CERIAS

The Center for Education and Research in Information Assurance and Security

Fulgor: Concurrent and Privacy Preserving Transactions with Payment-Channel Networks

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

[§]Purdue University [†]CISPA, Saarland University [‡]TU Vienna

* Both authors contributed equally and are considered to be co-first authors

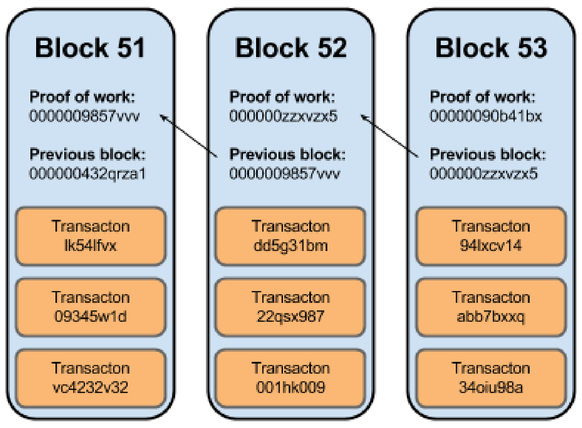
(1) Bitcoin Blockchain

Bitcoin today:

- Decentralized cryptocurrency
- Payments logged in blockchain
- Widely used in practice
  - → > 200,000 daily payments
  - → > 12M accounts

Scalability Issues:

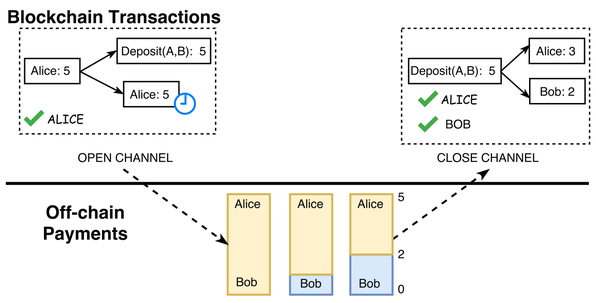
- New block every 10 min on average
- Limited to ~10 payments per second



(2) Addressing Scalability Issues

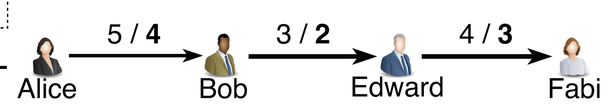
A Bitcoin payment channel:

1. Open a channel in the blockchain
2. Several off-chain payments
3. Close the channel in the blockchain



A payment-channel network:

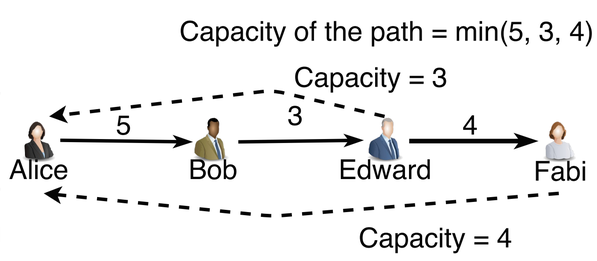
- Network of pairwise channels
- Payment value up to lowest capacity in the path (e.g., min(5,3,4))
- Each channel decreased by payment value (e.g., pay 1 bitcoin)



(3) Problem Definition (I): Privacy

Challenges:

- Find path capacity without revealing individual channels capacity
- Perform payment revealing payment value only to users in the path



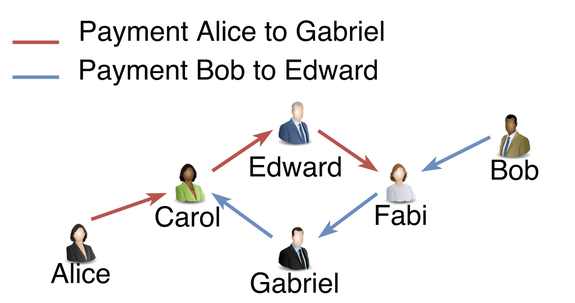
Our privacy goals:

1. **Test Privacy:** Only reveal whether there is enough capacity in the path
2. **Value Privacy:** Reveal payment value only to users in the path
3. **Anonymity:** Sender and receiver remain unknown to other users

(4) Problem Definition (II): Concurrency

Challenge:

