Concurrency and Privacy with Payment Channel Networks

Giulio Malavolta[†], **Pedro Moreno-Sanchez**[‡], Aniket Kate[‡], Matteo Maffei[*], and Srivatsan Ravi[§]

[†]Friedrich-Alexander-University
[‡]Purdue University
[*]TU Vienna

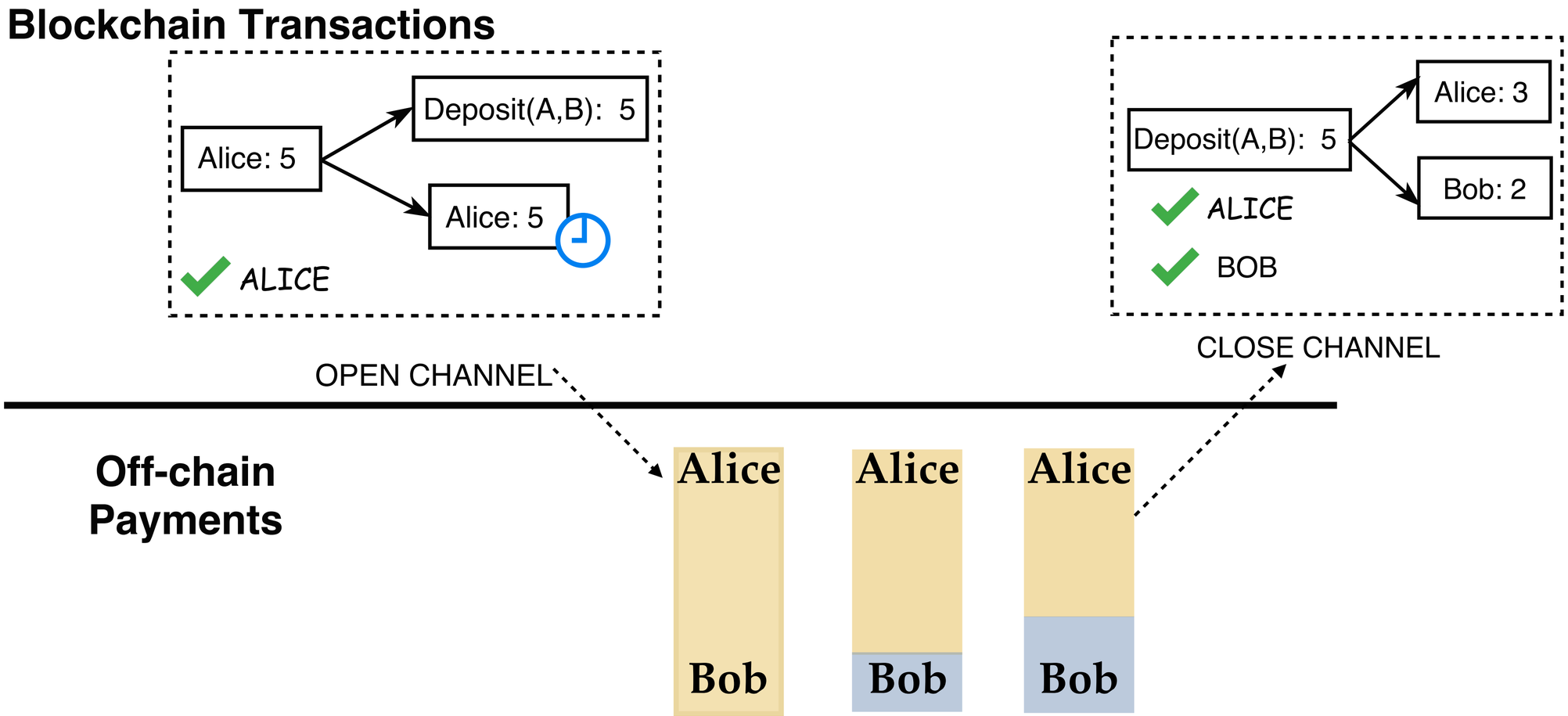
Bitcoin Scalability Issues

- < 10 transactions per second
- > 135 GB of memory required
- No micropayment (high fees)

Scalingbitcoin

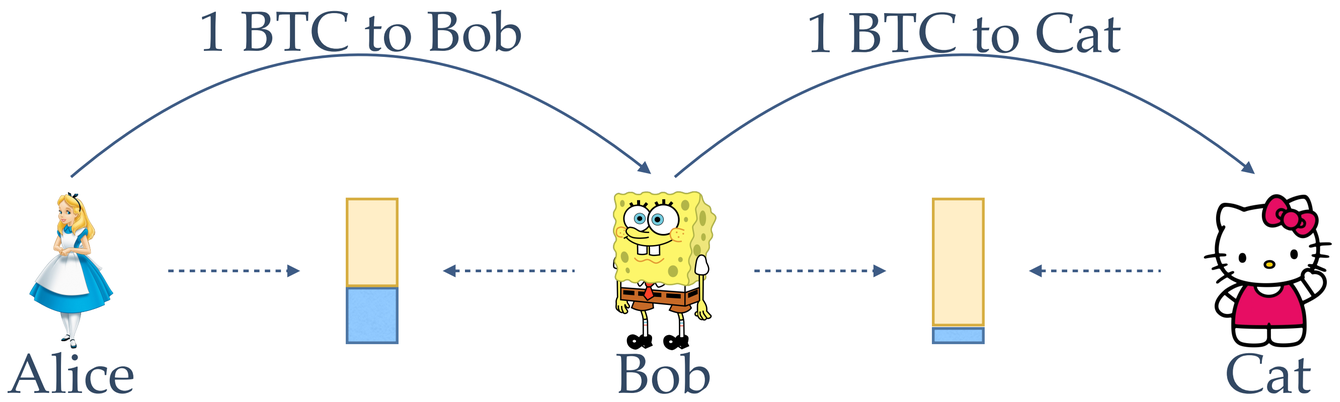
Payment Channels

- Enable multiple payments between two users without committing every single payment to the blockchain



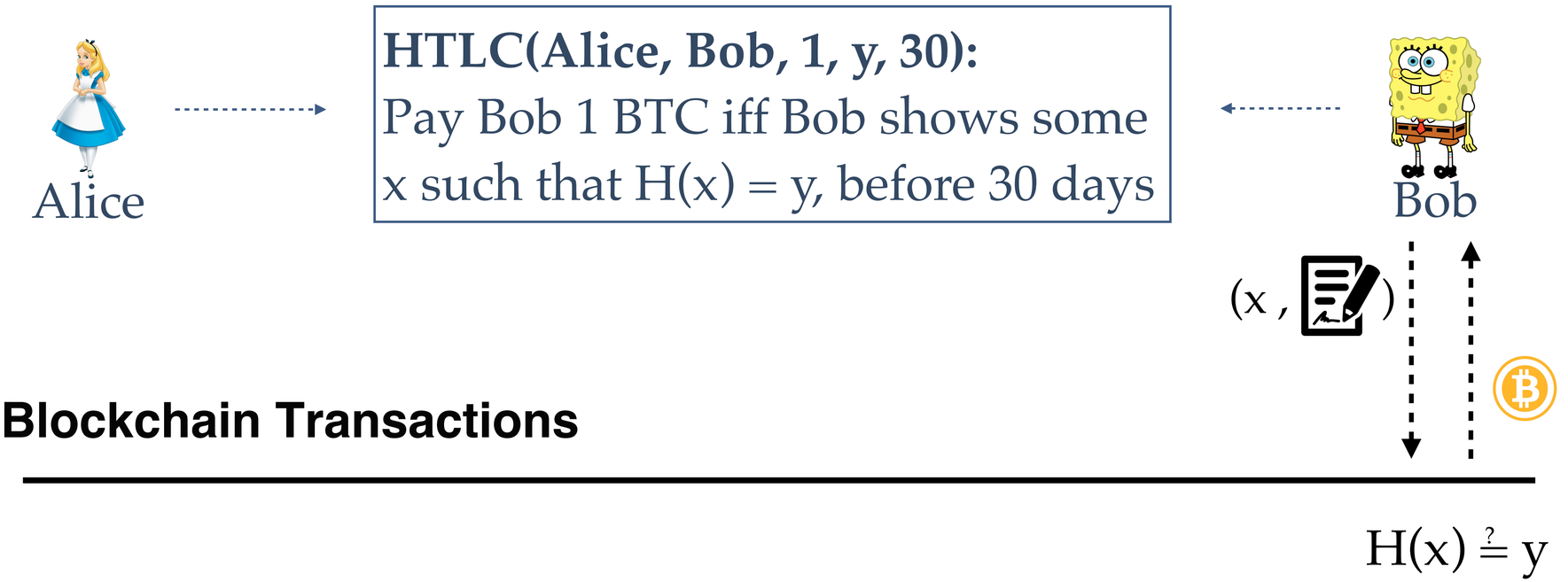
Payment Channel Networks (PCN)

- Each payment channel requires to deposit bitcoins
- Impractical to open a channel with every other user



