Bolt: Blind Offchain Lightweight Transactions

Ian Miers

Cornell Tech/ Zcash

(Joint work with Matthew Green)

Blockchain payments are costly in terms of:

Latency/time

Resource usage

Money

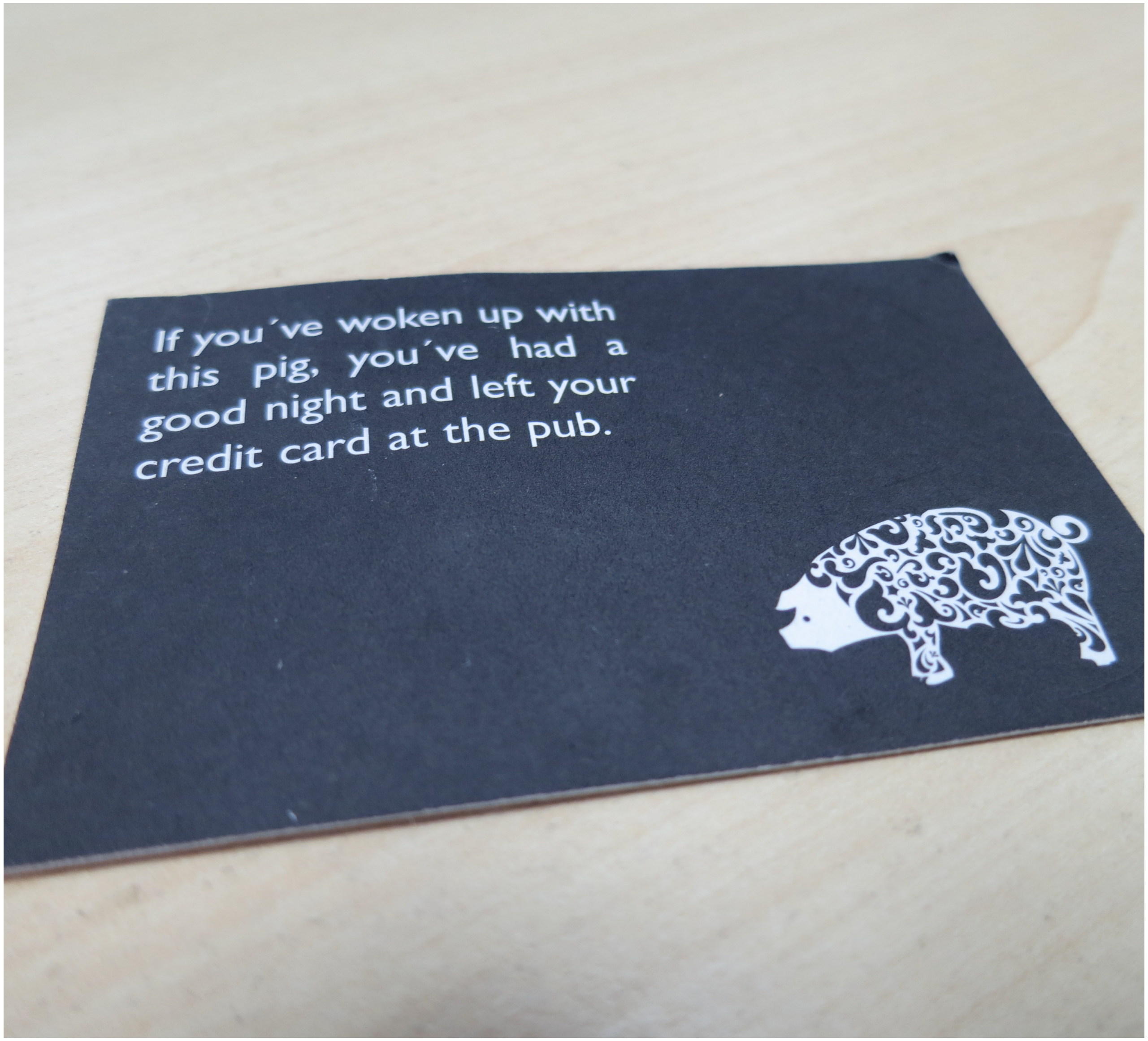
Bank BPH
MasterCard

JAMESON
IRISH WHISKEY
KNOB CREEK
Kentucky straight bourbon whiskey
small batch
9 aged nine years
JIM BEAM
KENTUCKY STRAIGHT BOURBON WHISKEY
JAMES B. BEAM DISTILLING CO.
JACK DANIEL'S
Old No. 7
Tennessee WHISKEY
Dewar's
"White Label"
SOUTHERN COMFORT
Tanqueray
IMPORTED
BOMBAY SAPPHIRE
Distilled LONDON DRY GIN
Jose Cuervo
BACARDI
SUPERIOR
PUERTO RICAN RUM
Captain Morgan
ORIGINAL SPICED RUM
MALIBU
CARIBBEAN RUM
COCONUT FLAVOR
209361
208963

