Blockchain Scalability and Interoperability

Öz, B., Hoops, F., Gebele, J., & Matthes, F. (2024). “Blockchain-based Systems Engineering”. Lecture Slides. TU Munich.

Chair of Software Engineering for Business Information Systems (sebis)
Department of Computer Science
School of Computation, Information and Technology (CIT)
Technical University of Munich (TUM)
wwwmatthes.in.tum.de

Outline

1. Blockchain Scalability

2. Scaling via Rollups

3. Blockchain Interoperability

Transaction Capacity and Scalability Challenges in Blockchain Systems

Blockchain-based systems currently face significant limitations in transaction capacity when compared to traditional payment networks.

Comparison of Average Transaction Rates[1]

- **Bitcoin** 4 Tx/sec
- **Ethereum** 20 Tx/sec
- **Paypal** 193 Tx/sec
- **Visa** 1,667 Tx/sec

Traditional Payment Networks handle a high volume of transactions through centralized infrastructure, which optimizes network efficiency. This results in low and stable transaction fees.

Blockchain-based Systems are limited by decentralized network constraints, leading to lower transaction capacity. As user demand exceeds network capacity, transaction fees increase significantly, causing higher fees and longer confirmation times.

[1] Daniela Mechkaroska et al. "Analysis of the Possibilities for Improvement of Blockchain Technology.", Nov 2018.

Ethereum Transaction Fees Over the Last Eight Years

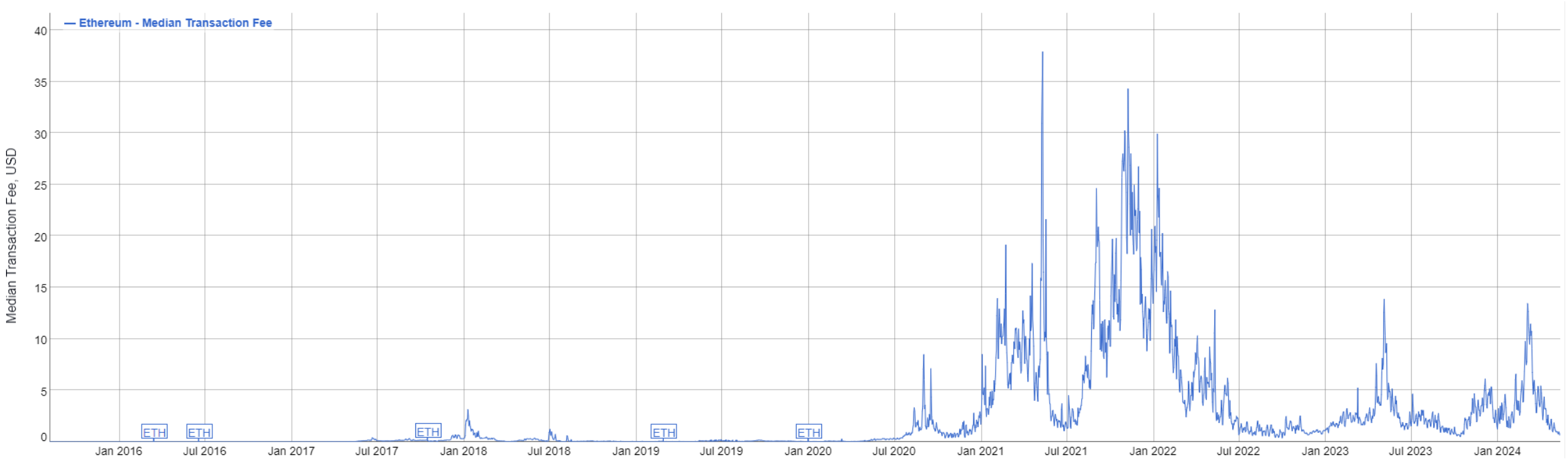


Image Source - https://bitinfocharts.com/comparison/ethereum-transactionfees.html

Factors Influencing Transaction Fees

- **Block Capacity**: Limited transaction capacity per block creates a competitive fee market.
- **Rising Network Activity**: DeFi and NFTs drive increased transactions, leading to higher fees.

May 2021: The highest median transaction fee reached $37.85. This spike was primarily due to network congestion caused by extreme price volatility in the cryptocurrency market.

Understanding the Blockchain Scalability Trilemma

Scalability Solutions aim to reduce high transaction fees and long confirmation times by increasing network capacity.

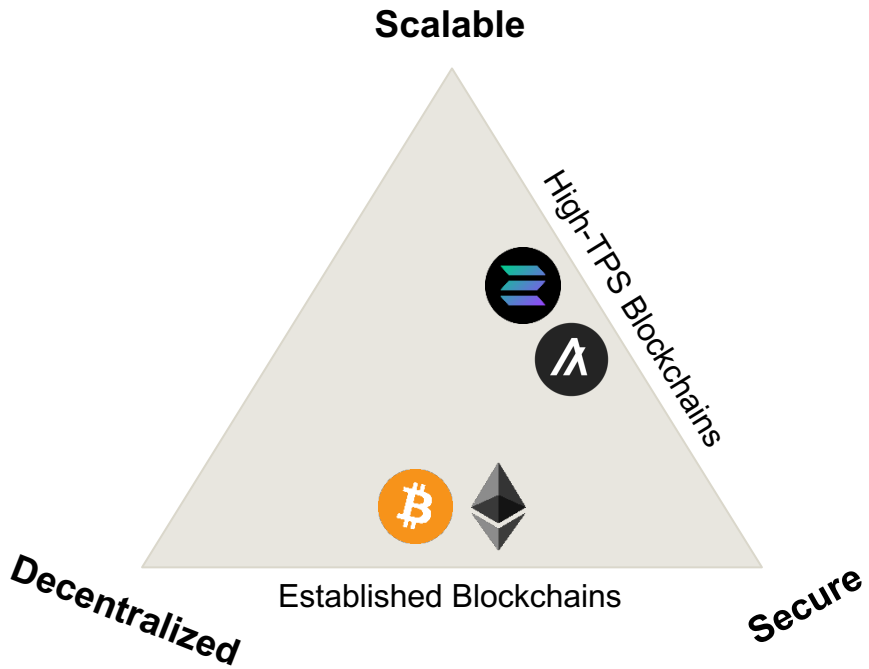
The Scalability Trilemma highlights the difficulty of enhancing blockchain performance without compromising other aspects. Achieving decentralization, security, and scalability simultaneously is challenging, with improvements in one often requiring trade-offs among the others.