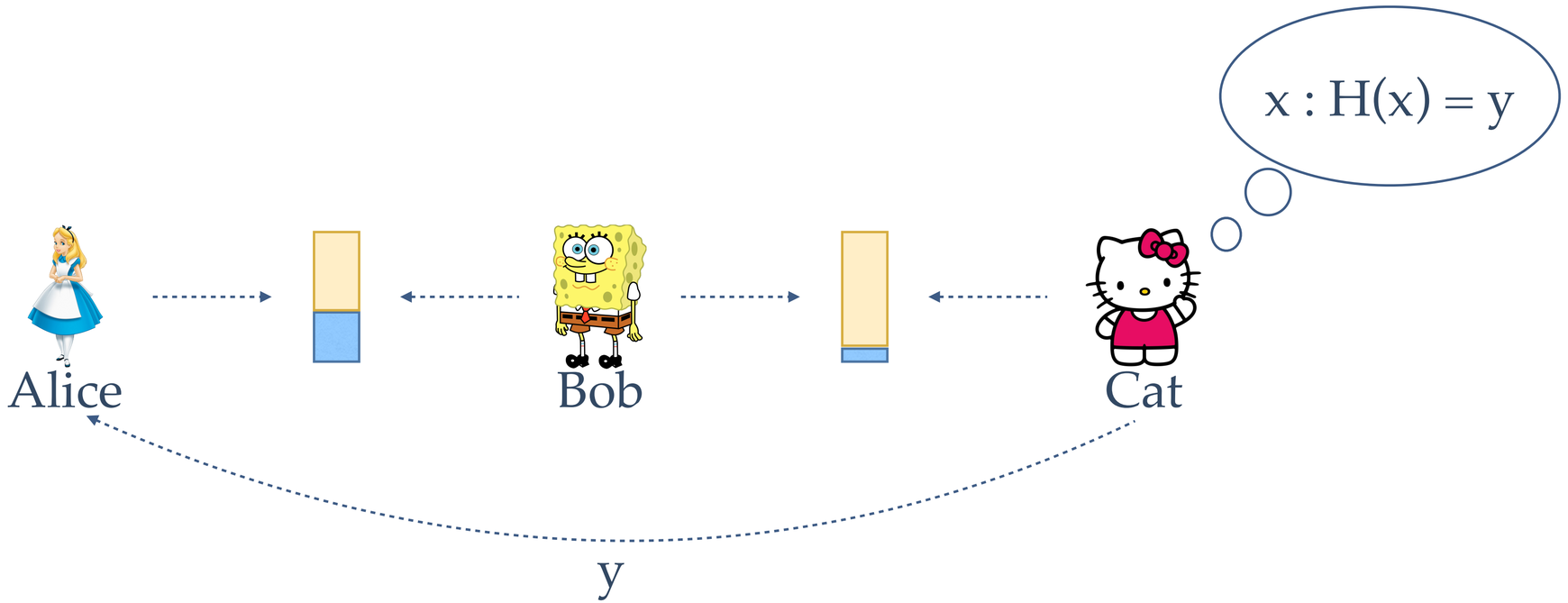
Hash Time-Lock Contracts

- Hash-Time Lock Contract (HTLC) enables conditional payments between two users



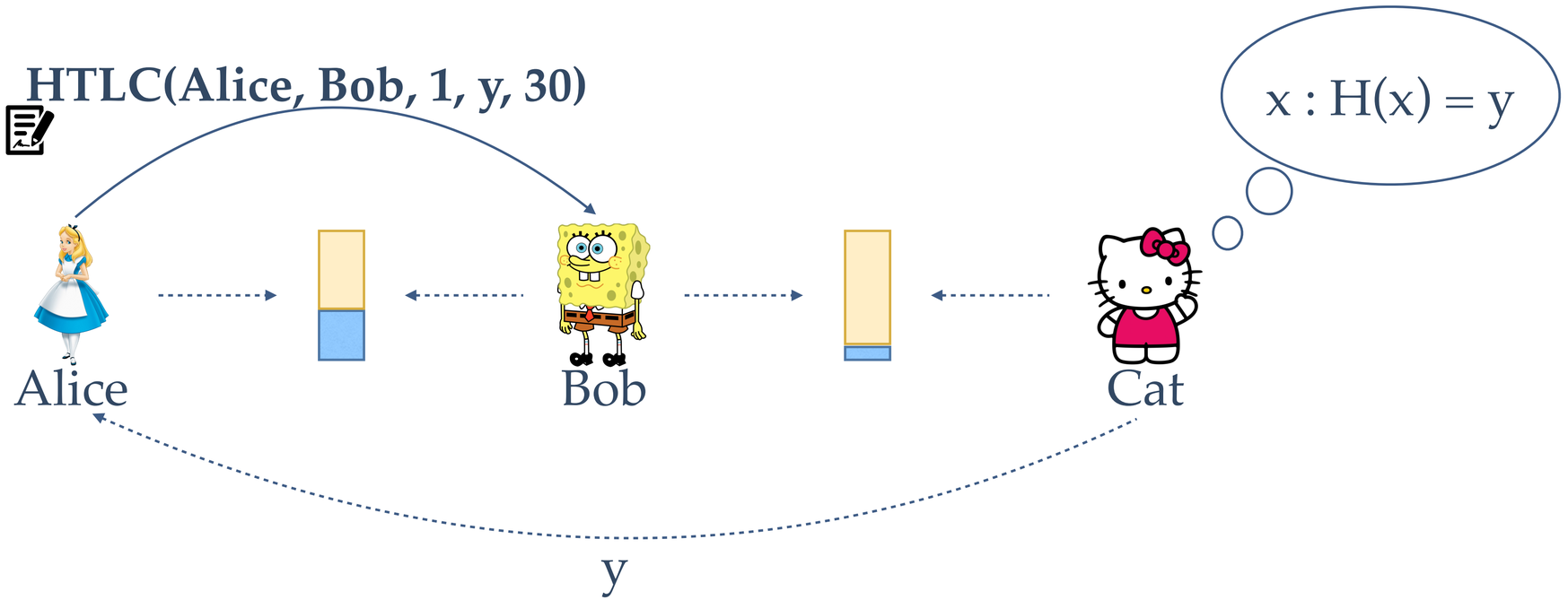
The Lightning Network

- Multiple “chained” HTLC enable multi-hop payments in the presence of untrusted intermediaries



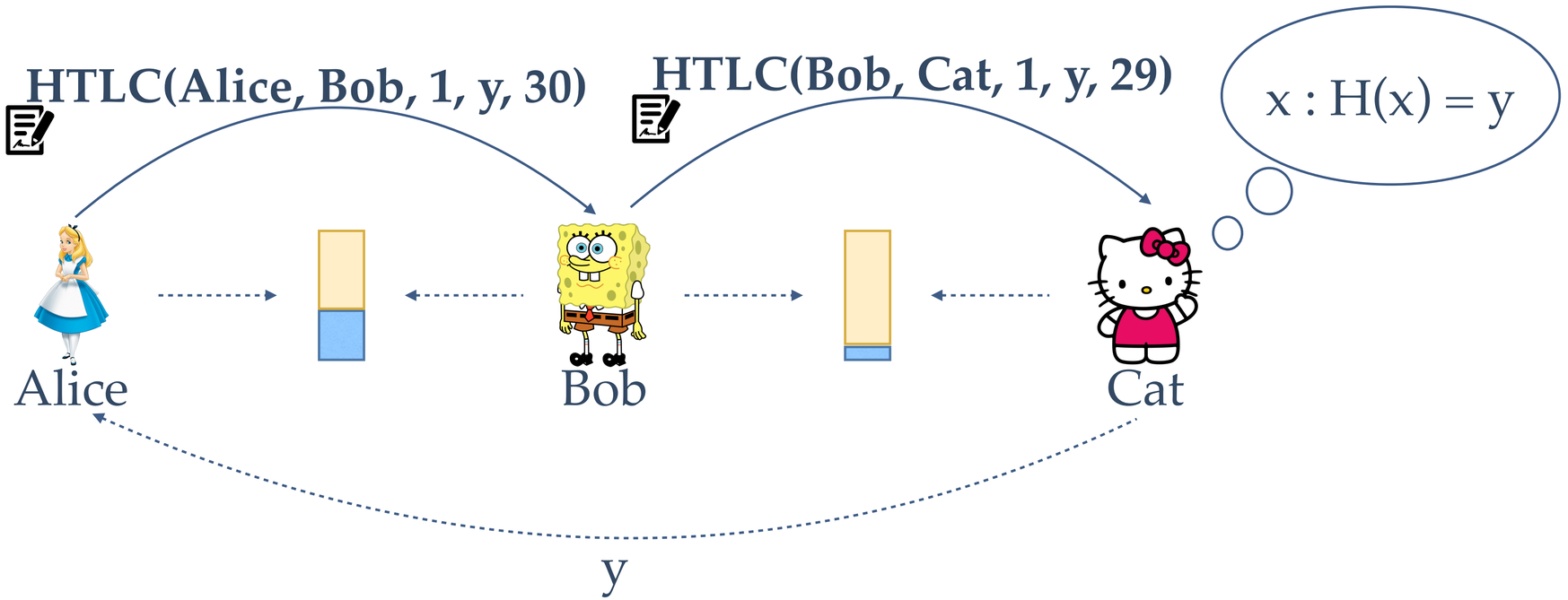
The Lightning Network

- Multiple “chained” HTLC enable multi-hop payments in the presence of untrusted intermediaries



