TECHNISCHE UNIVERSITÄT WIEN
Vienna | Austria

FAKULTÄT FÜR INFORMATIK
Faculty of Informatics

S&P SECURITY & PRIVACY GROUP

Blitz: Secure Multi-Hop Payments Without Two-Phase Commits

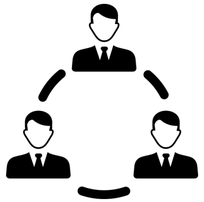
Lukas Aumayr[1], Pedro Moreno-Sanchez[2], Aniket Kate[3], Matteo Maffei[1]

[1]TU Wien, [2]IMDEA Software Institute, [3]Purdue University

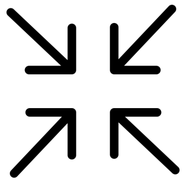
What’s in store?

- Blitz is a new multi-hop payment paradigm for Payment Channel Networks:

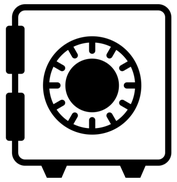
More efficient



Smaller size



Reduced collateral from linear to constant



More secure

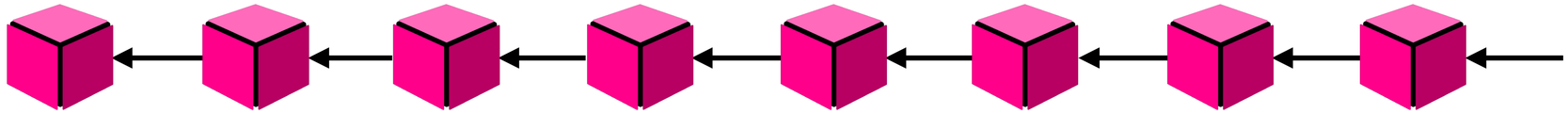
Motivation and background

Blitz construction

Evaluation + comparison to current solutions

Summary

Scalability



- Blockchain: records every transaction
- Global consensus: everyone checks the whole blockchain

Bitcoin's **transaction rate:** ~10 tx/sec
Visa's transaction rate: ~10K tx/sec

Exchange transactions off-chain, Blockchain for disputes

Payment Channels

1) Open

2) Update

3) Close

Alice

Bob

Payment Channels

Lock 8 coins

Lock 2 coins

Alice

Bob

1) Open

2) Update

3) Close

Payment Channels

1) Open

2) Update

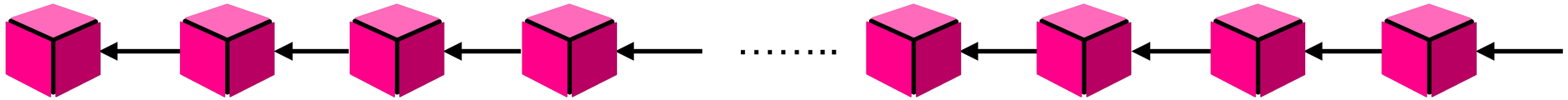
3) Close

Alice

State 0

Bob

Payment Channels



1) Open

2) Update

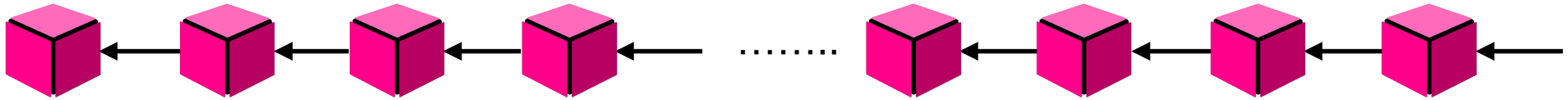
3) Close

Alice

State 0

Bob

Payment Channels



1) Open

2) Update

3) Close

Alice

Bob

State 0

2	8

State 1

4	6

Payment Channels

1) Open

2) Update

3) Close

Alice

Bob

State 0

State 1

State 2

Payment Channels

1) Open

2) Update

3) Close

Alice

Bob

State 0

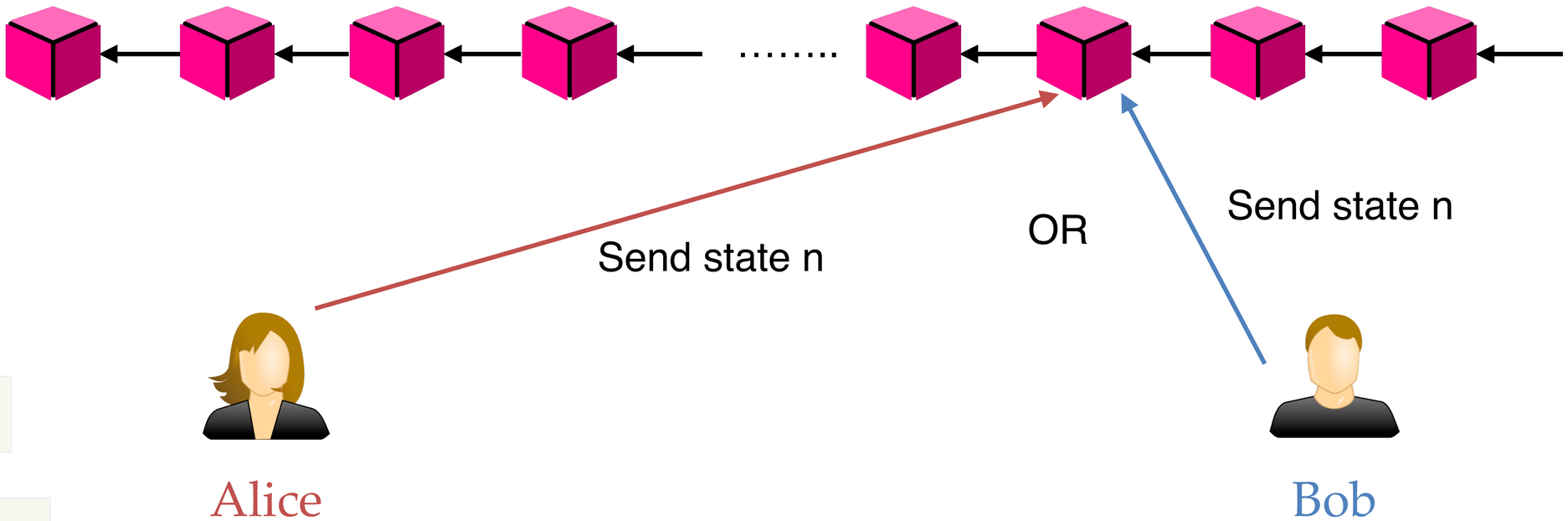
State 1

State 2

...

State n

Payment Channels

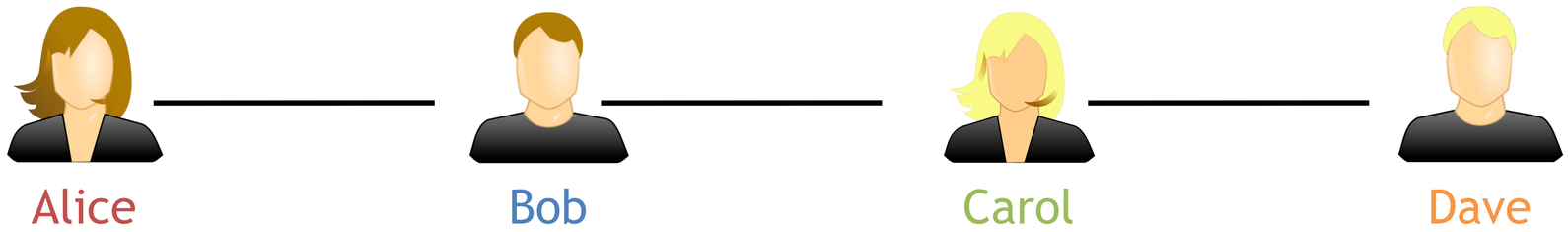


1) Open

2) Update

3) Close

Payment Channel Network (PCN)



- Infeasible to open channels with everyone
- Link channels to form a PCN
- Multi-hop payments
- e.g., Lightning Network (LN) [1]
  - 53M $ locked
  - 20k nodes
  - 46k channels