Features of the Trilemma

- **Scalability**: Ability to handle increasing transactions.
- **Security**: Ensuring integrity and resistance to attacks.
- **Decentralization**: Distributing power to avoid central control.

Balancing Act

Maintaining a balance between scalability, security, and decentralization is crucial for blockchain adoption. Developers continuously seek ways to improve scalability without compromising the other two aspects.



Enhancing Blockchain Throughput with Vertical Scaling

To address increasing transaction fees in blockchain networks, vertical scaling offers a straightforward solution by tweaking core blockchain parameters.

Method: Increase block size and reduce block time.

Result: Validators process more transactions faster.

Advantages of Vertical Scaling

- Lowers transaction fees and boosts network capacity.
- Supports real-time applications like high-frequency trading and gaming.
- Makes blockchain viable for microtransactions and daily use.

Examples

Algorand and Solana can sustain high transaction speeds using advanced hardware.

- **Solana** 2390 Tx/sec[1]
- **Algorand** 2300 Tx/sec[2]

[1] https://solana.com (Mai 2024)
[2] https://algonaut.space/algorand-breaks-mainnet-tps-record

The Limits of Vertical Scaling

While vertical scaling can enhance blockchain performance, there are technical limitations.

Technical Limitations

- **Compute**: Consumer hardware has limited processing power.
- **Bandwidth**: Larger blocks could slow down nodes in regions with lower internet speeds.
- **Storage**: Bigger blocks need more disk space, making it harder for average users to run nodes.

Risk to Decentralization

Vertical scaling could centralize the network by excluding users who lack high-performance hardware.

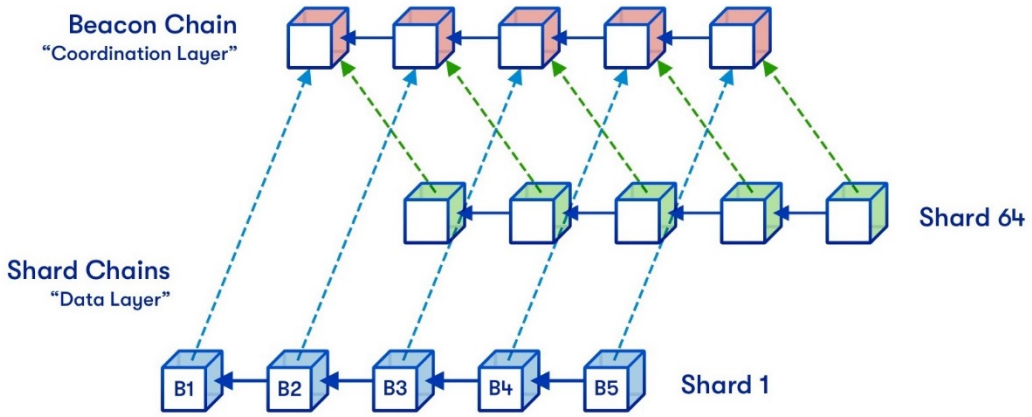
This reduces overall participation and creates a barrier to entry for joining the network.

Image Source - https://x.com/elonmusk/status/1393738154889338884

Scaling Blockchains with Sharding

Sharding is a scaling solution that increases transaction throughput without increasing demands on individual nodes.

- **Network Division**: The blockchain network is divided into smaller segments called shards.
- **Parallel Processing**: Each shard processes its own set of transactions, allowing multiple transactions to be handled simultaneously.
- **Coordination**: Shards communicate and coordinate to maintain network consistency and security.



Sharding in the Context of the Blockchain Scalability Trilemma

- **Scalability**: Shards work independently, handling many more transactions than a single node could.
- **Decentralization**: Shards can run on regular consumer hardware, avoiding the need for high-performance hardware.
- **Security**: Spreading validation across many shards makes it harder for attackers to compromise the network.

Image Source - https://vitalik.eth.limo/general/2021/04/07/sharding.html

Technical Challenges of Sharding

Blockchain Scalability Trilemma Solved?

Not Quite.

While sharding offers significant benefits, it also introduces technical complexities for developers and the blockchain architecture that the blockchain trilemma doesn't account for.

Challenges of Implementing Sharding

- **Data Consistency**: Ensuring data remains consistent across different shards.
- **Cross-Shard Communication**: Efficiently coordinating transactions between different shards.
- **Data Availability**: All necessary data is accessible and verifiable without requiring every node to download the entire data.

Polkadot is one example of a blockchain that has successfully implemented sharding to enhance scalability.

For more detailed information on sharding, consider exploring these resources:

- https://vitalik.eth.limo/general/2021/04/07/sharding.html
- https://hackmd.io/@vbuterin/sharding_proposal

Exploring Layer 2 Scaling Techniques

The idea of Layer 2 Scaling is to build on foundations of existing blockchains.

Scaling the blockchain by handling transactions off the main blockchain (Layer 1), reducing load and increasing efficiency without sacrificing security.

Payment Channels: Private pathways between two parties for off-chain transactions. The main blockchain only records the channel's opening and closing, lowering the number of on-chain transactions.