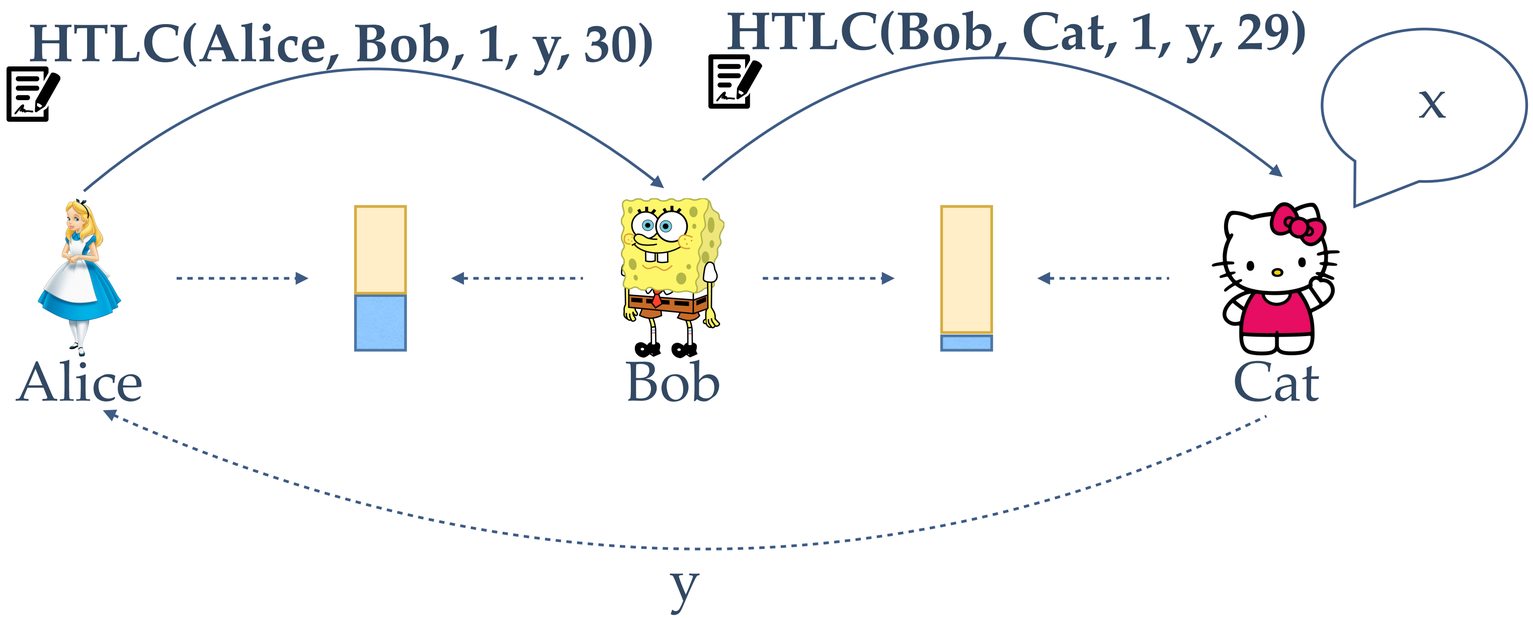
The Lightning Network

- Multiple “chained” HTLC enable multi-hop payments in the presence of untrusted intermediaries



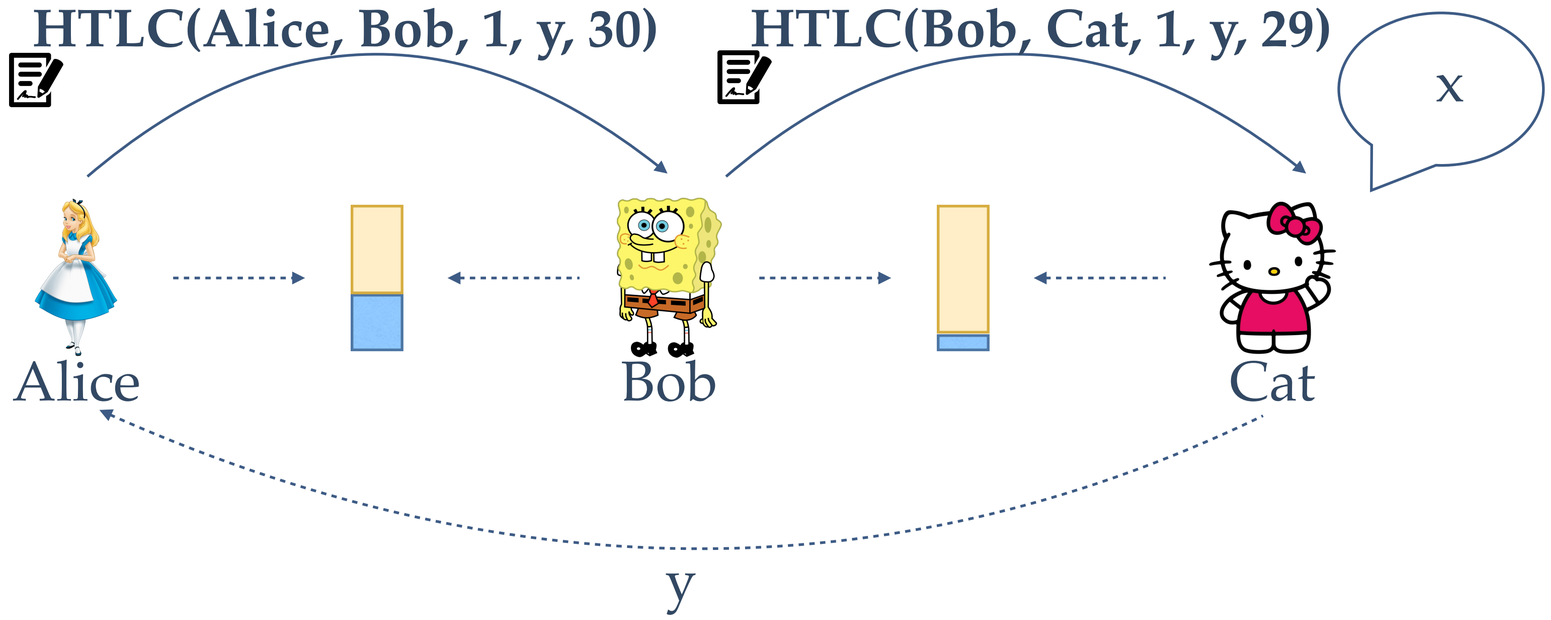
The Lightning Network

- Multiple “chained” HTLC enable multi-hop payments in the presence of untrusted intermediaries



The Lightning Network

- Multiple “chained” HTLC enables multi-hop payments in the presence of untrusted intermediaries
- Bob does not gain or lose coins



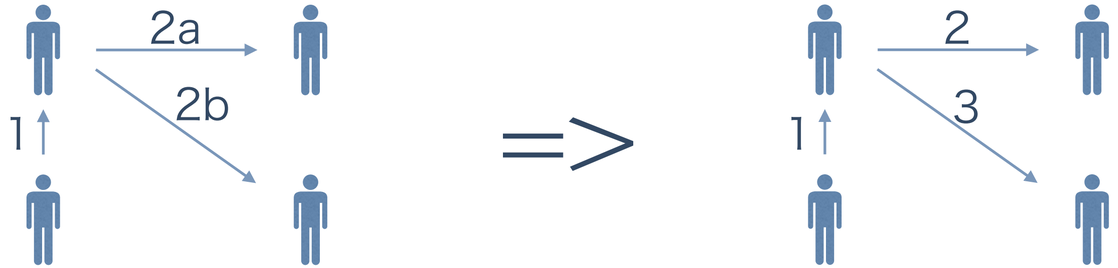
Contributions

- Definition of security and privacy properties for PCNs
- Privacy analysis of PCNs and solution (Fulgor)
- Concurrency analysis of PCNs and solution (Rayo)
- Prototype implementation

Security Properties

- Our model highlights two main security properties:
  - **Balance Security:**

  - **Serializability**:



Privacy Properties

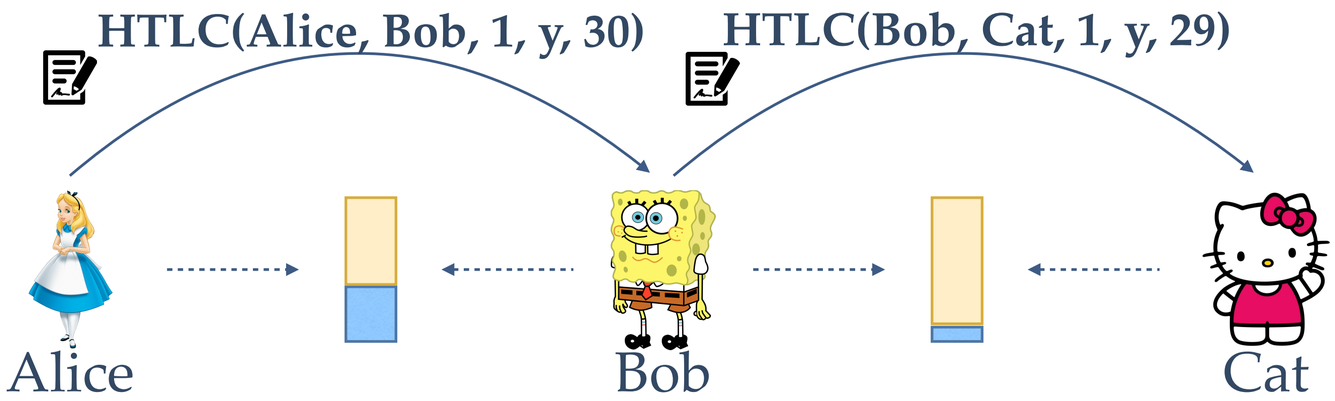
- Our model highlights two privacy properties
  - **(Off-path) value privacy:**

  - **(On-path) relationship anonymity:**

Privacy in PCNs: Challenge?

