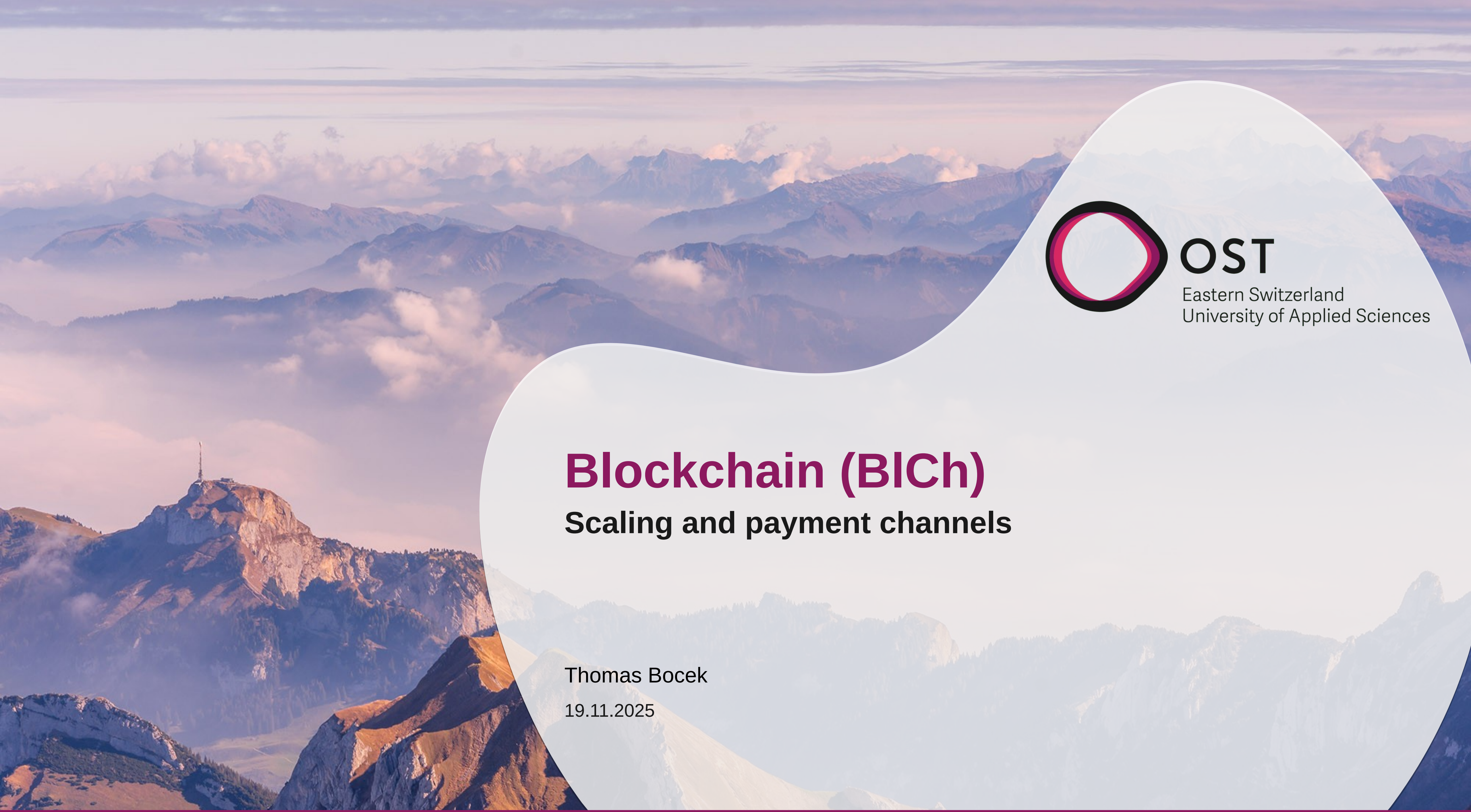


OST
Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

Scaling and payment channels

Thomas Bocek

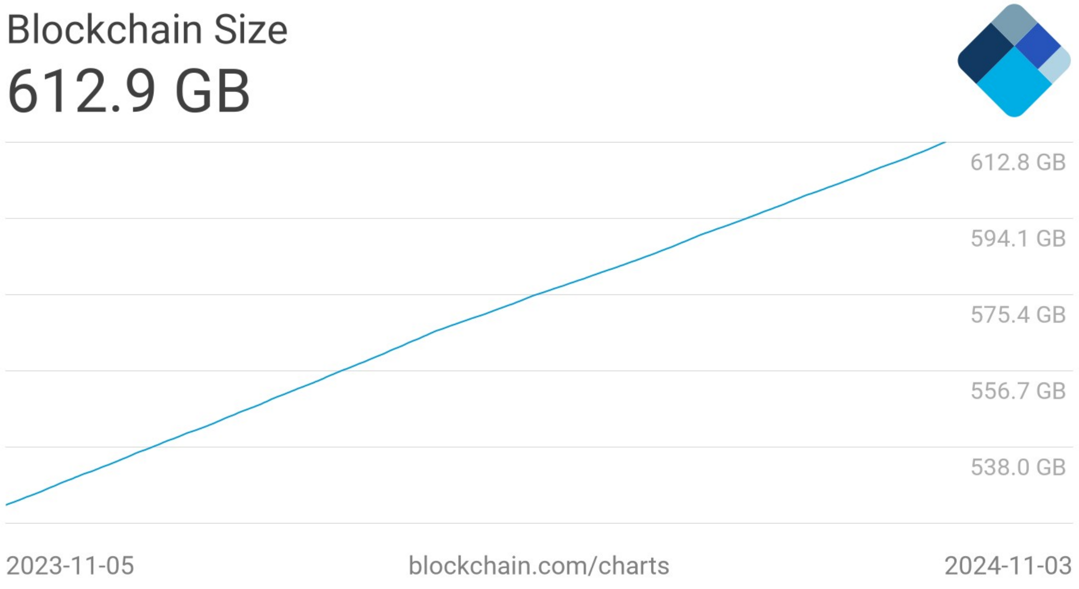
19.11.2025

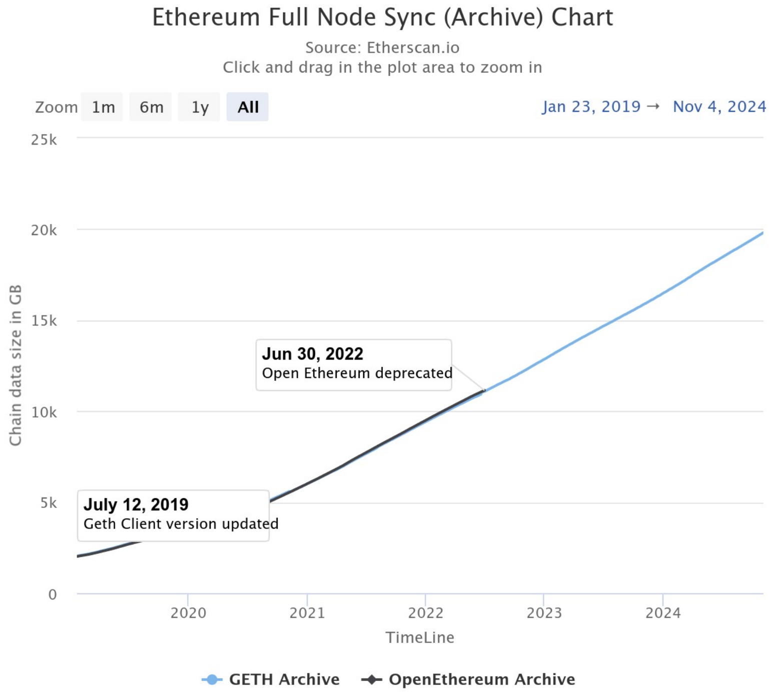
Learning Goals

- Lecture 11
  - Understand blockchain scalability challenges and evaluate different scaling approaches
  - Compare Layer 1 and Layer 2 solutions and their trade-offs in decentralization, security, and scalability
  - Explain how rollups work and the differences between Optimistic and ZK approaches
  - Understand payment channels using multisig contracts and HTLCs for atomic off-chain transactions

Scalability Solutions

- Blockchains grow linearly [ETH, ETH]
- Solutions
  - 1. First Layer Scalability Solutions (on-chain)
    - Sharding (distribute storage)
    - Improve protocol (SegWit, Taproot, Rollups)
  - 2. Second Layer Scalability Solutions (off-chain)
    - State Channels (payment channels)
      - Lightning Network
    - Sidechains / Blockchain Interoperability