- E.g., Bitcoin Lightning Network (multiple different implementations)

Scaling via Rollups: Rollups process transactions off-chain but commit data back to the main chain for verification.

- Rollup Networks on Ethereum: Optimism[1], Arbitrum[2], zkSync[3], Base[4]

[1] https://community.optimism.io/
[2] https://docs.arbitrum.io/welcome/get-started
[3] https://docs.zksync.io/
[4] https://docs.base.org/

Outline

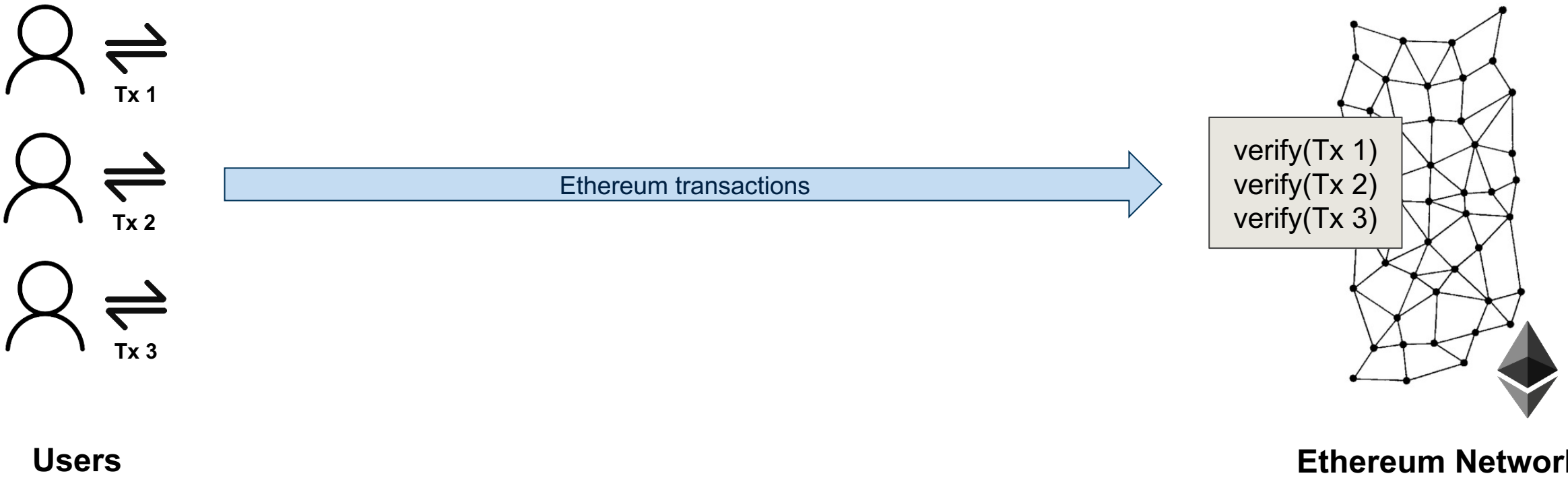
1. Blockchain Scalability

2. Scaling via Rollups

3. Blockchain Interoperability

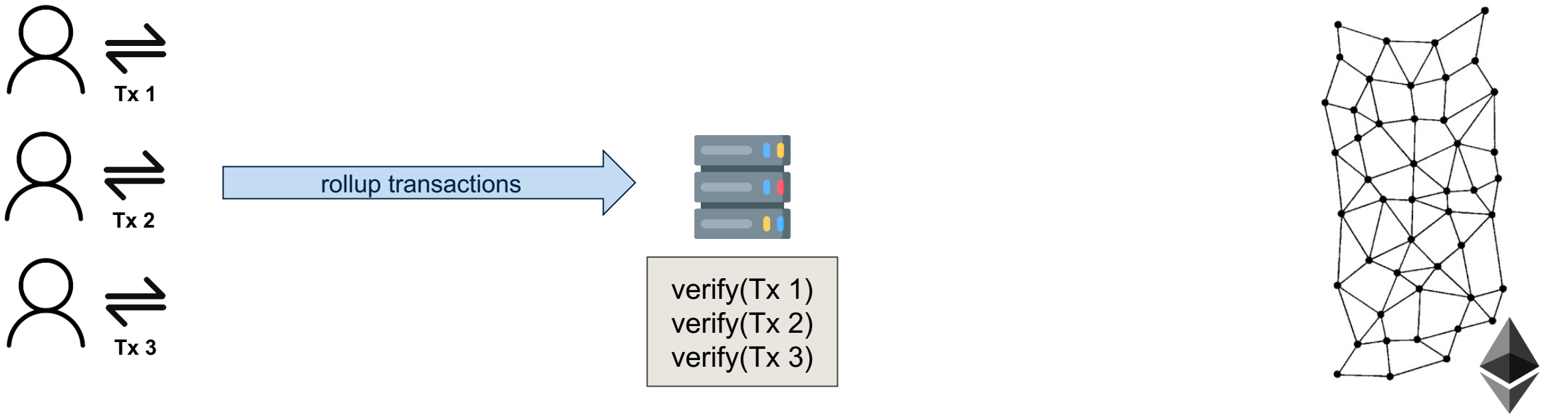
Ethereum Transaction Validation Bottleneck

- Each transaction on Ethereum must be validated by all validators.
- This slows down the network, limiting transaction throughput.