- Off-chain payments => Privacy-preserving payments

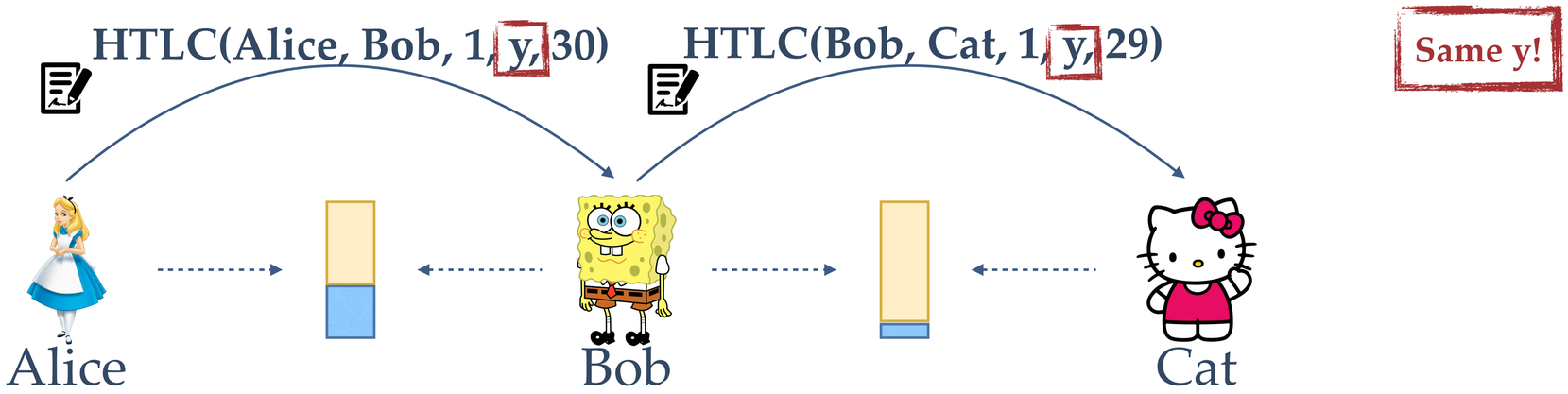
Blockchain Transactions



Privacy in PCNs: Challenge?

- Off-chain payments ⇏ Privacy-preserving payments

Blockchain Transactions

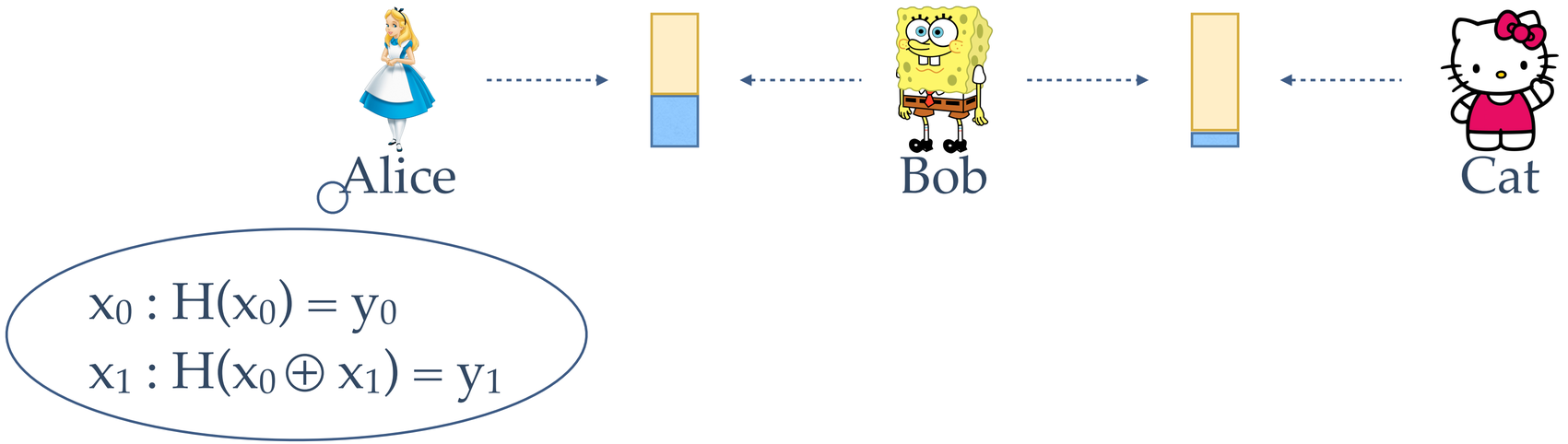


Privacy in PCNs: Our Solution

- Our setting: P2P Network
- Our goal:
  - On-chain operations: HTLC as in the Lightning Network
  - Rest of cryptographic operations must be off-chain
  - Full compatibility with the current Bitcoin script
- Our solution:
  - Fulgor: Based on Multi-hop HTLC

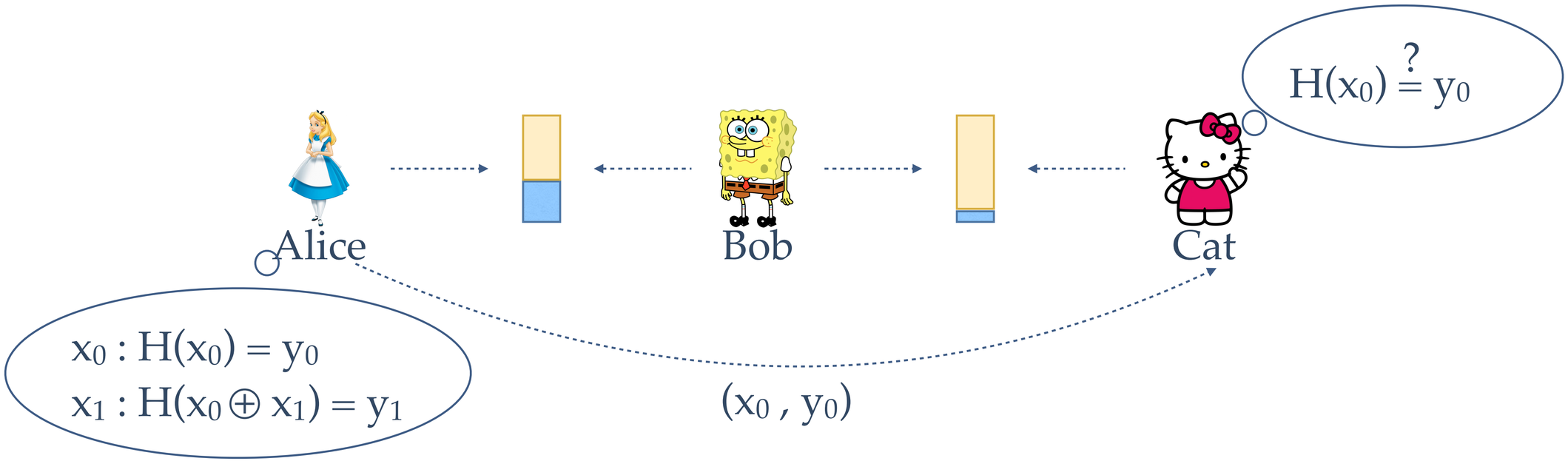
Multi-hop HTLC

- Building block: Non-interactive zero knowledge (ZKBoo [GMO16])