[1] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," *2016*

Multi-hop payments in the Lightning Network

Alice

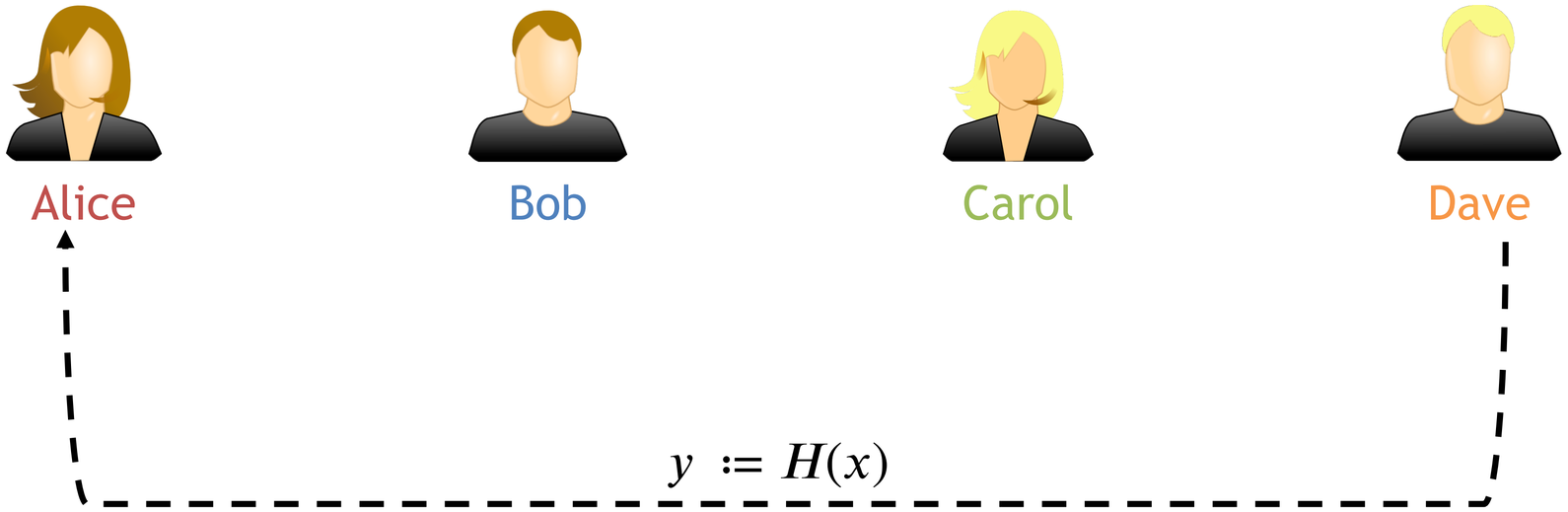
Bob

Carol

Dave

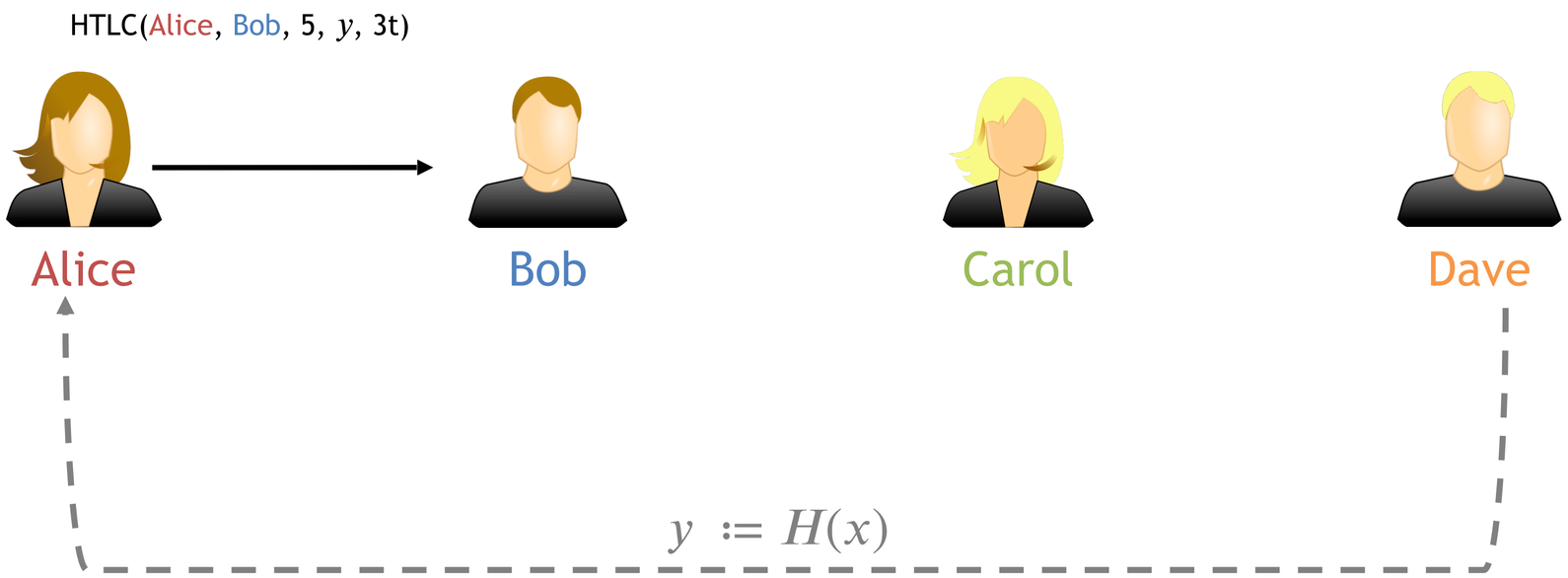
Scenario: Alice wants to pay 5 coins to Dave, via Bob and Carol

Multi-hop payments in the Lightning Network



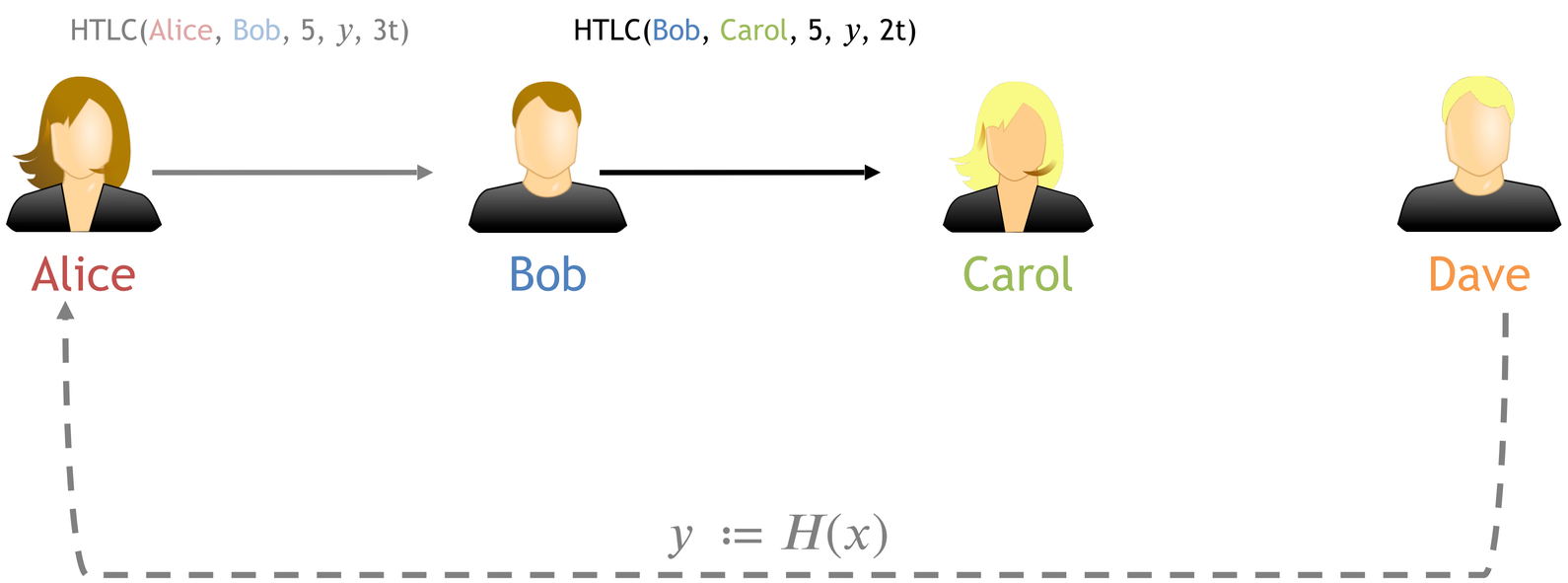
1. Dave samples x and sends $y := H(x)$ to Alice