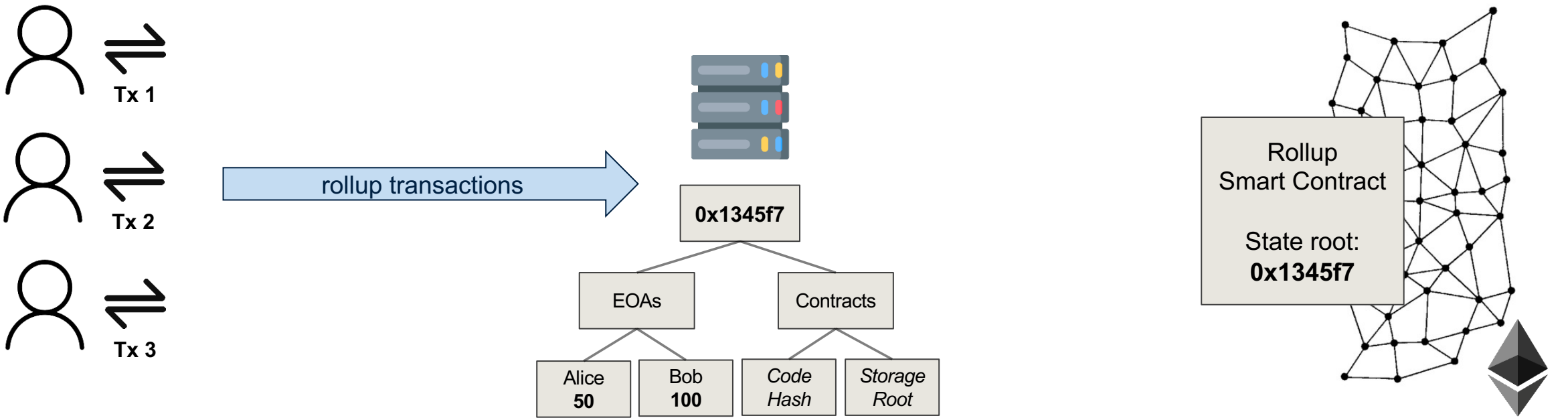
Introduction of the Rollup Coordinator

- Rollups introduce a new party, a single **off-chain coordinator**.
- Users send **rollup-transactions** to the coordinator instead of Ethereum transactions.
- The coordinator **checks the transactions for validity and attests** that all transactions are valid.



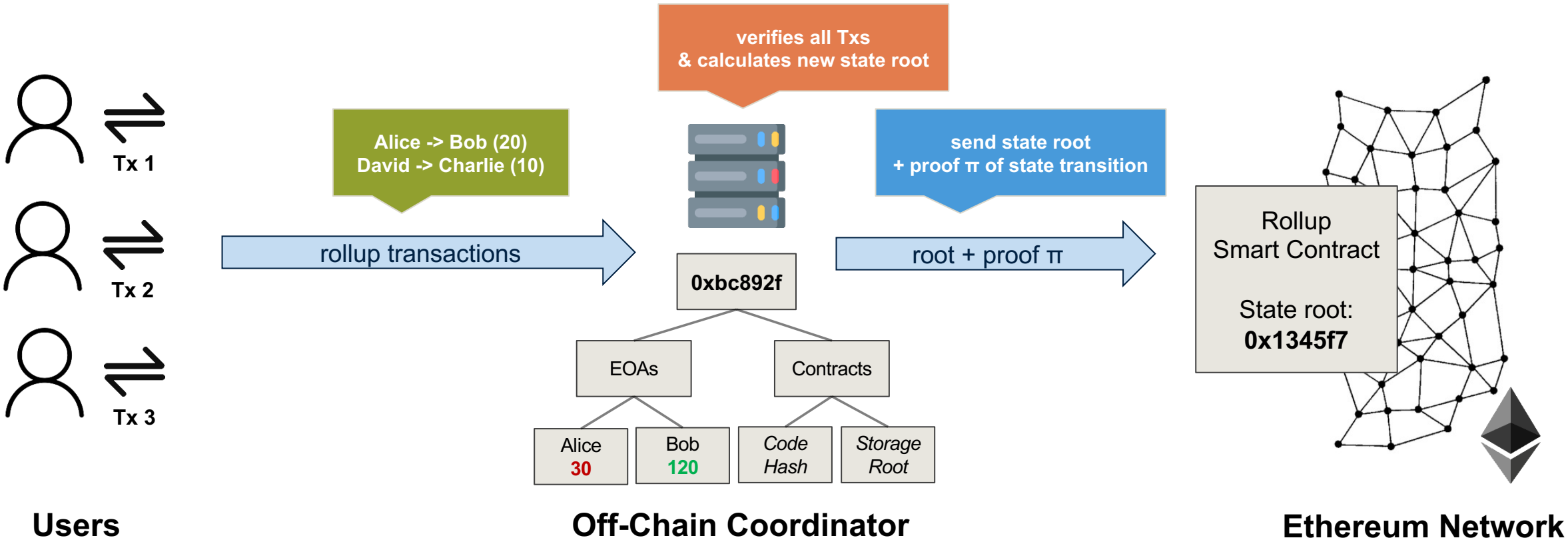
Merkle Tree Management and State Root

- The coordinator manages an independent blockchain and creates a Merkle tree of its state.
- The coordinator writes the tree's root into a smart contract on Ethereum.
  - Ensures the integrity of all off-chain transactions