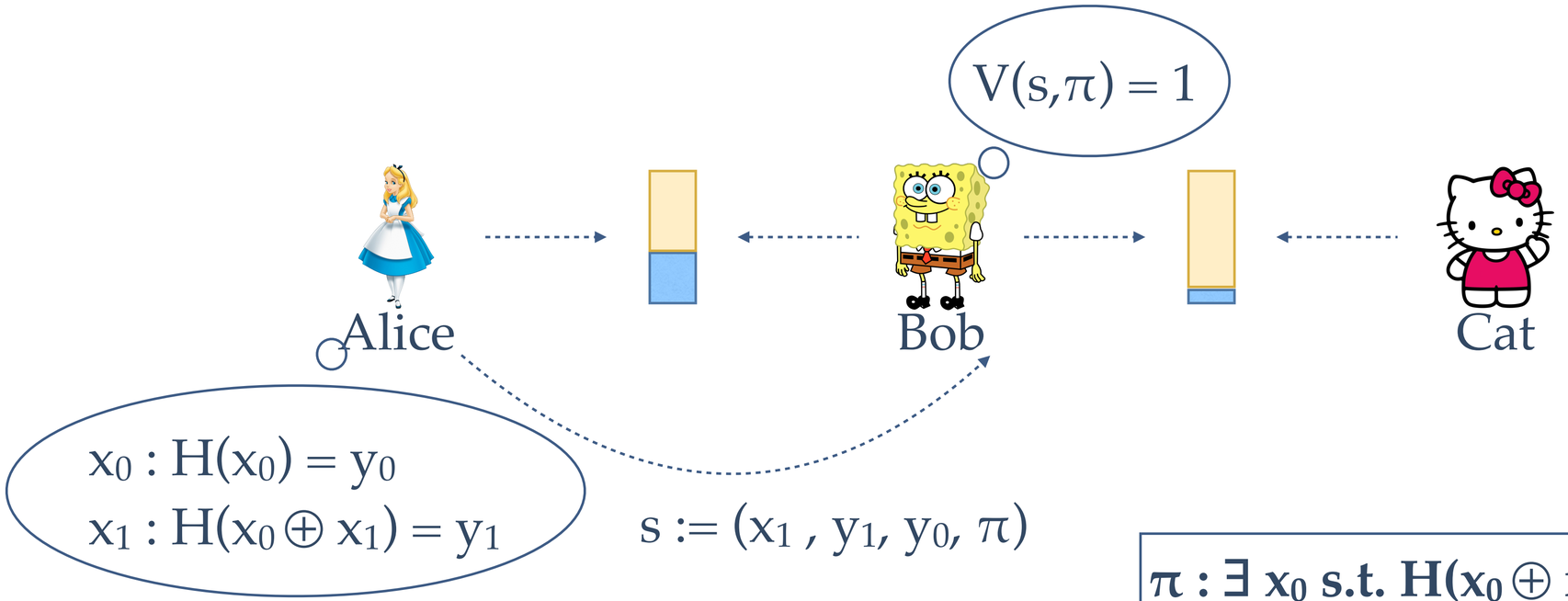
Multi-hop HTLC

- Building block: Non-interactive zero knowledge (ZKBoo [GMO16])



Multi-hop HTLC

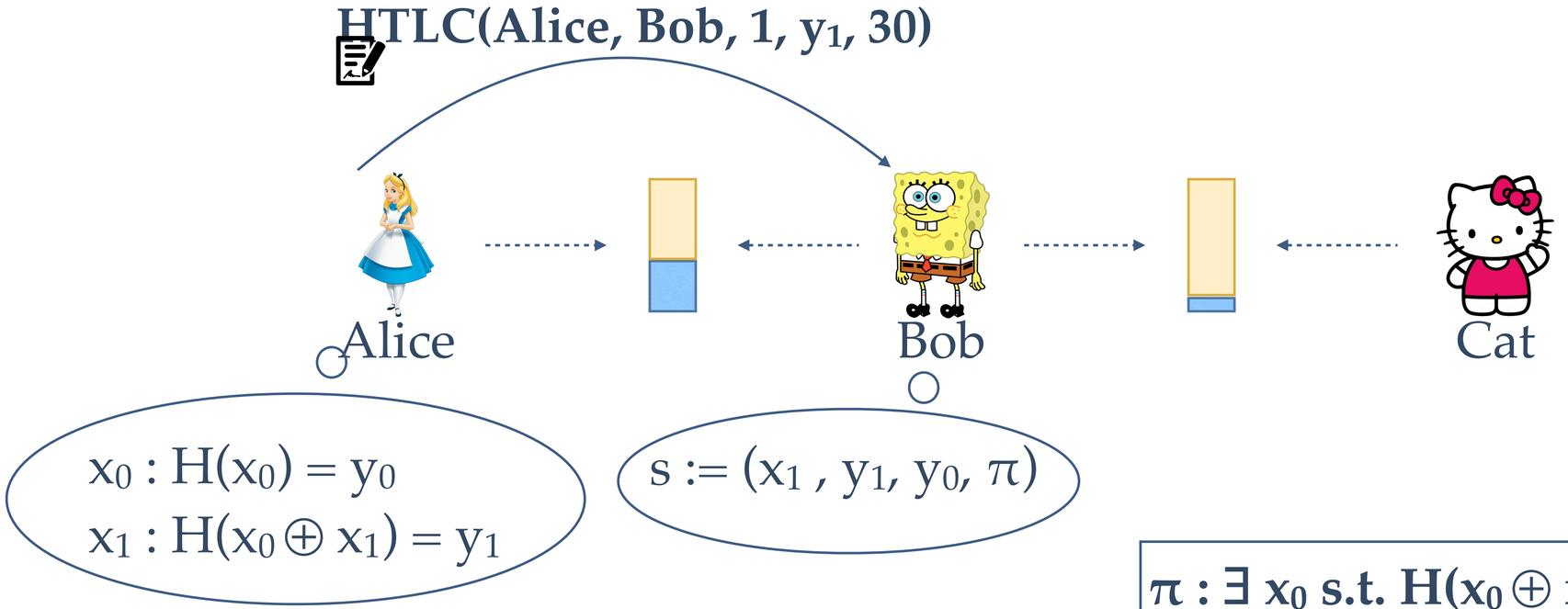
- Building block: Non-interactive zero knowledge (ZKBoo [GMO16])



π : ∃ x_0 s.t. $H(x_0 \oplus x_1) = y_1 \wedge H(x_0) = y_0$

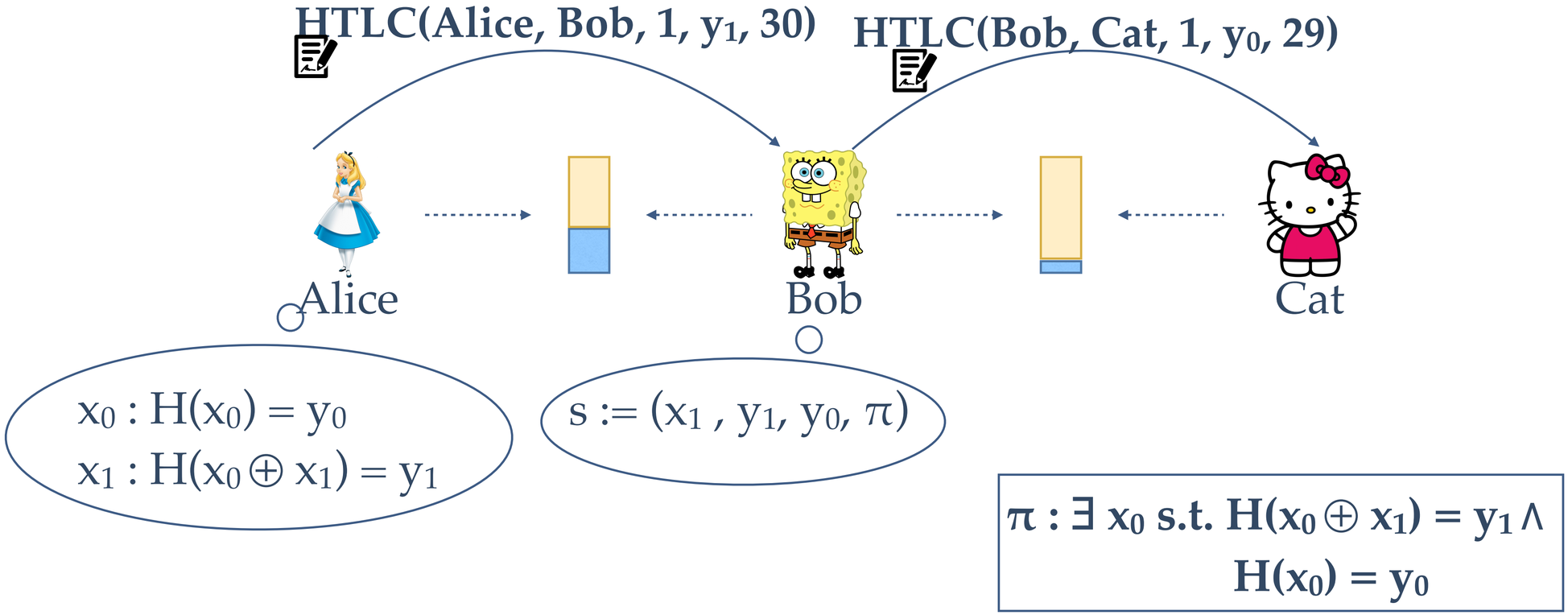
Multi-hop HTLC

- Building block: Non-interactive zero knowledge (ZKBoo [GMO16])