Multi-hop payments in the Lightning Network



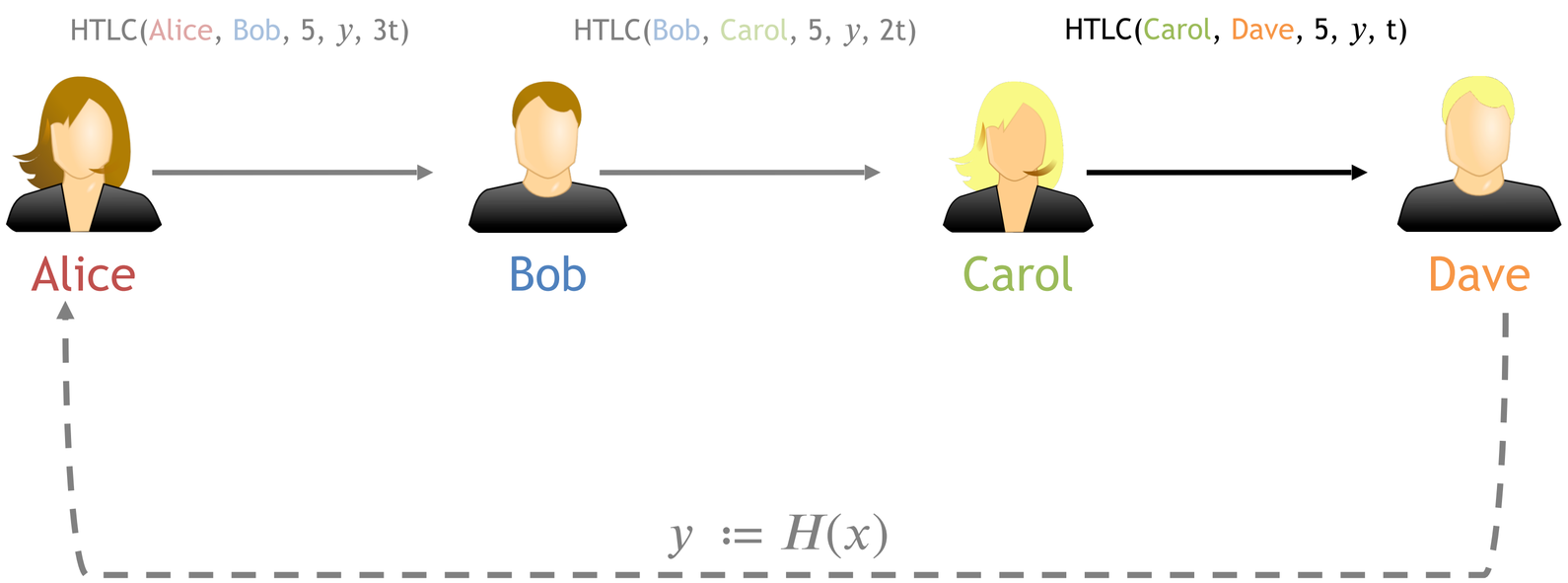
2. Alice sets up an HTLC with Bob holding 5 coins
   - Bob gets money if he knows x, s.t. $H(x) = y$
   - Alice gets money after timeout 3t