Transaction Verification and Merkle Root Update

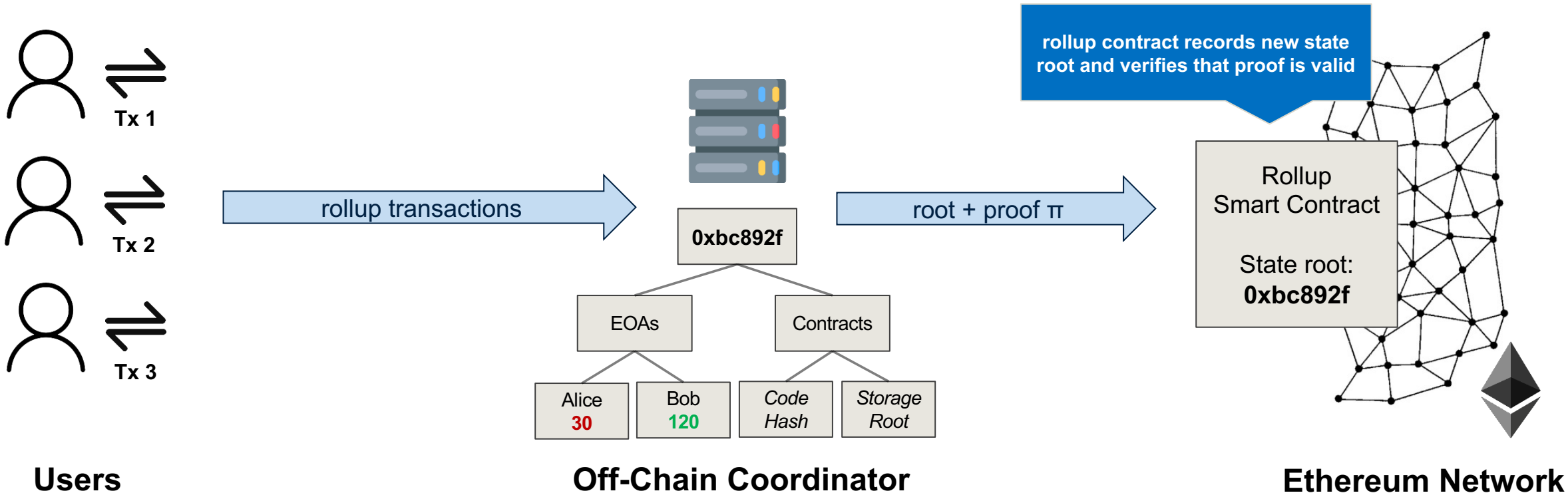
1. Users **send (rollup)-transactions** to the coordinator.
2. The coordinator **updates account balances** and **calculates a new Merkle tree root**.
3. The coordinator generates a proof of the validity of the new Merkle-tree root.
4. The coordinator **sends the new root and proof to Ethereum contract**.



Reduction of On-Chain Data Posting and Proof Verification

- The rollup coordinator updates the new state root in the rollup contract along with a proof of integrity.
- The rollup contract records the new state root and verifies that the proof is valid.

✓ The amount of data posted to the blockchain is minimal (spreading costs across multiple transactions).



Rollup Taxonomy: Optimistic vs. Zero-Knowledge Rollups

How can the rollup contract check if the state root transition proof is valid?

There are two main approaches: **Optimistic Rollups** and **Zero-Knowledge Rollups**.

Optimistic Rollups (e.g., Optimism Implementation[1])

- Transaction data sent every ~10 minutes to the rollup contract.
- Rollup assumes all transactions to be valid unless proven otherwise.
- Auditors have a challenge period of 1 week to dispute a batch by providing a fraud proof on chain.
- After the challenge period, the state root is updated on the contract.

Zero-Knowledge Rollups (e.g., zkSync Era Implementation[2])

- Proof consists of a cryptographic proof of the validity for each transaction batch.
- Proofs are stored and immediately verified on the blockchain, eliminating the need for a challenge period.
- zkSync Era mainnet already supports zero knowledge proofs for EVM compatible rollups.
- Although at this point only with a centralized coordinator.

[1] https://docs.optimism.io/stack/protocol/rollup/overview
[2] https://docs.zksync.io/build/developer-reference/zkSync.html

Rollup Taxonomy: Property Comparison

Property	Optimistic Rollup (Optimsm)	Zero Knowledge Rollup (zkSync Era)
Fixed Gas Usage per Transaction Batch	**~40,000**[2] (lightweight transaction)	**~500,000**[2] (computationally intensive verification)
Withdrawal Period	**~1-week**[1] (allows time for fraud proofs)	**Immediate** (wait for the next batch)
Contract Complexity	**Low**	**High** (complex ZK cryptography)
Off-chain computation costs	**Lower**	**Very High** (ZK proving can be very expensive)

[1] https://docs.optimism.io/stack/protocol/rollup/transaction-flow
[2] https://vitalik.eth.limo/general/2021/01/05/rollup.html

Transferring Assets to and from Rollups

Transactions Within a Rollup

- Transactions between accounts within Rollup system are natively supported by the rollup network, with batch settlement on Ethereum.

Moving Funds In and Out of Rollup

- Rollup transactions can include external inputs/outputs for deposits and withdrawals.
- To facilitate deposits and withdrawals, assets must be transferred to the rollup contract.
- More expensive due to higher transaction fees from posting additional data on Ethereum.

Transferring Funds Between Rollup Systems

- Expensive via Ethereum, cheaper via direct Rollup ⇔ Rollup Bridge (covered in Interoperability section).