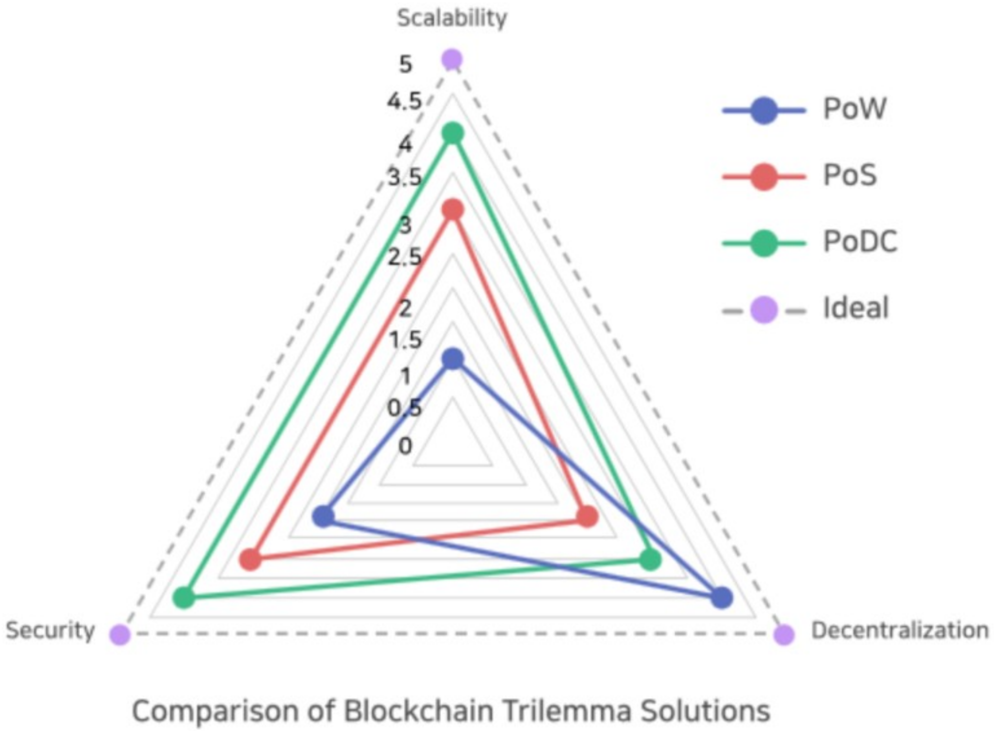
Layer 1 vs Layer 2: Basic Concepts

- Layer 1 (Base Chain)
  - Main Ethereum blockchain
  - Handles consensus, security, data availability
  - All nodes process all transactions
  - Limited by block size and time
- Layer 2 (Scaling Solutions)
  - Additional networks/protocols built on top of Ethereum
  - Inherit security from Layer 1
  - Process transactions externally
  - Post results back to mainnet

- Core Concepts
  - Additional networks/protocols built on top of Ethereum
  - Process transactions off-chain, post results to L1
  - Inherit Ethereum's security guarantees
- Key Benefits
  - 10-100x lower fees (pick one contracts - fees $10 now, random from 2024 – 308$, L2 e.g., arbiscan)
  - Increased transactions per second (TPS)
  - Trade-off: reduced decentralization vs. L1

Why Do We Need Layer 2?

- Ethereum's current limitations
  - ~10-20 transactions per second (depends how you count)
  - Average gas fees is highly variable
  - Block space competition
  - Growing demand for DeFi and NFTs
- The Blockchain Trilemma
  - Decentralization: Network participants and control
  - Security: Protection against attacks, 51% on shards
  - Scalability: Transaction throughput and costs
  - Why we can't have all three on L1



Source: https://www.halborn.com/blog/post/what-is-sharding

Main Types of Layer 2 Solutions

- Layer 2 Solutions (inherit L1 security)
  - Rollups
    - Bundle multiple transactions into one
    - Submit transaction data to Ethereum mainnet
    - Two main types:
      - Optimistic Rollups
      - Zero-Knowledge (ZK) Rollups
  - State Channels
    - Private payment channels between parties

- Not Layer 2 (separate security)
  - Sidechains
    - Independent security (separate from Ethereum)
    - Own consensus mechanism (e.g., PoS)
    - Risk: If compromised, assets can be lost
    - Protocol-level connection to parent chain
    - Regularly anchors state to L1
    - Examples: Polygon PoS

Optimistic vs. Zero-Knowledge Rollups

- Optimistic Rollups
  - Post transactions without proofs
  - Assume transactions are valid by default
  - Use fraud proofs to challenge invalid transactions
  - 7-day withdrawal period for security
  - Pros: EVM compatible, simpler technology
  - Cons: Longer withdrawal times
  - Examples: Optimism, Arbitrum