Repeated payments: bar tab

- Trust you: give card when you leave and pay tab

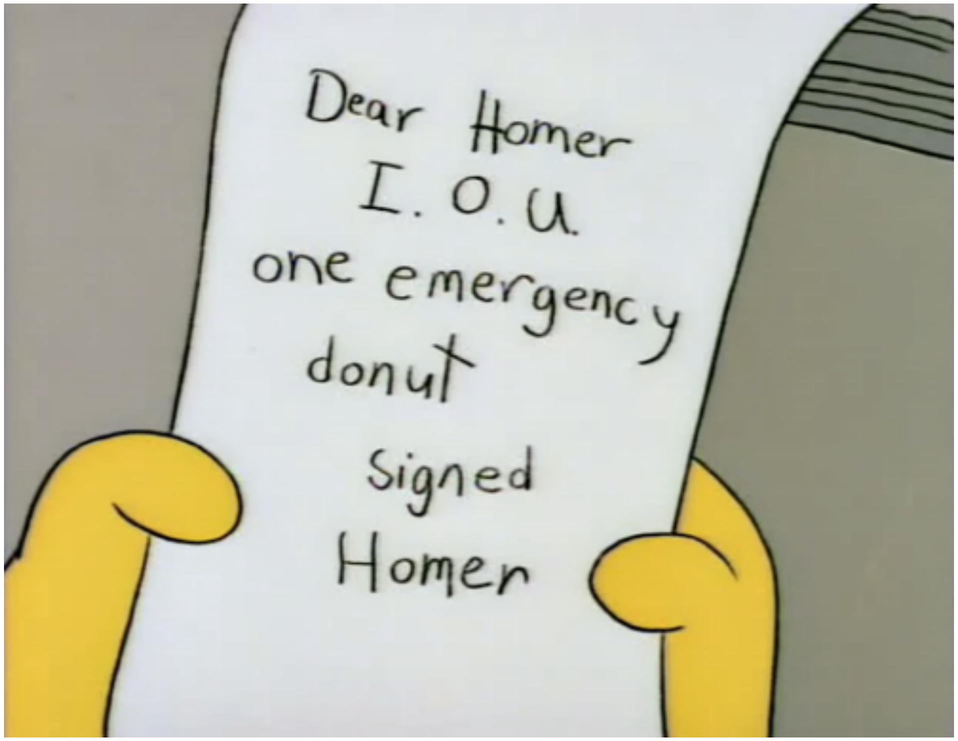
- Trust bar: give card at the start

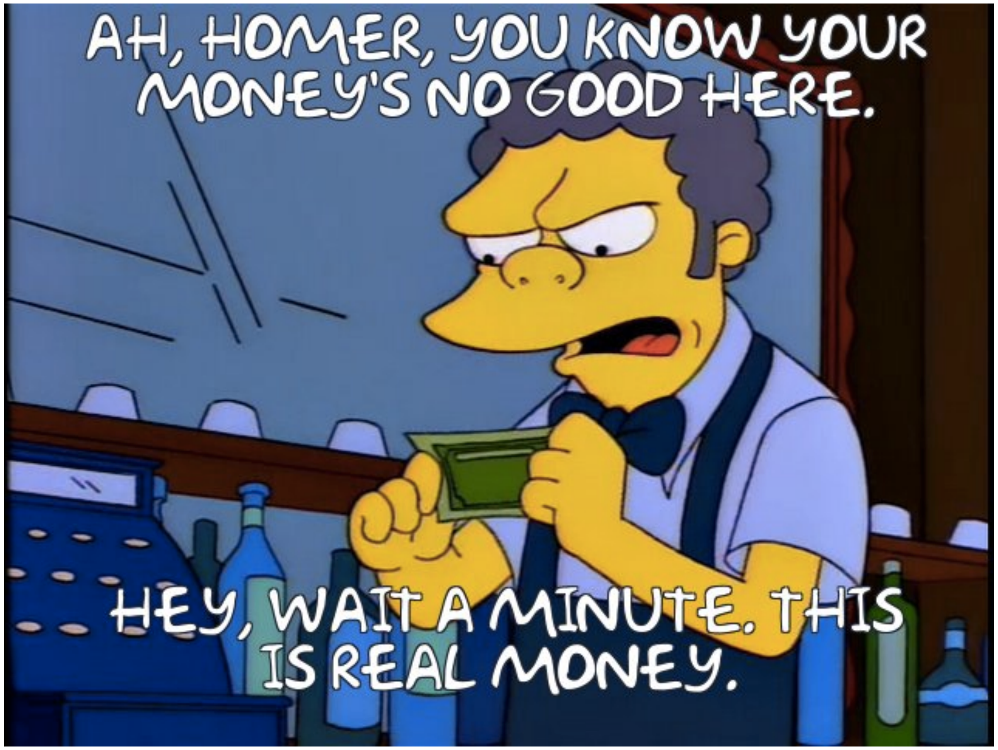


If you´ve woken up with this Pig, you´ve had a good night and left your credit card at the pub.

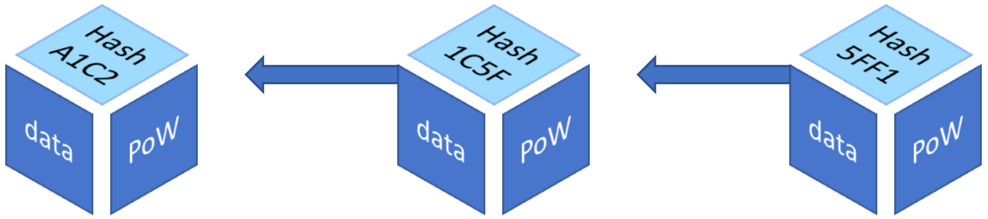
What if there is no trust?

- Pay Moe 100 bucks with credit card.
- Moe gives you an IOU for $95 and one beer.
- Want another beer? Update IOU to $90, get beer.