Multi-hop payments in the Lightning Network



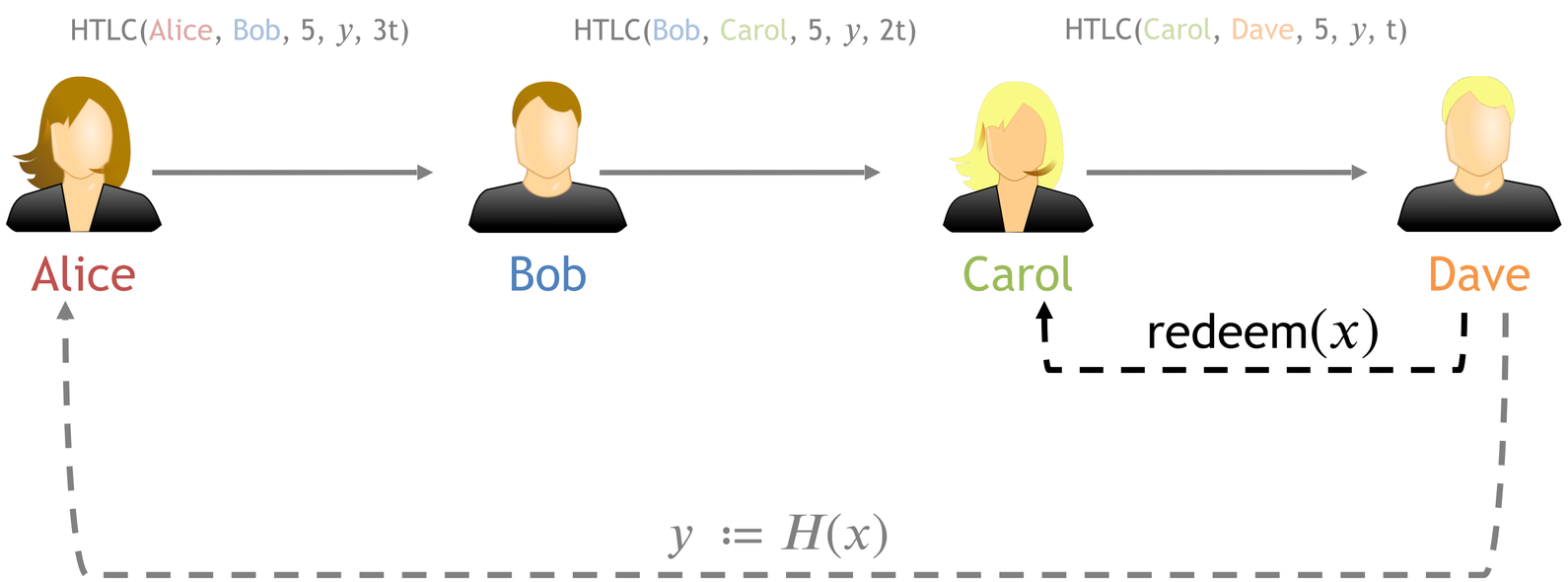
3. Bob sets up an HTLC with Carol

Multi-hop payments in the Lightning Network



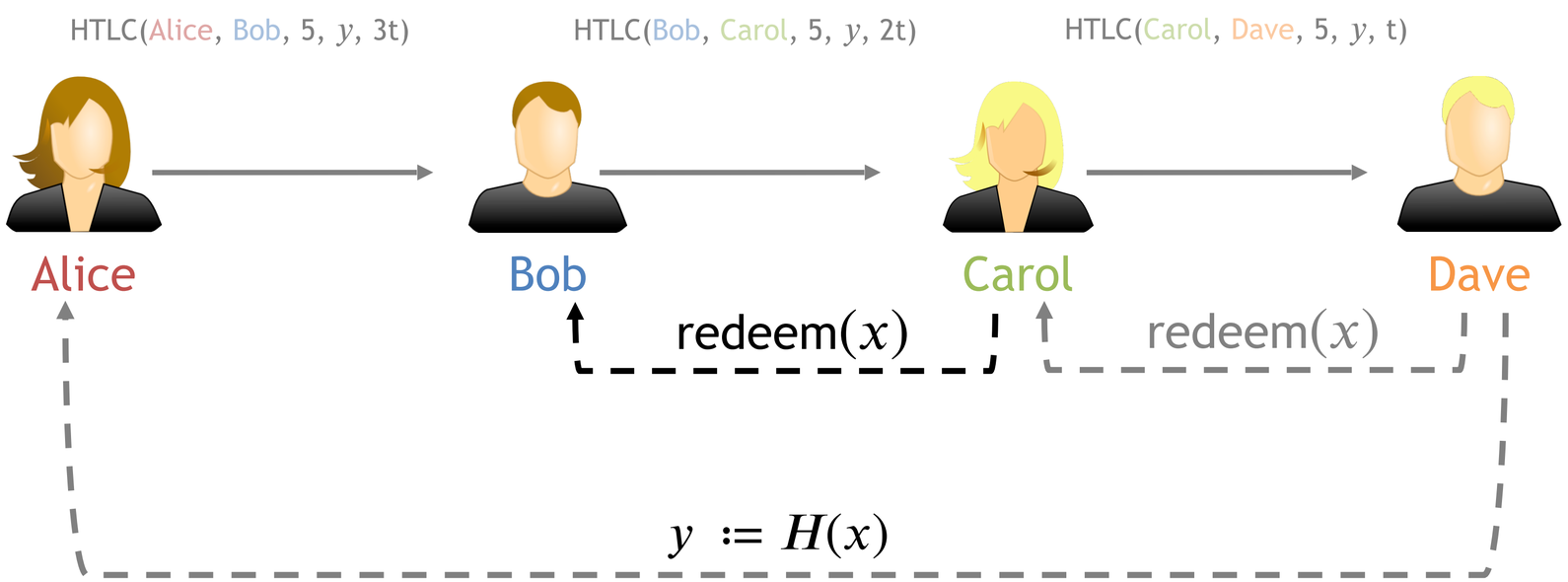
4. Carol sets up an HTLC with Dave

Multi-hop payments in the Lightning Network



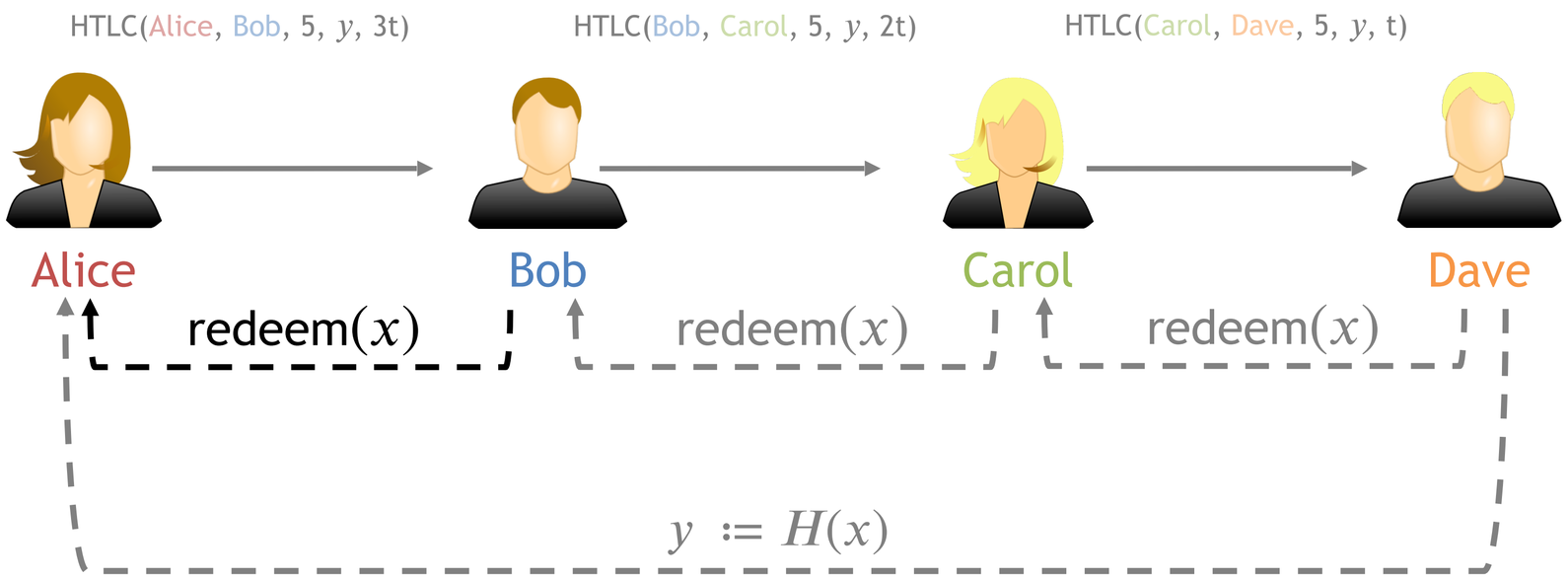
5. Dave redeems the HTLC with Carol by revealing x and claims the 5 coins

Multi-hop payments in the Lightning Network



6. Carol redeems the HTLC with Bob

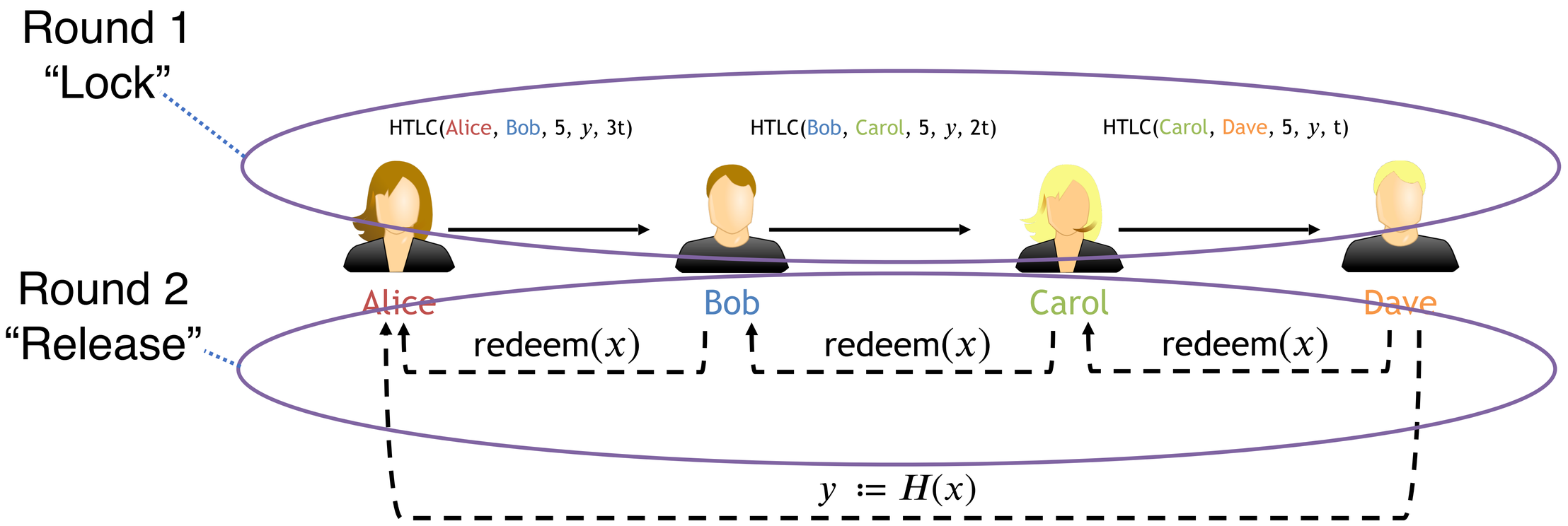
Multi-hop payments in the Lightning Network