- ZK Rollups
  - ZKP: “A Zero-Knowledge Proof (ZKP) is a cryptographic method that allows one party to prove they know or possess specific information without revealing the information itself.”
  - Generate validity proofs for each batch
  - Use mathematical proofs to verify transactions
  - Immediate finality once proven
  - Pros: Faster withdrawals, more efficient
  - Cons: More complex technology, limited EVM compatibility, compute intensive
  - Examples: zkSync, StarkNet

Technical Details

- Key Components
  - Smart Contracts on L1
    - Handle deposits/withdrawals
    - Store transaction batches
    - Verify proofs
  - Off-chain Infrastructure
    - Sequencers for transaction ordering
    - Provers/Validators for verification
  - State Management
    - Maintain current state off-chain
    - Regular state roots posted to L1

- Flow

  1) User submits transaction
  2) Sequencer processes & orders
  3) Batch posted to Ethereum (~10-15 min)

- Security levels:
  - L2 confirmation from sequencer: immediate
  - L1 Batch Confirmation: ~10-15 minutes
  - Full Security: 7 days

Decentralization & Security: Sequencer and Nodes

- Sequencer malicious or down
  - Users can force-include transactions directly through L1
  - Alternative sequencers can take over
  - Worst case: delays, but funds remain safe
- Data availability
  - ALL transaction data is posted to Ethereum
  - Posted in compressed calldata ~ratio 1:10
  - Anyone can reconstruct the entire Arbitrum state, not just summaries - full transaction data
- Arbitrum node
  - Anyone can run an Arbitrum node
    - validate all transactions
    - Challengers are rewarded for finding fraud
    - Can challenge incorrect state transitions within 7 days
- ZK is resource intensive
  - ZK proof for Sui: 1-2v cores: 20-30sec
    - My Threadripper 2990WX 32-Core Processor, 2sec

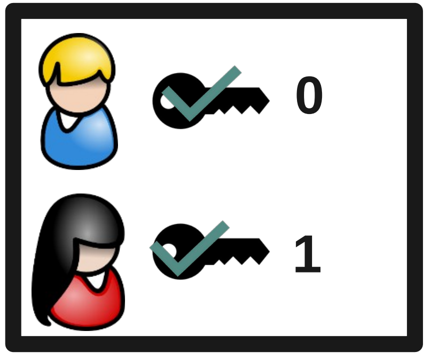
Bridges / Future of L2

- For L1 to L2: ETH on L1
  - → ETH locked in Bridge contract
  - → Message to L2 to mint WETH
  - → Auto-unwrapped to ETH on L2
- For L2 to L1: ETH on L2
  - → Initiate withdrawal
  - → Wait 7 days
  - → Claim on L1
  - → ETH released from bridge contract
- You need on both chains ETH for fees
  - Or use exchanges / fast bridges (fee vs risk)

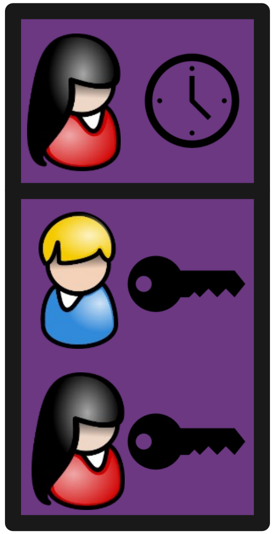
- L2 Ecosystem Growth
  - Total Value Locked (TVL) trends
  - Major DApps deploying on L2s
  - User adoption metrics
  - Cost comparisons with L1
  - L2 vs. fast L1
- Future
  - Cross-L2 communication protocols
  - Protocol standardization, Proto-Danksharding
  - Role in Ethereum's scalability roadmap