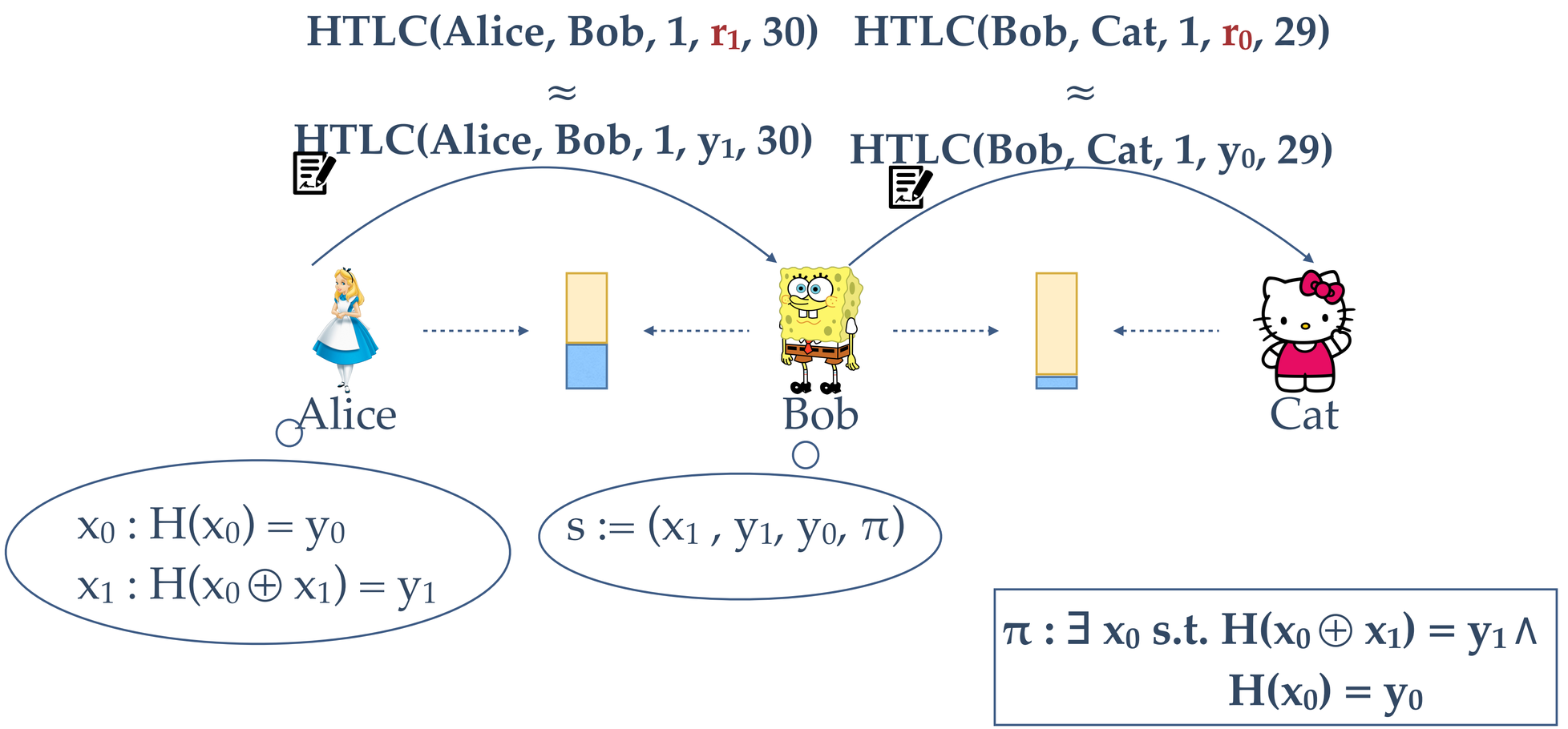


Multi-hop HTLC

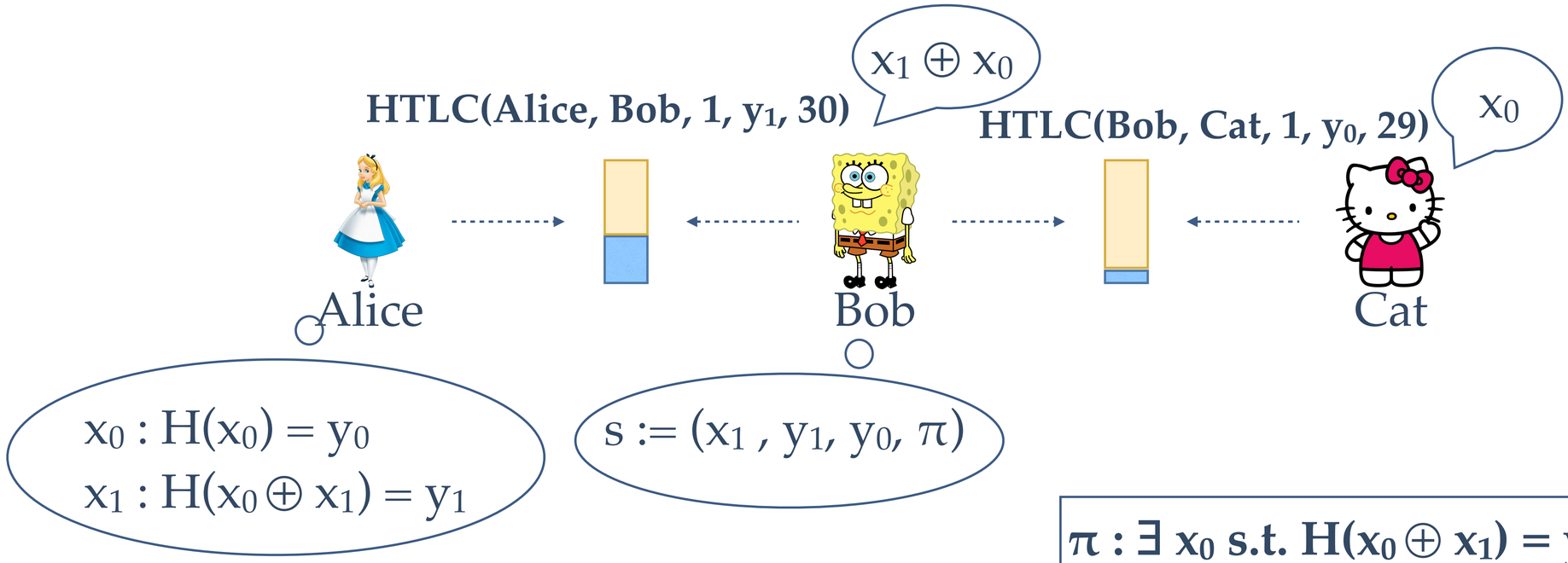
- Building block: Non-interactive zero knowledge (ZKBoo [GMO16])