7. Bob redeems the HTLC with Alice

➡ Payment successful

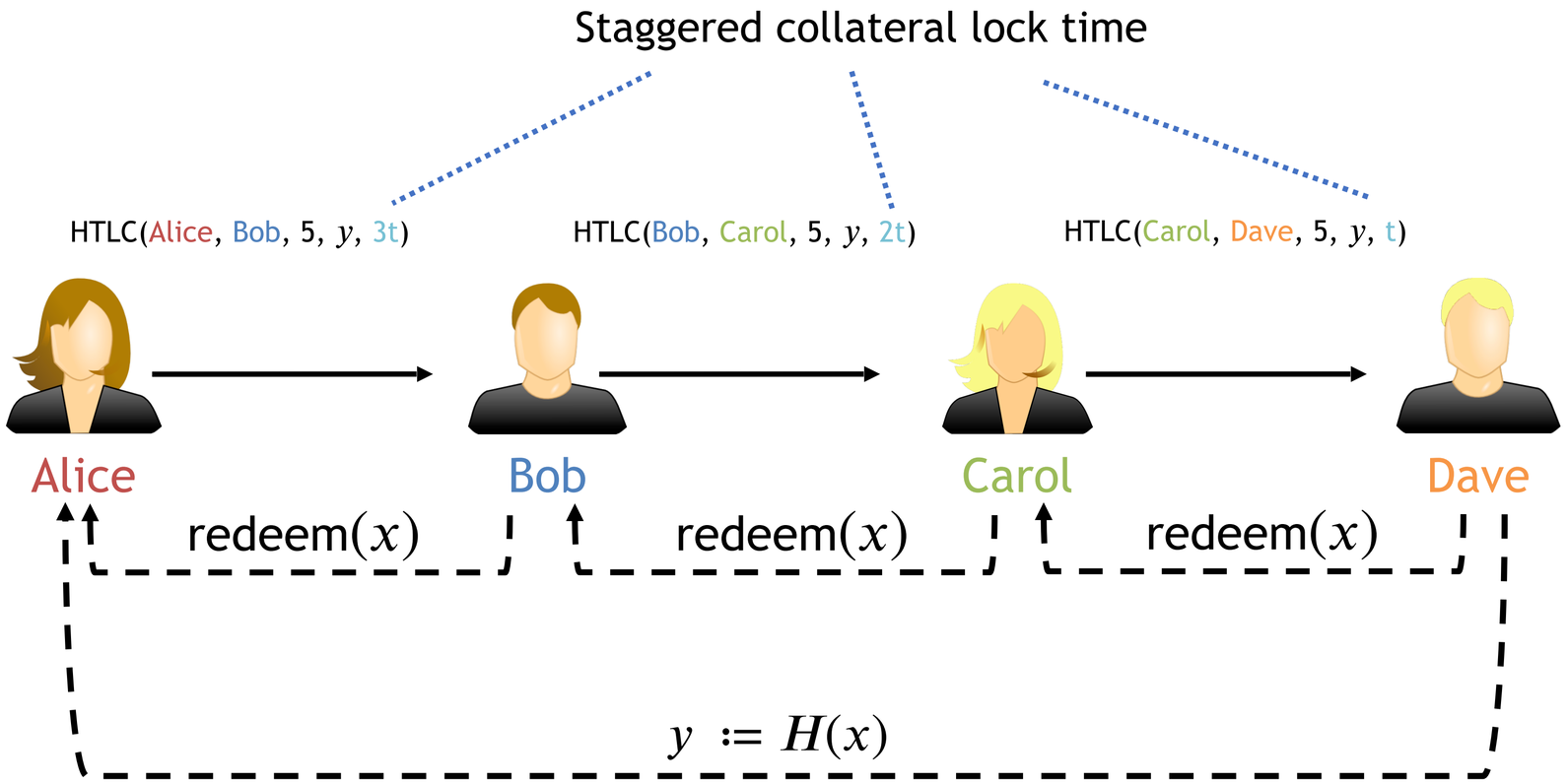
Two-Phase Commit



Two rounds of communication are required!

Round := sequential, pairwise communication from sender to receiver

Multi-hop payments in the Lightning Network



Payments happen off-chain in honest case

Staggered collateral to give enough time to claim on-chain in case of dispute

Properties & drawbacks of Lightning payments

- Scalability ✔
- “Balance Security” ✔
- Privacy ✔

Drawbacks:

- Staggered collateral lock time ✖
  - Decreases network throughput
- Takes two rounds ✖
- HTLC scripting requirements ✖
- Wormhole attack [2] ✖

[2] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate and M. Maffei, "Anonymous Multi-Hop Locks for Blockchain Scalability and Interoperability,” NDSS, *2019*