Direct Payment Channel with 2-of-2 Multisig Contracts

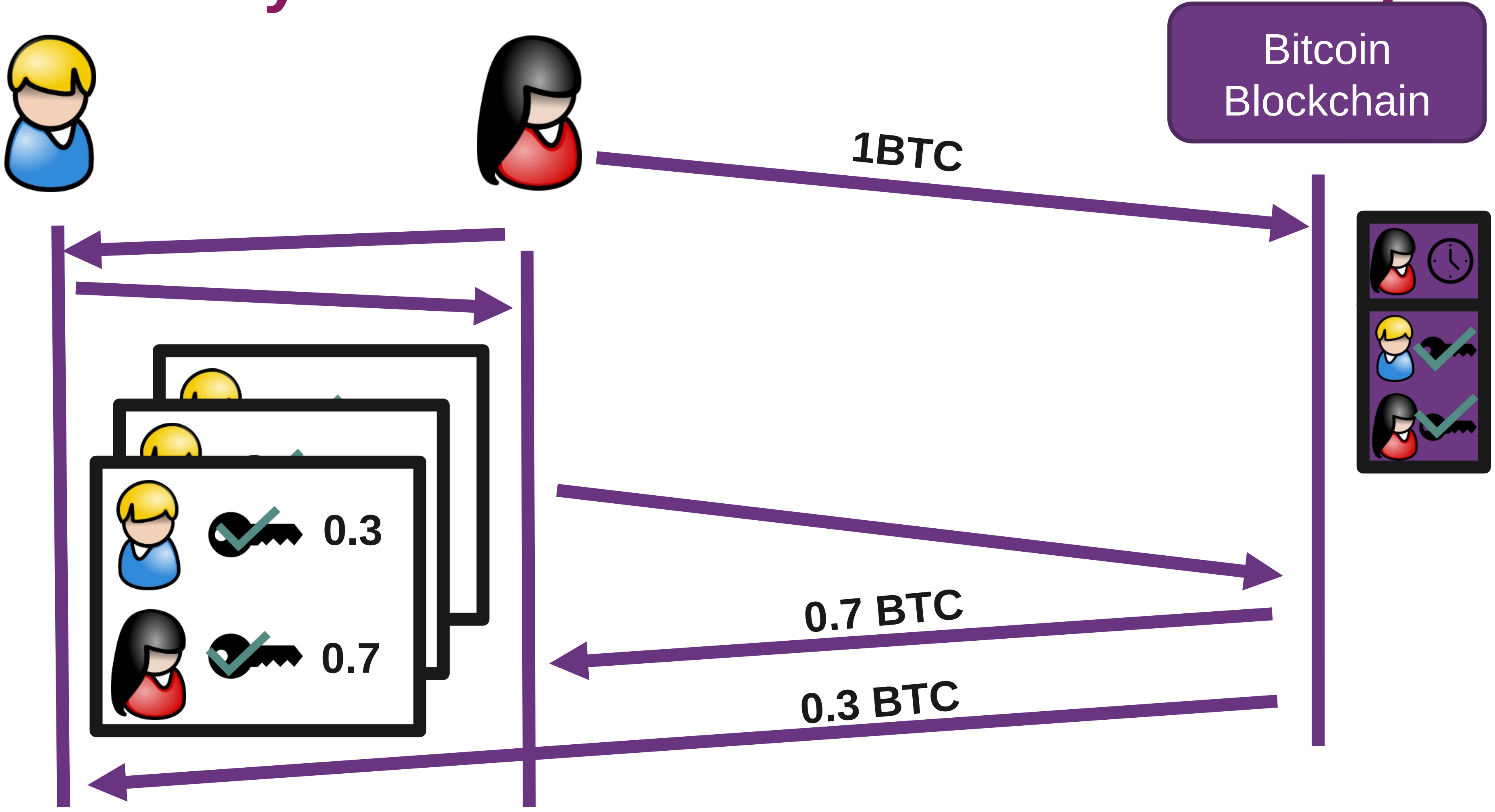
- Open a payment channel between Alice and Bob
  - 1 BTC of Alice to Locked Multisig
  - 2-of-2 multisig
    - Initial offchain TX
  - Bob does nothing



1 BTC

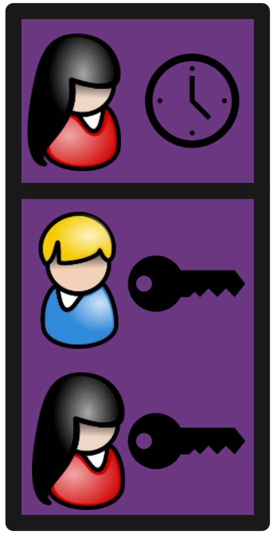


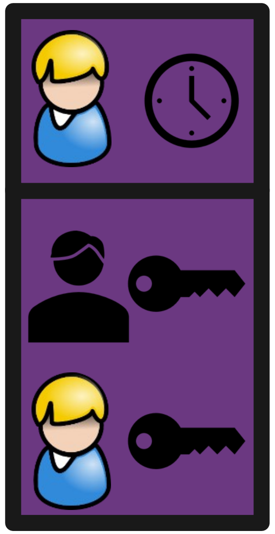
Direct Payment Channel with 2-of-2 Multisig Contracts