Outline

1. Blockchain Scalability

2. Scaling via Rollups

3. Blockchain Interoperability

Motivation for Blockchain Interoperability

Isolation of Funds

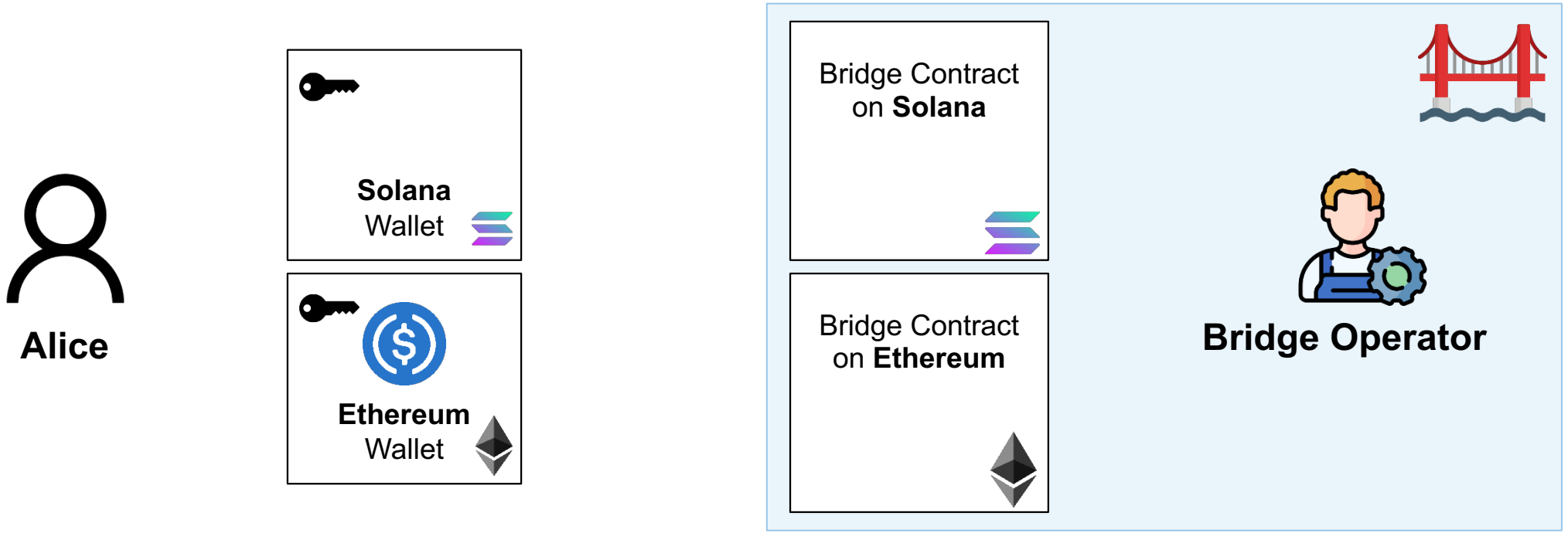
- Funds on one chain or rollup cannot be easily transferred to another, leading to isolated and less efficient blockchain projects.
- This isolation hinders the growth and full potential of decentralized networks.

Blockchain Interoperability

- The ability of different blockchain networks to communicate, share data, and build on each other's features.
- Enables the seamless exchange of data and assets without intermediaries.

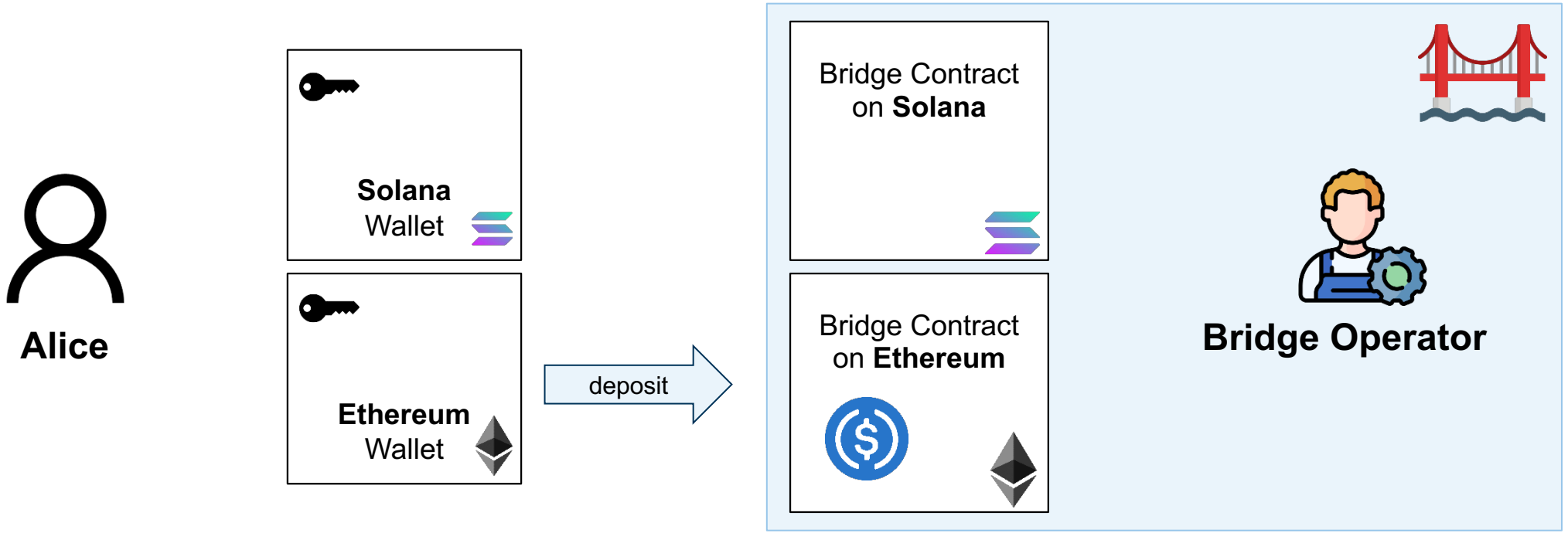
Token Bridges

- Facilitate the transfer of value between different blockchain networks.
- Enable interoperability by locking tokens on the source chain and minting equivalent tokens on the destination chain.