- At the end of the night, cash in the IOU.


Dear Homer
I.O.U.
one emergency
donut
Signed
Homer


AH, HOMER, YOU KNOW YOUR MONEY'S NO GOOD HERE.
HEY, WAIT A MINUTE. THIS IS REAL MONEY.

A blockchain always pays its debts



Payment channels: bar tabs for blockchains

Open/ Deposit

Pick a party you want to make payments with

- Escrow funds on the Blockchain under both your control.
- Get IOU for those funds.

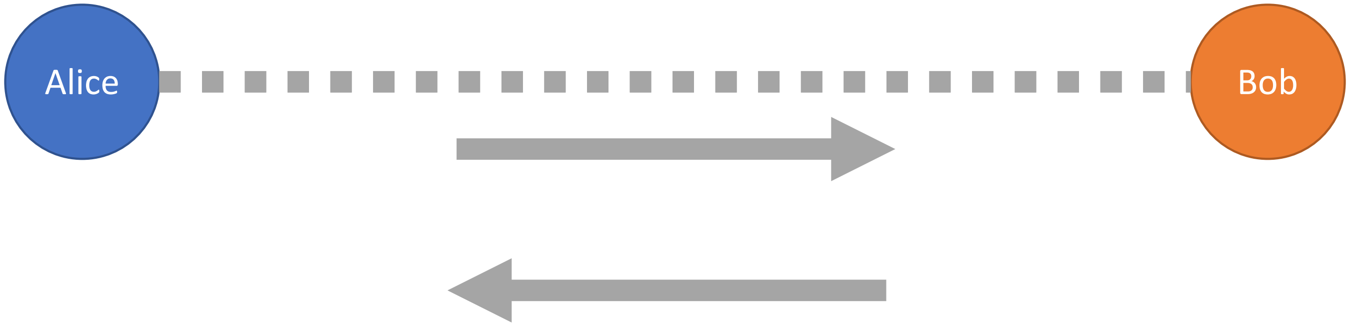
Transact

Make payments to and from counterparty by changing the balance on the IOU.

