redbellyassets.xyz/assets as of 10 Aug. 2025 (beta version)

Central banks tested blockchains for years

Permissionless

- Jasper 1 Ethereum
- Brazil 1 Ethereum
- Ubin 1 Ethereum

Private

- Acacia 1 Quorum
- Brazil 2 Corda vs HLF
- Jasper 2 Corda
- Stella 1 HLF
- Ubin 2 Corda vs HLF
- Khokha Quorum
- Helvetia 1 SDX
- Ensemble mBridge
- HLF HL Besu mBridge

Centralised

- Thailand 1 mBridge
- China 1 e-RMB
- Helvetia 2 SDX
- Luxembourg DL3S
- France 2 DL3S

Central bank partners with public blockchain

Permissionless

- Jasper 1 Ethereum
- Brazil 1 Ethereum
- Ubin 1 Ethereum

Private

- Acacia 1 Quorum
- Brazil 2 Corda vs HLF
- Jasper 2 Corda
- Stella 1 HLF
- Ubin 2 Corda vs HLF
- Khokha Quorum
- Helvetia 1 SDX
- Ensemble mBridge
- HLF HL Besu mBridge

Centralised

- Thailand 1 mBridge
- China 1 e-RMB
- Helvetia 2 SDX
- Luxembourg DL3S
- France 2 DL3S

Public

- Acacia Redbelly Network

Conclusion

Full privacy can be detrimental to blockchain users

Redbelly Network is the result of almost a decade of research

It was only commercialized recently

It requires its users to identify offchain to ensure accountability

It is the platform of choice for industry and government to tokenise RWA

https://x.com/VincentGramoli

Backup