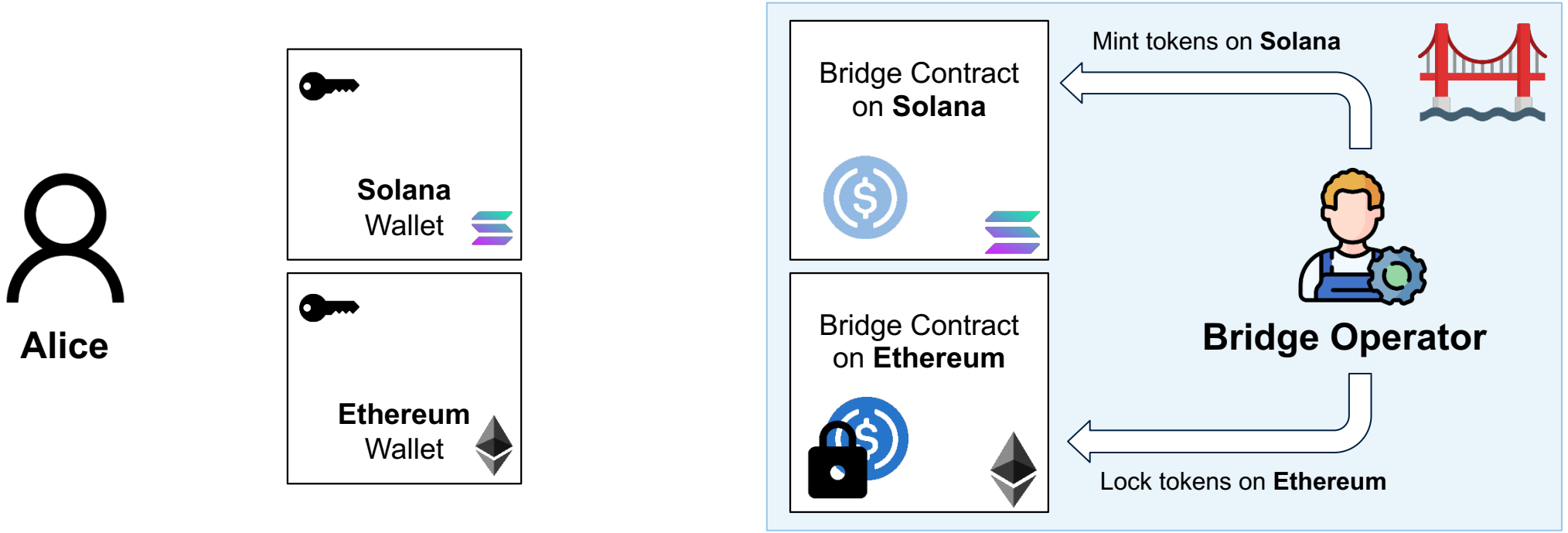
Token Bridges

- Facilitate the transfer of value between different blockchain networks.
- Enable interoperability by locking tokens on the source chain and minting equivalent tokens on the destination chain.



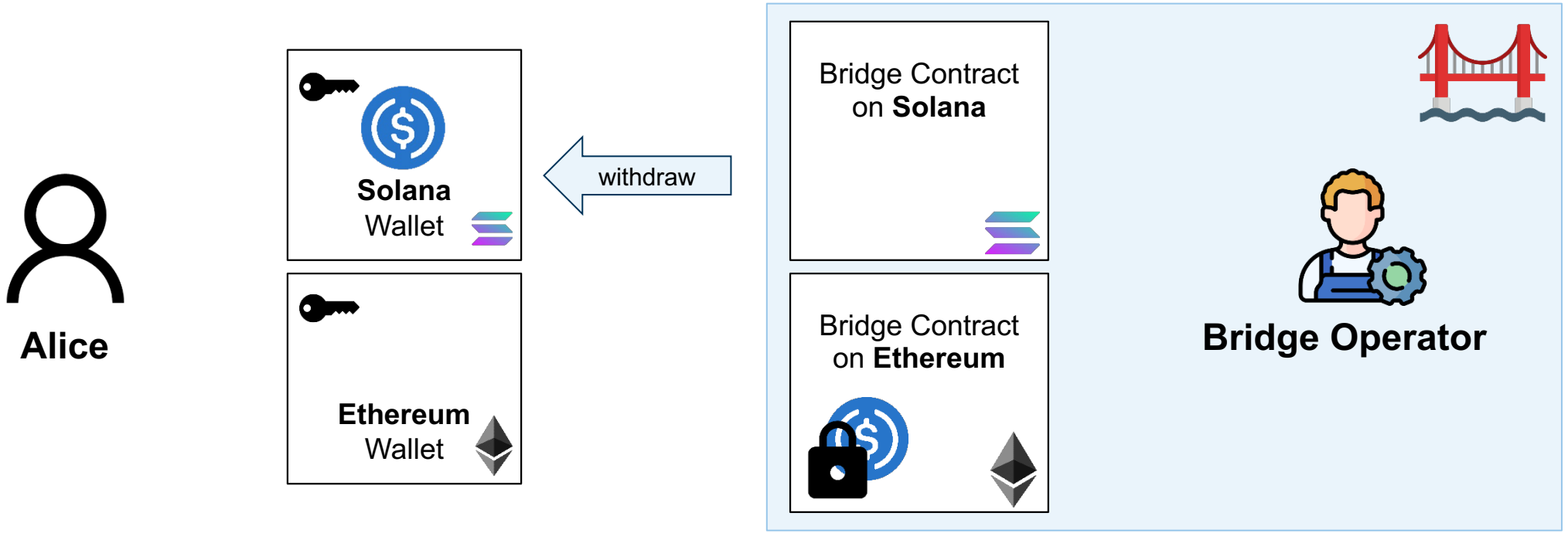
Token Bridges

- Facilitate the transfer of value between different blockchain networks.
- Enable interoperability by locking tokens on the source chain and minting equivalent tokens on the destination chain.