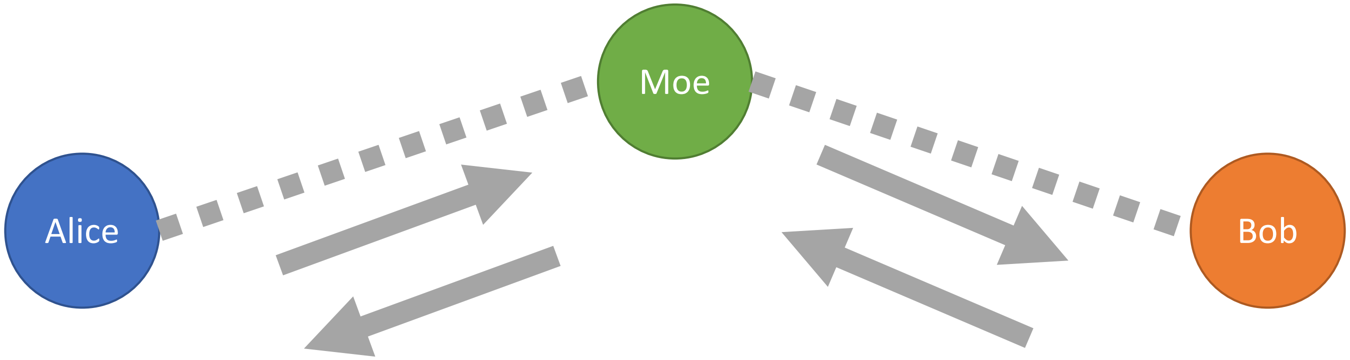
Close

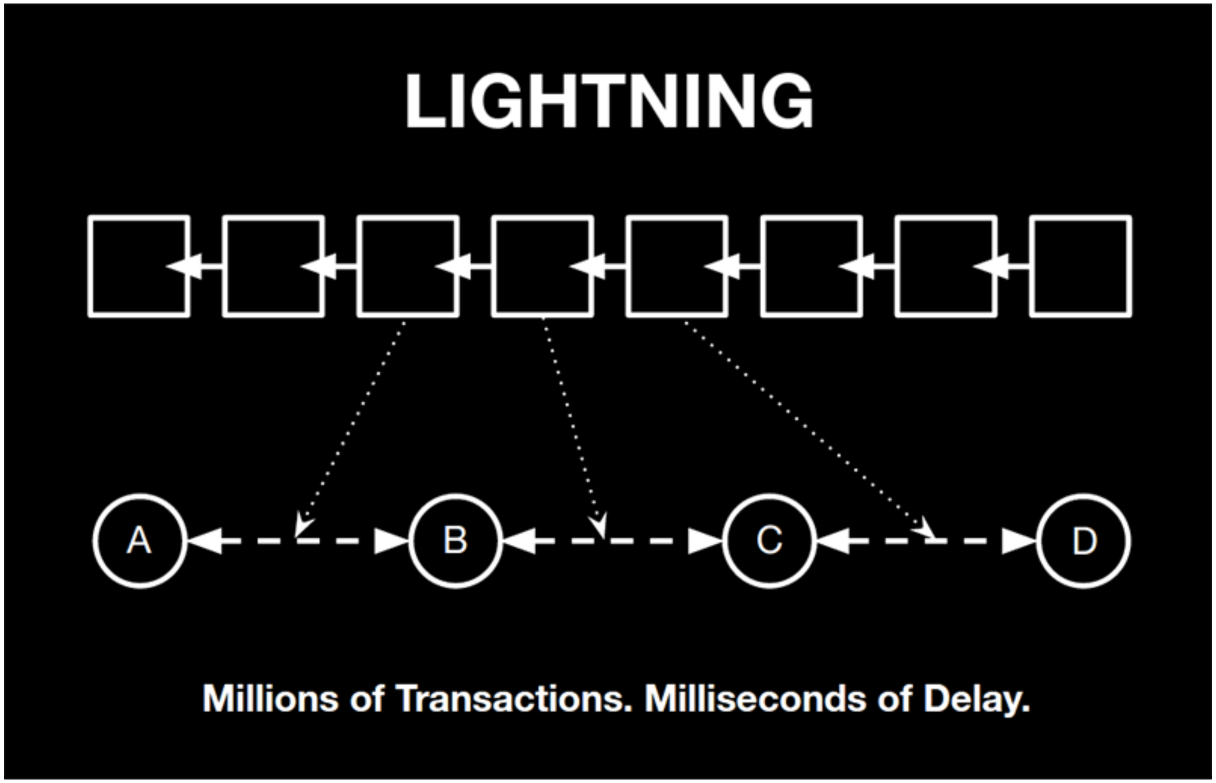
Use IOU to retrieve money from blockchain.