Multi-hop HTLC

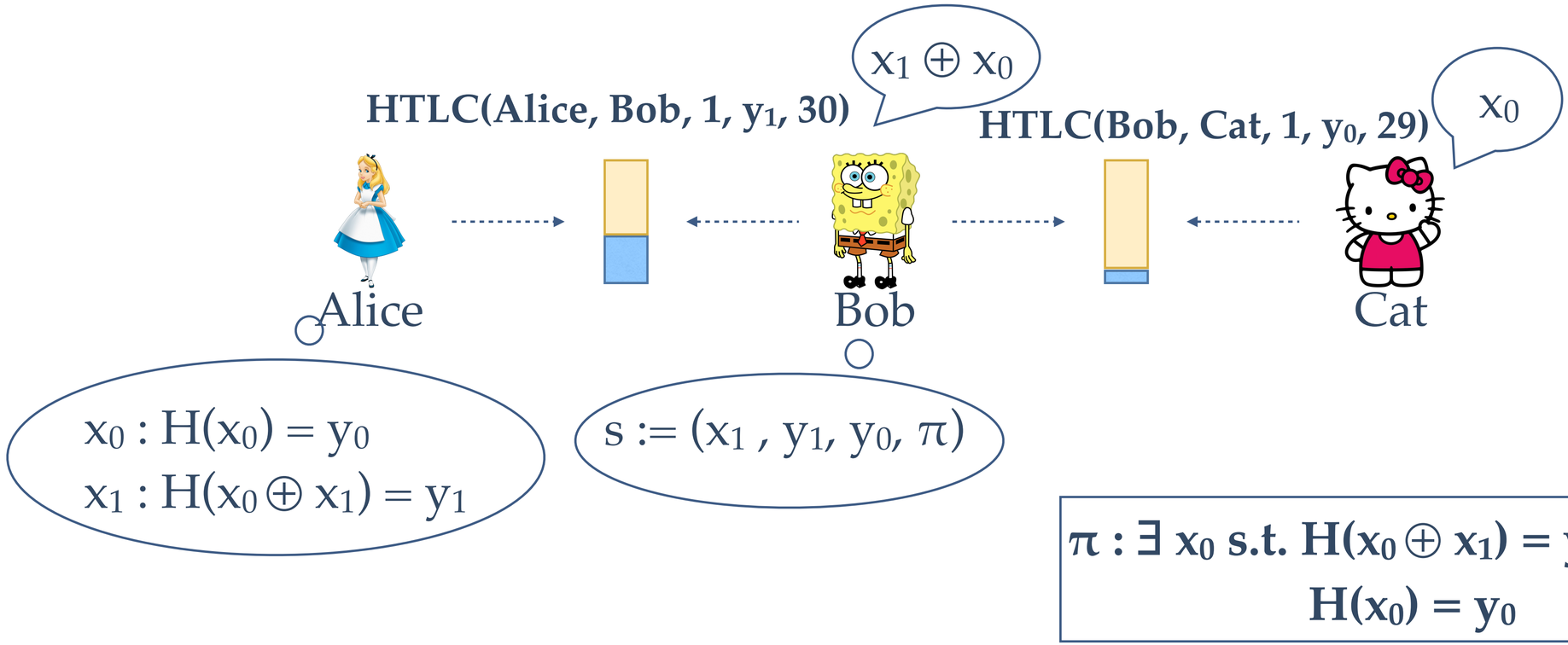


Multi-hop HTLC



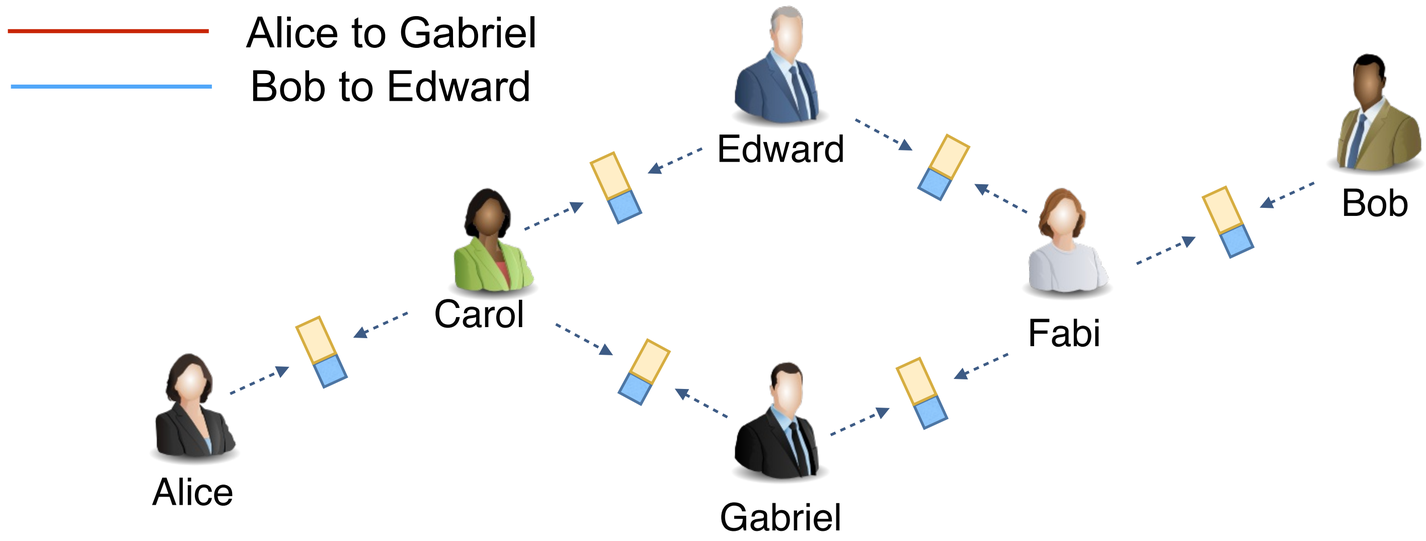
Multi-hop HTLC

- Soundness of NIZK => Bob does not loss coins
- Zero-knowledge of NIZK => Bob does not steal coins



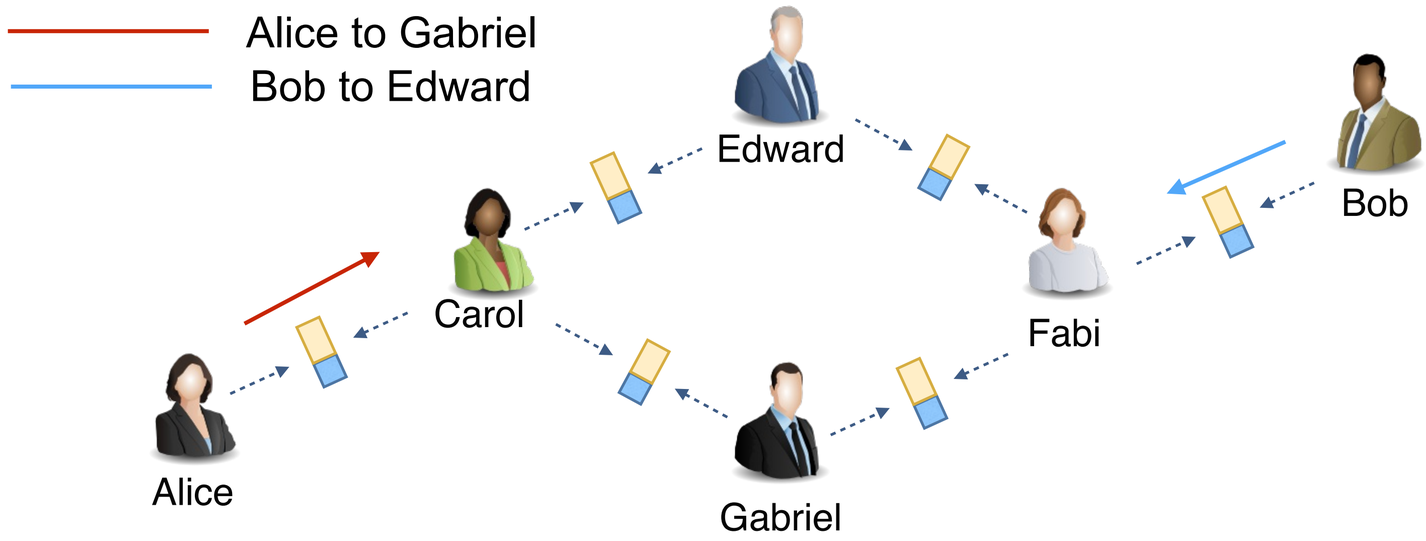
Concurrency in PCNs

- Concurrent on-chain payments can be easily ordered by miners
- No user has a complete view of off-chain concurrent payments in a P2P network
- A blocking solution can lead to deadlocks



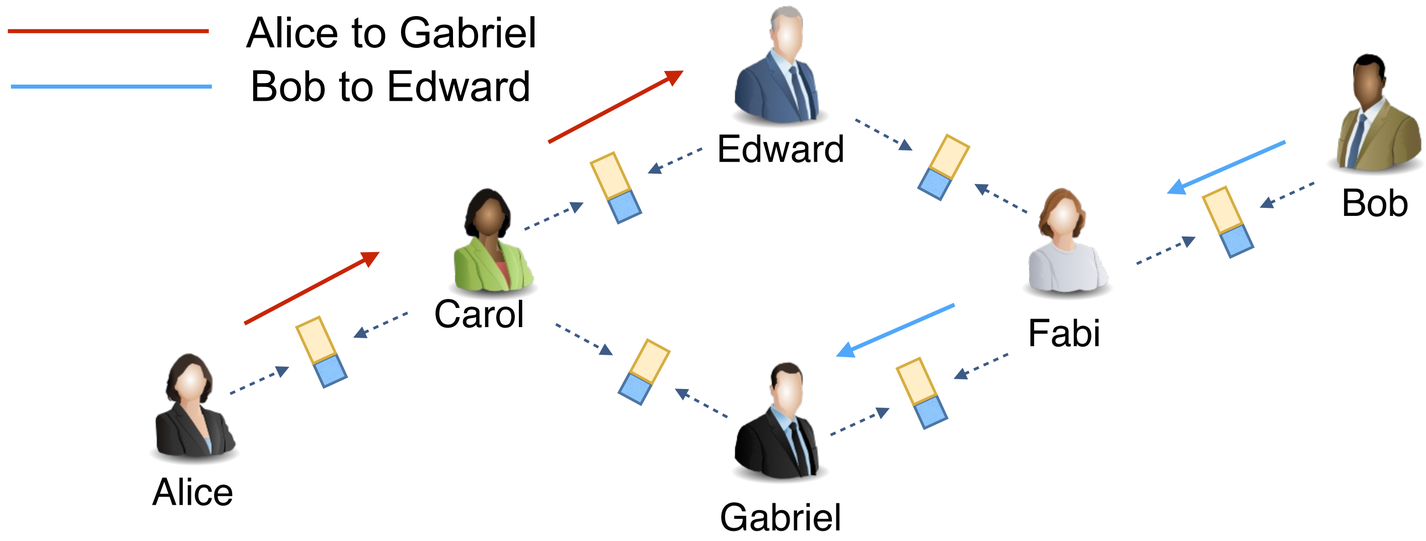
Concurrency in PCNs

- Concurrent on-chain payments can be easily ordered by miners
- No user has a complete view of off-chain concurrent payments in a P2P network
- A blocking solution can lead to deadlocks