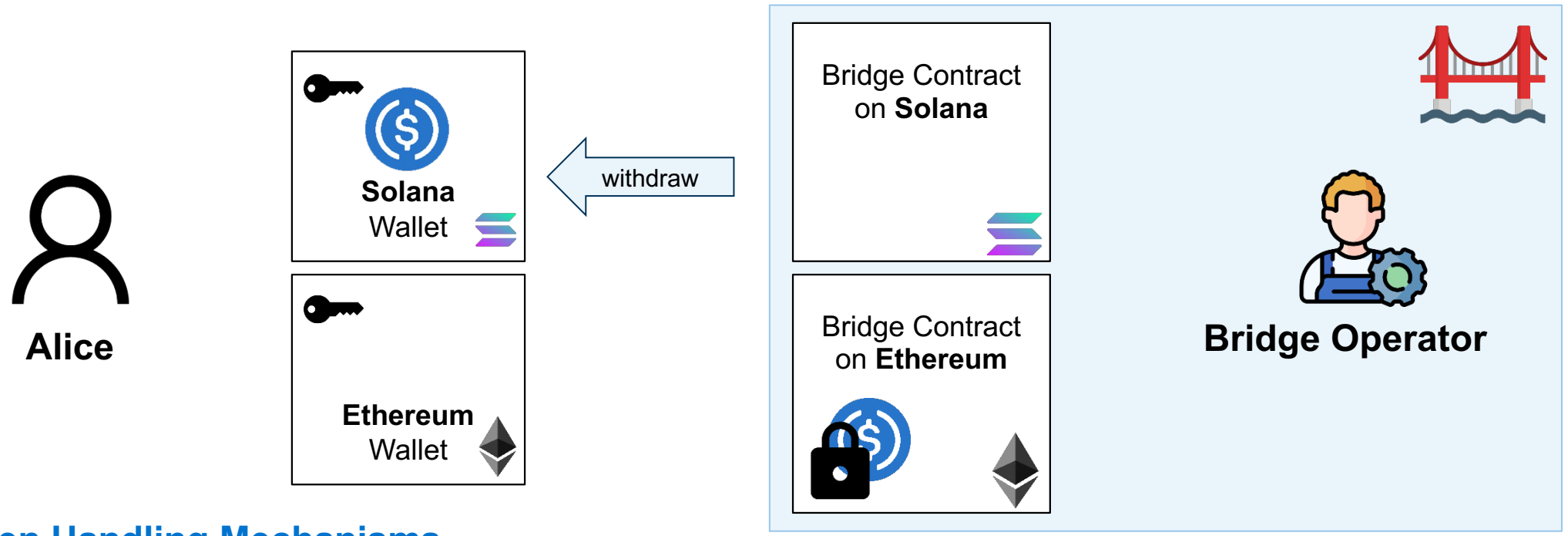
Token Bridges

- Facilitate the transfer of value between different blockchain networks.
- Enable interoperability by locking tokens on the source chain and minting equivalent tokens on the destination chain.



Token Bridges

- Facilitate the transfer of value between different blockchain networks.
- Enable interoperability by locking tokens on the source chain and minting equivalent tokens on the destination chain.



Token Handling Mechanisms

- **Lock and Mint**: Lock tokens on the source chain and mint equivalent tokens on the destination chain.
- **Burn and Mint**: Burn tokens on the source chain and mint equivalent tokens on the destination chain.
- **Lock and Release**: Lock tokens on the source chain and release tokens from a reserve on the destination chain.

Security Risks of Blockchain Bridges

Bridges can be major targets due to central points of control.
Bugs or exploits in bridge contracts can lead to significant losses.

Wormhole Bridge Hack

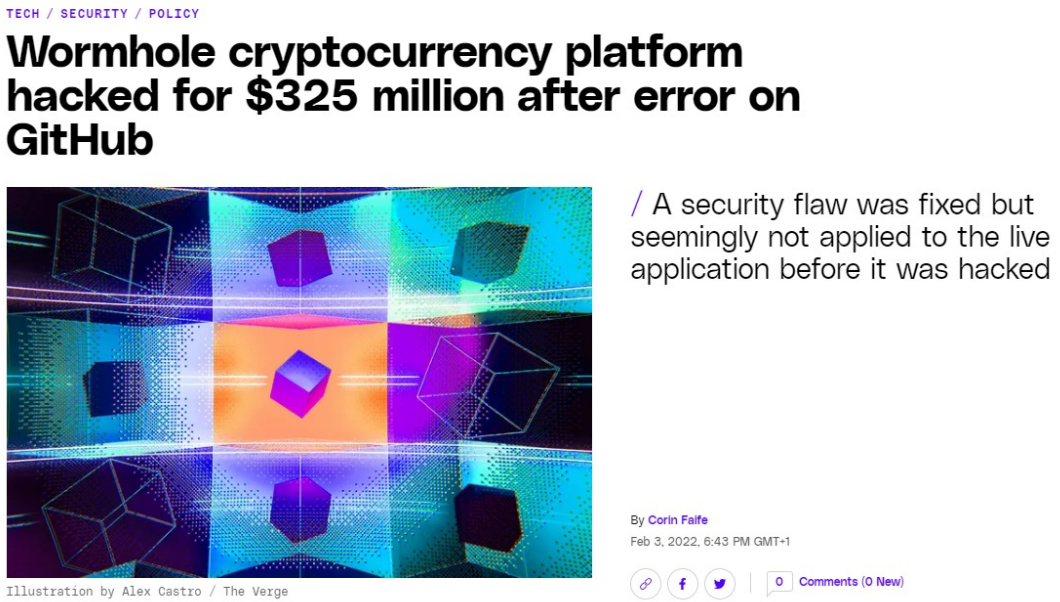
In February 2022, the Wormhole bridge was hacked for $325 million due to a security flaw.

Method

- The attacker forged a valid signature.

Impact

- Minted 120,000 wETH on the Solana blockchain.
- Exchanged it for $250 million in ETH.



TECH / SECURITY / POLICY

Wormhole cryptocurrency platform hacked for $325 million after error on GitHub

/ A security flaw was fixed but seemingly not applied to the live application before it was hacked

By Corin Faife
Feb 3, 2022, 6:43 PM GMT+1

0 Comments (0 New)

Illustration by Alex Castro / The Verge

Source - https://www.theverge.com/2022/2/3/22916111/wormhole-hack-github-error-325-million-theft-ethereum-solanal