Motivation and background

Blitz construction

Evaluation + comparison to current solutions

Summary

Pay-or-revoke paradigm

Again: Alice wants to pay 5 coins to Dave, via Bob and Carol

Alice

Bob

Carol

Dave

Pay-or-revoke paradigm

Alice

Alice defines a timeout T, independent of the path length

Alice

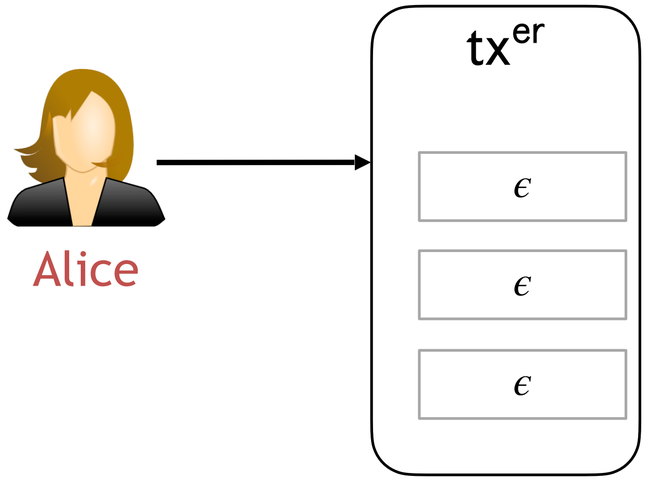
Bob

Carol

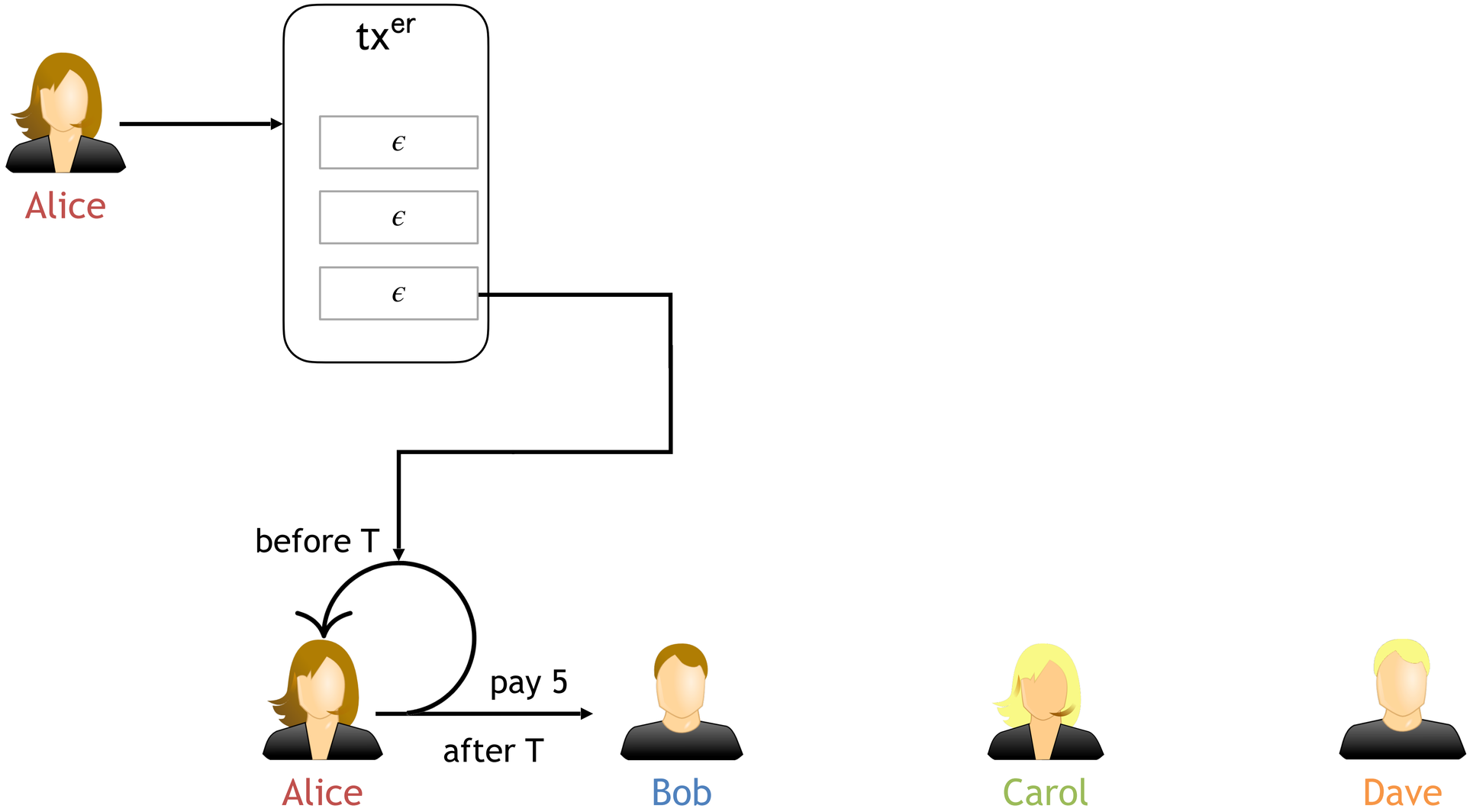
Dave

Pay-or-revoke paradigm

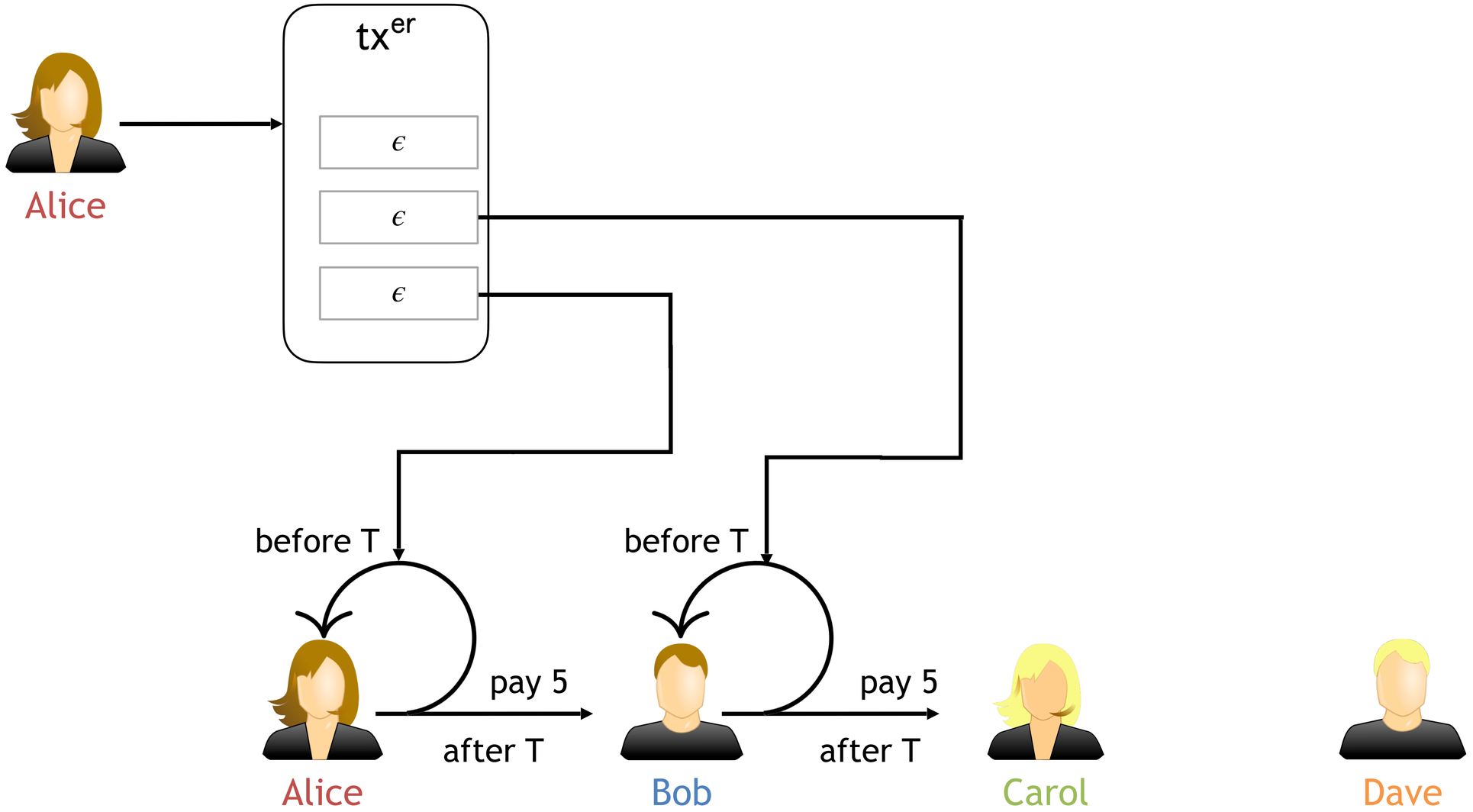
Alice creates refund enabling transaction: tx^{er}