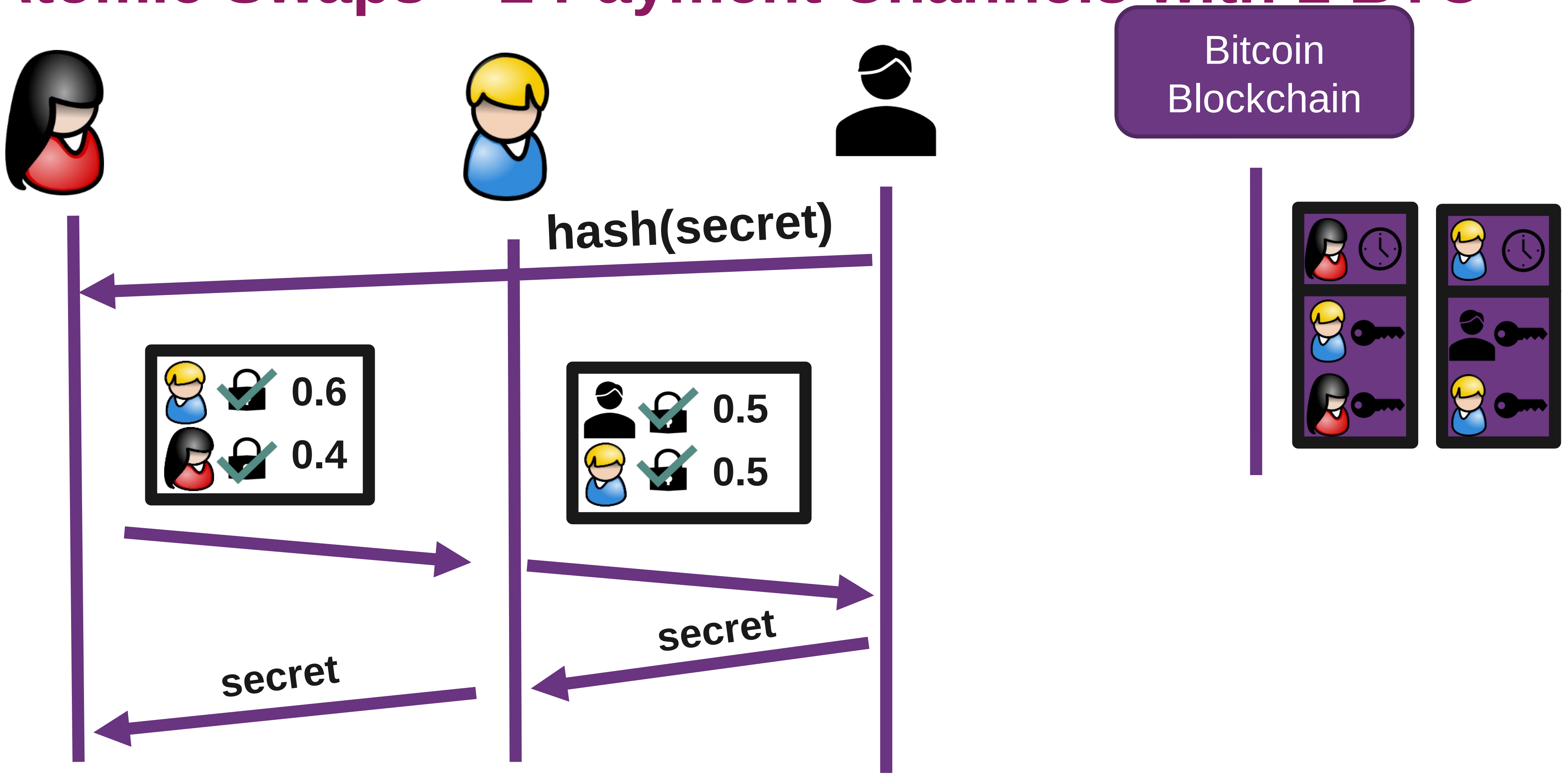
Indirect Payment Channel with HTLC

- Now we are ready to open a payment channel between Alice and Bob and Charlie
  - 1 BTC lockup, Alice – Bob, Bob – Charlie
  - Alice wants to send 0.5 BTC to Charlie (no direct channel)





Atomic Swaps – 2 Payment Channels with 1 BTC


Bitcoin Blockchain
hash(secret)
0.6
0.4
0.5
0.5
secret
secret