- Perform concurrent payments that use common payment channels in their payment paths



Our concurrency goals:

1. **Two users agreement:** Both users agree on their payment channel state
2. **Atomicity:** All or none of the payment channels in a path are updated
3. **Progress:** At least one of the concurrent payments finishes

(5) Fulgor: Test Operation

Ideas:

- Communication between neighbors. A user only knows her neighbors
- Test operation reveals whether path capacity is smaller than a value v

$\mathsf{test}_{\mathsf{Sdr}}(\{u_i\}_{i\in[n]}, \mathsf{Rcv}, v)$:

$\forall i \in [n-1]$:
  $r_i \leftarrow \{0,1\}^\lambda$
  $c_i \leftarrow \mathsf{Enc}(\mathsf{ek}_{u_i}, r_i || u_{i+1})$
$r_n \leftarrow \{0,1\}^\lambda$
$c_n \leftarrow \mathsf{Enc}(\mathsf{ek}_{u_n}, r_n || \mathsf{Rcv})$
$r_0 \leftarrow \{0,1\}^\lambda$
$\pi \leftarrow \mathcal{P}^n$
$\mathsf{Send}(\mathsf{Rcv}, (r_0, \ldots, r_n))$
return $(c_{\pi(1)}, \ldots, c_{\pi(n)}, r_0, v)$ **to** u_1

$\mathsf{test}_{u_j}(\{c_i\}_{i\in[n]}, r, v)$:

$\forall i \in [n]$:
  if $\perp \neq \mathsf{Dec}(\mathsf{dk}_{u_j}, c_i)$
    $r_j || u_{j+1} = \mathsf{Dec}(\mathsf{dk}_{u_j}, c_i)$
if $v \leq \mathsf{cap}_{(u_j, u_{j+1})}$
  $r := r \oplus r_j$
else
  $s \leftarrow \{0,1\}^\lambda$
  $r := s$
return $(\{c_i\}_{i\in[n]}, r, v)$ **to** u_{j+1}

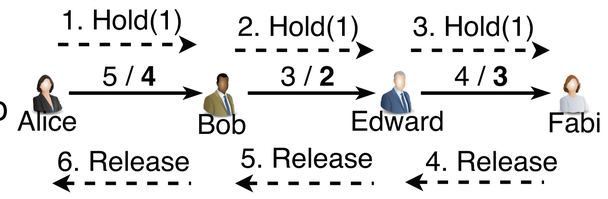
$\mathsf{test}_{\mathsf{Rcv}}(\{c_i\}_{i\in[n]}, r, v)$:

$\mathsf{Recv}(\mathsf{Sdr}, (r_0, \ldots, r_n))$
$r' := \bigoplus_{i\in\{0,\ldots,n\}} r_i$
if $r' = r$
  return 1 **to** Sdr
else
  return 0 **to** Sdr

(6) Fulgor: Payment Operation

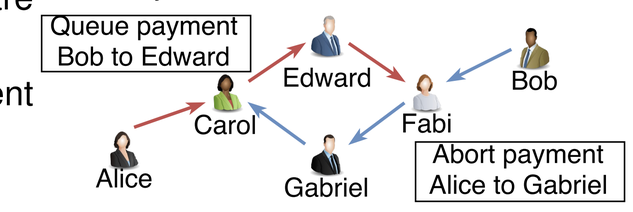
Decentralized payment operation in two phases:

1. Hold coins from sender to receiver
2. Release coins from receiver to sender



Concurrent payments are prioritized by their identifiers

- Payments with higher identifier are forwarded first
- If not enough capacity, payment with higher identifier is queued



(7) Implementation

Implementation details:

- Proof-of-concept in Python
- Path up to 20 users
- Results similar to non-private version

Evaluation:

	Computation	Communication	
		test	pay
Sender	112 ± 7.44 ms	10264 B	10244 B
Int. User	96 ± 5.43 ms	10264 B	10244 B
Receiver	3 ± 1.2 ms	8 B	8 B

(8) Conclusions

- Fulgor is payment-channel network compatible with current Bitcoin
- Provides privacy properties and non-blocking concurrent payments
- Efficient *test* and *payment* operations

Acknowledgments: This project has been supported by the CERIAS/Intel Research Assistantship

CERIAS

PURDUE UNIVERSITY