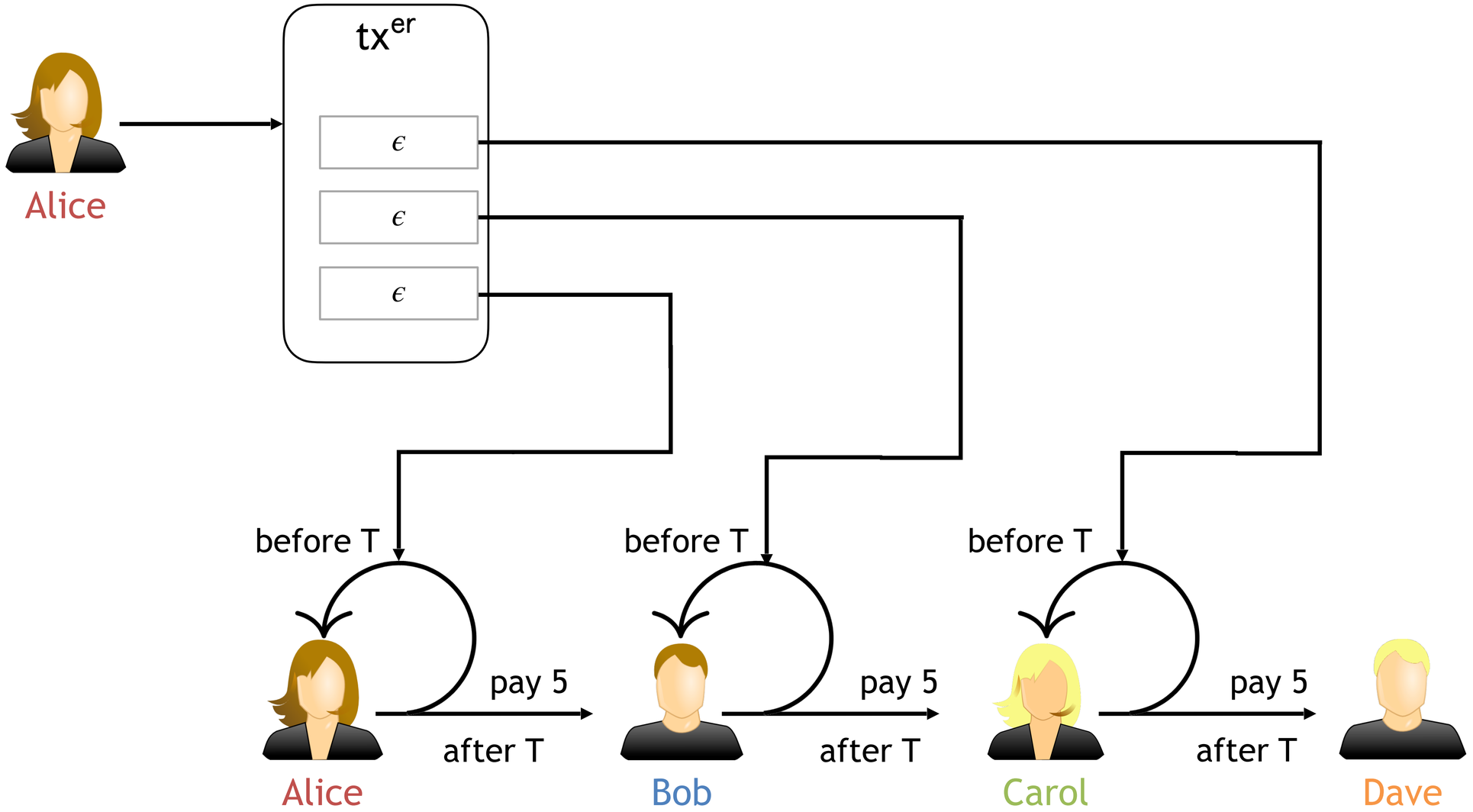
Pay-or-revoke paradigm



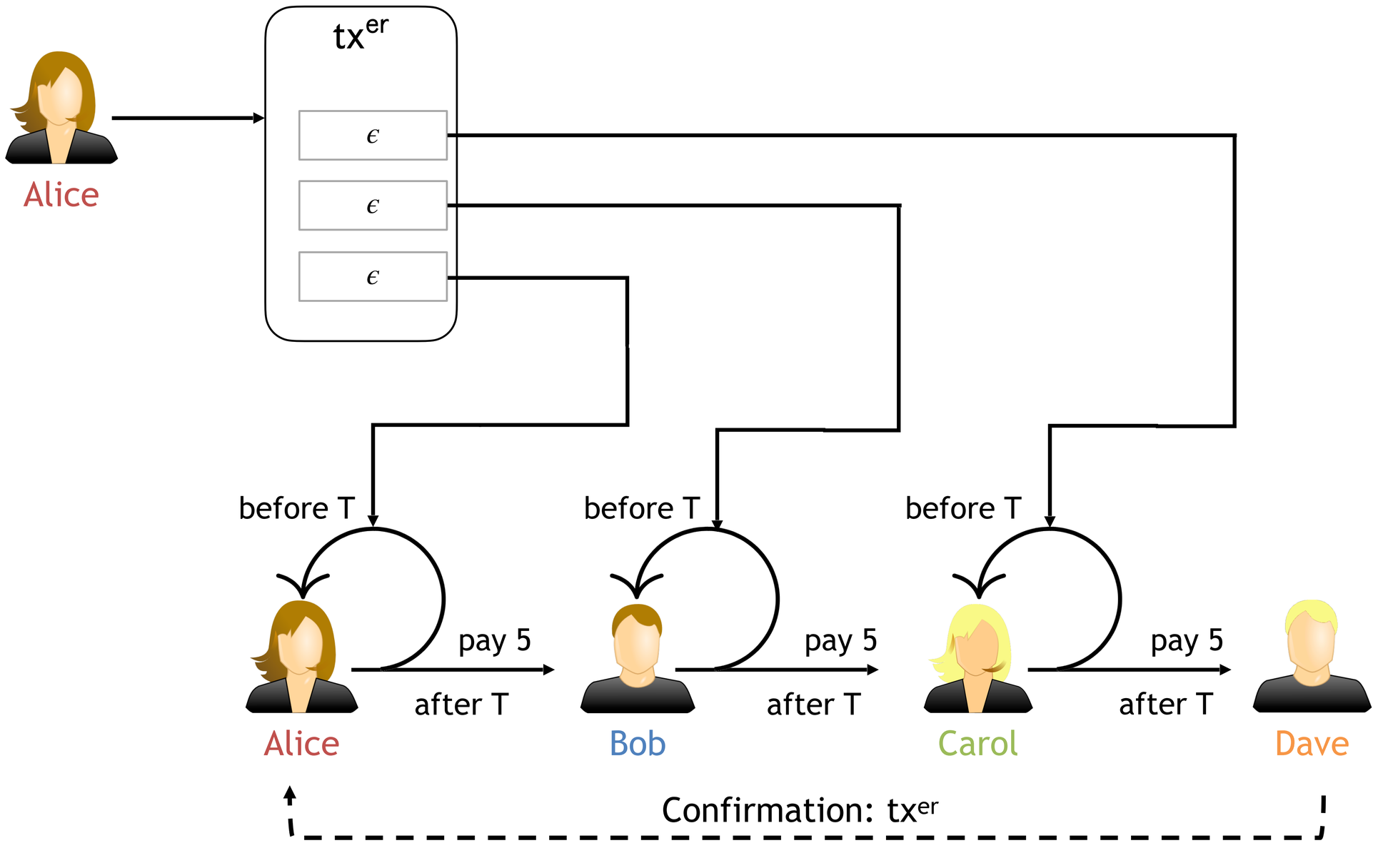
Pay-or-revoke paradigm



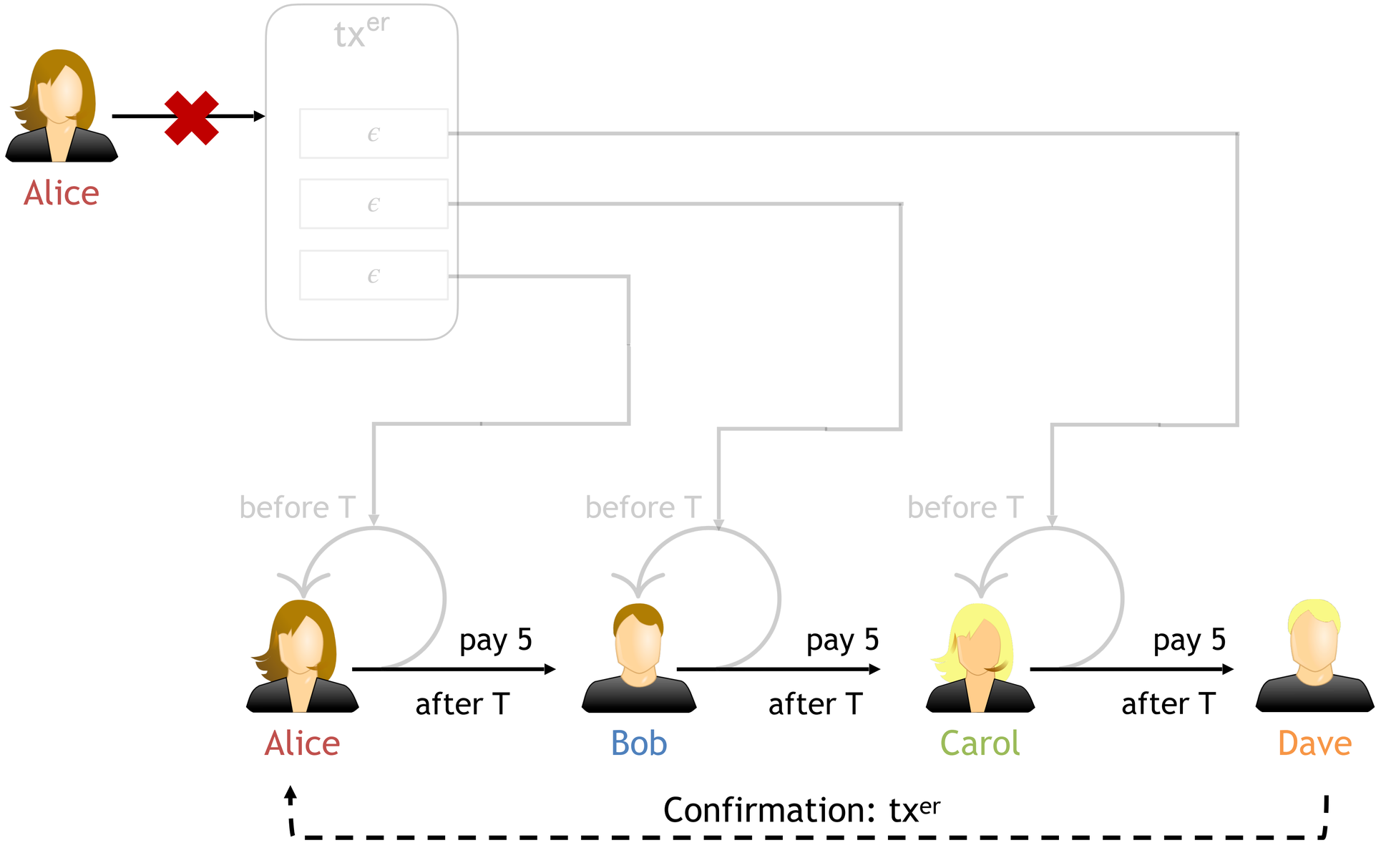
Pay-or-revoke paradigm



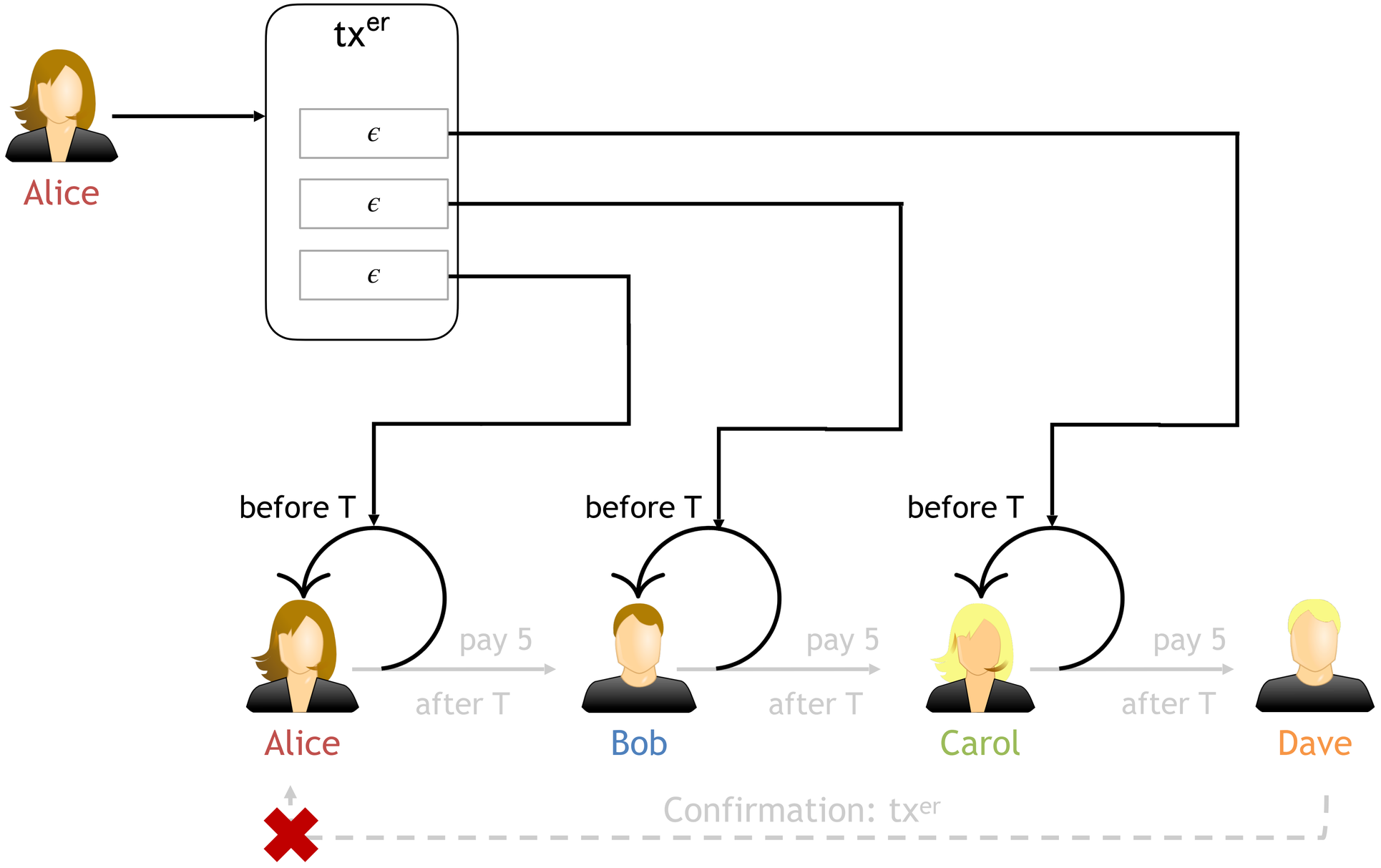
Pay-or-revoke paradigm



Successful payment



Refund


tx^er
ϵ
ϵ
ϵ
Alice
before T
before T
before T
pay 5
after T
pay 5
after T
pay 5
after T
Alice
Bob
Carol
Dave
Confirmation: tx^er

More

- Fast track for instant payments 
- Fast revoke for refunds without posting tx[er] 
- Privacy by using stealth addresses 
- Check the paper for more information!

Motivation and background

Blitz construction

Evaluation + comparison to current solutions

Summary

Comparison to current solutions

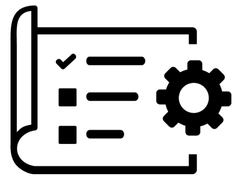
	ILP [3]	Lightning [1]	AMHL [2]	Blitz
Balance security	No	Yes	Yes	Yes
Number of rounds	1	2	2	1 (2 for fast track)
Collateral lock time	N/a	Linear	Linear	Constant
Atomicity	No	No (Wormhole)	Yes	Yes
Scripting capabilities	Signatures	Signatures, timelocks, hashlocks[1]	Signatures, timelocks	Signatures, timelocks

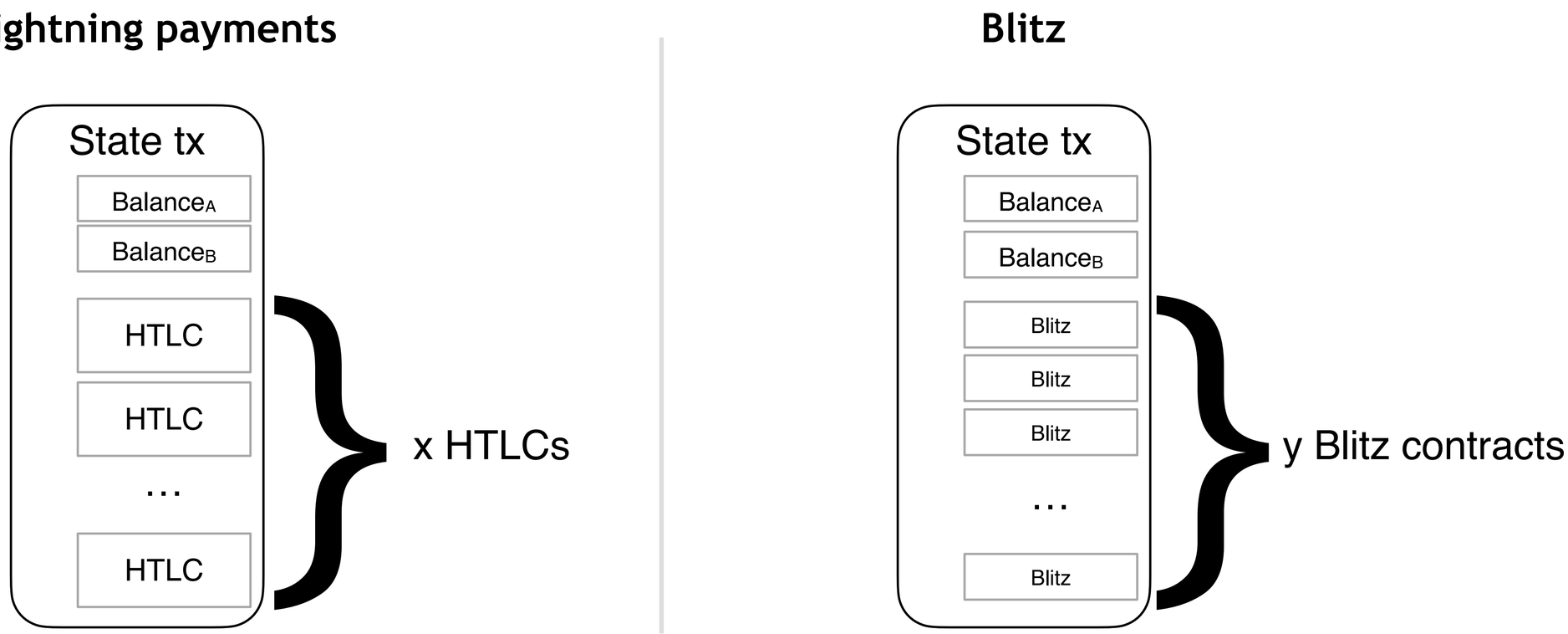
[1] Using constructions such as scriptless scripts, one could get rid of hashlocks.

[3] S. Thomas and E. Schwartz, "A Protocol for Interledger Payments," *2015*