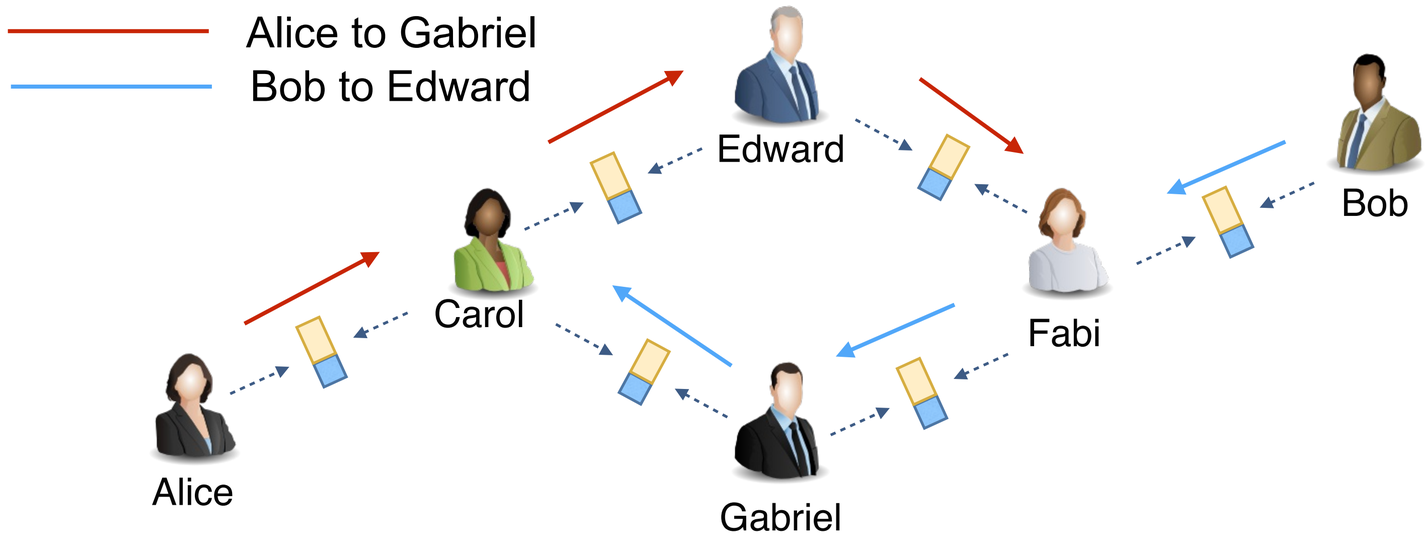
Concurrency in PCNs

- Concurrent on-chain payments can be easily ordered by miners
- No user has a complete view of off-chain concurrent payments in a P2P network
- A blocking solution can lead to deadlocks



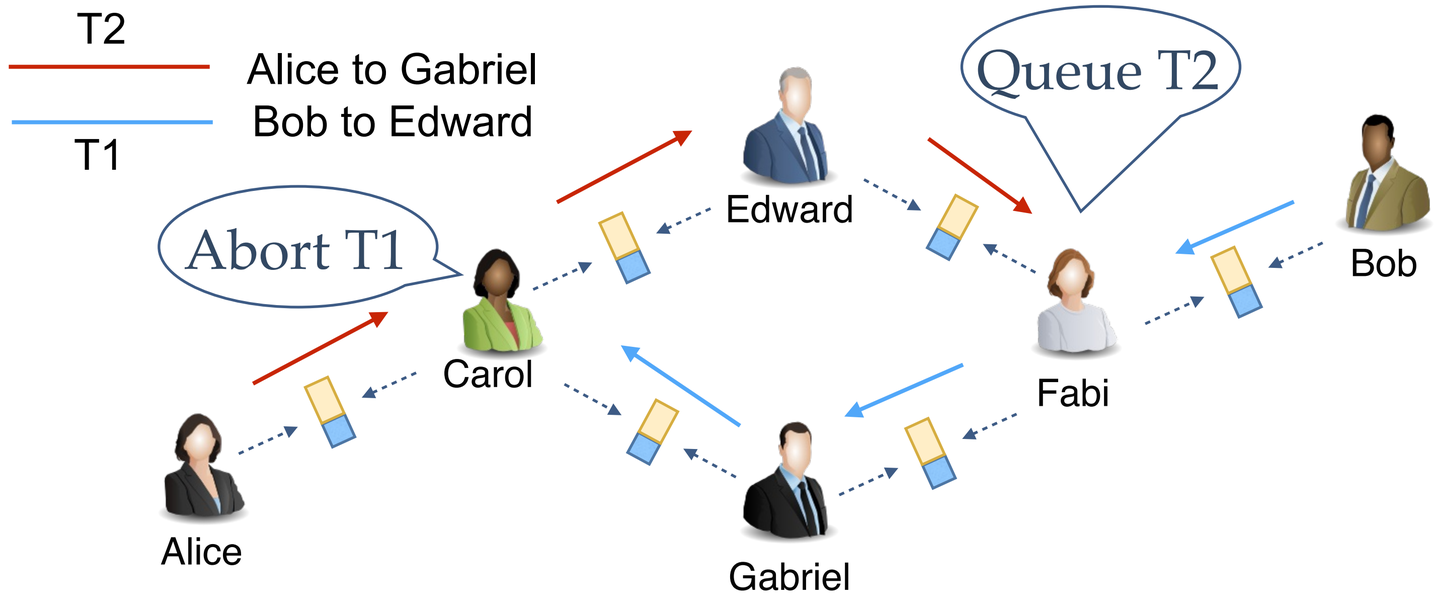
Concurrency in PCNs

- Concurrent on-chain payments can be easily ordered by miners
- No user has a complete view of off-chain concurrent payments in a P2P network
- A blocking solution can lead to deadlocks



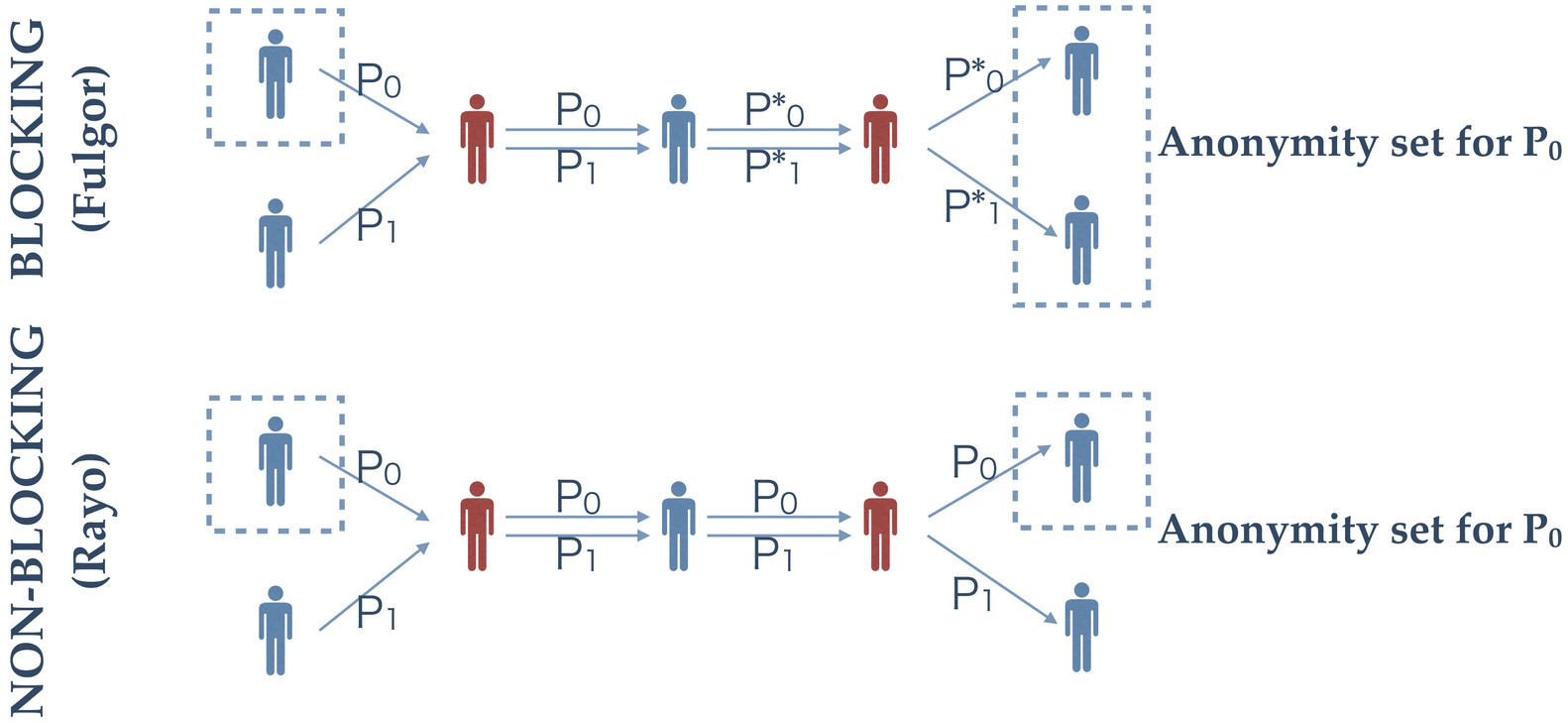
Concurrency in PCNs: Our Solution

- A non-blocking solution (Rayo): at least one payment finishes
- Main idea: Use global transaction identifiers



Concurrency vs Privacy Tradeoff

- Global identifiers leak transaction ID to intermediate users
- Non-blocking solutions cannot achieve strong privacy



Implementation and Performance

- Running time of our solution largely dominated by NIZK
  - Creating a proof requires 309 ms. Proof verification requires 130 ms
  - Proof size: 1.65MB
- 5-hop payment:
  - **Non-private (LN)**: 609 ms
  - **Private:** 1929 ms and ~ 5 MB (**Proofs are not included in the blockchain**)

Conclusions

- Define the security and privacy properties of interest in PCN
- Inherent tradeoff between concurrency and privacy
- Fulgor and Rayo: two approaches for concurrency and privacy
- Our solutions are efficient, compatible with Bitcoin script and without storage overhead in the blockchain

Paper: eprint.iacr.org/2017/820

Thank you for your attention!

Giulio Malavolta, Pedro Moreno-Sanchez,
@pedrorechez

Aniket Kate, Matteo Maffei, and Srivatsan Ravi
@aniketpkate @matteo_maffei