Evaluation

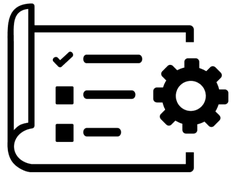
- Blitz contract 26% smaller than Lightning contract (HTLC)
- Can increase number of concurrent payments per channel



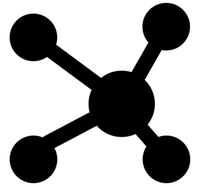


Evaluation

- Blitz contract 26% smaller than Lightning contract (HTLC)
- Can increase number of concurrent payments per channel



- Simulation on Lightning Network snapshot
- Random payments, some are disrupted
- Constant (Blitz) vs. staggered (Lightning) collateral
- Depending on setting, between 4x and 33x fewer failed payments in Blitz



Motivation and background

Blitz construction

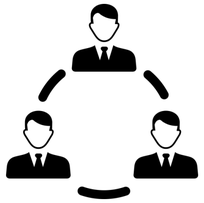
Evaluation + comparison to current solutions

Summary

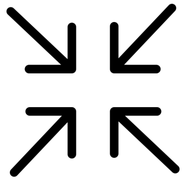
Take Home

- New multi-hop payment paradigm for Payment Channel Networks

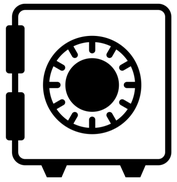
Only one round of communication



Contract size reduced by 26%



Reduced collateral from linear to constant



Security against Wormhole attack

- Only requires Signatures and Timelocks
- Simulation showing practical advantage of constant collateral
- Formally modelled in UC framework and security proofs
- Compatible with the Lightning Network

Thanks!

eprint.iacr.org/2021/176.pdf

lukas.aumayr@tuwien.ac.at

@lukas_aumayr