Payment channel



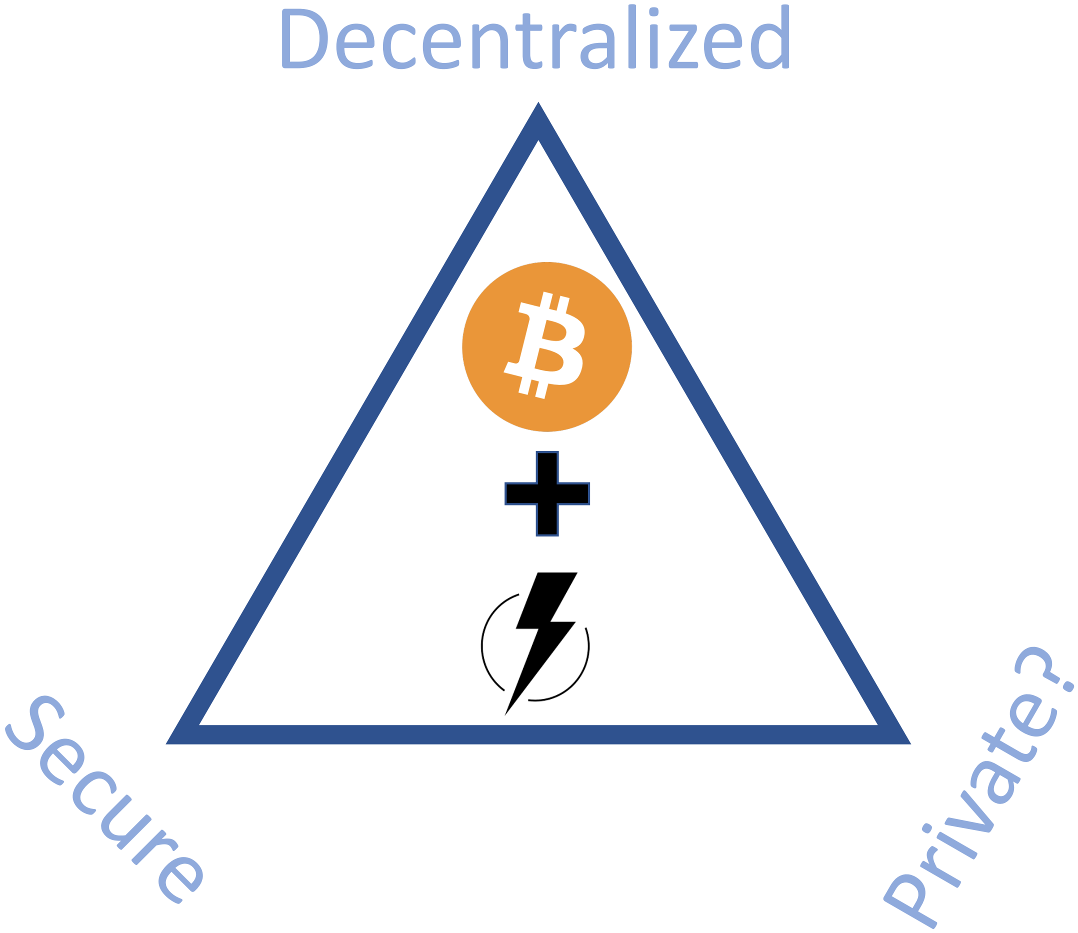
Payment channel network





LIGHTNING

Millions of Transactions. Milliseconds of Delay.



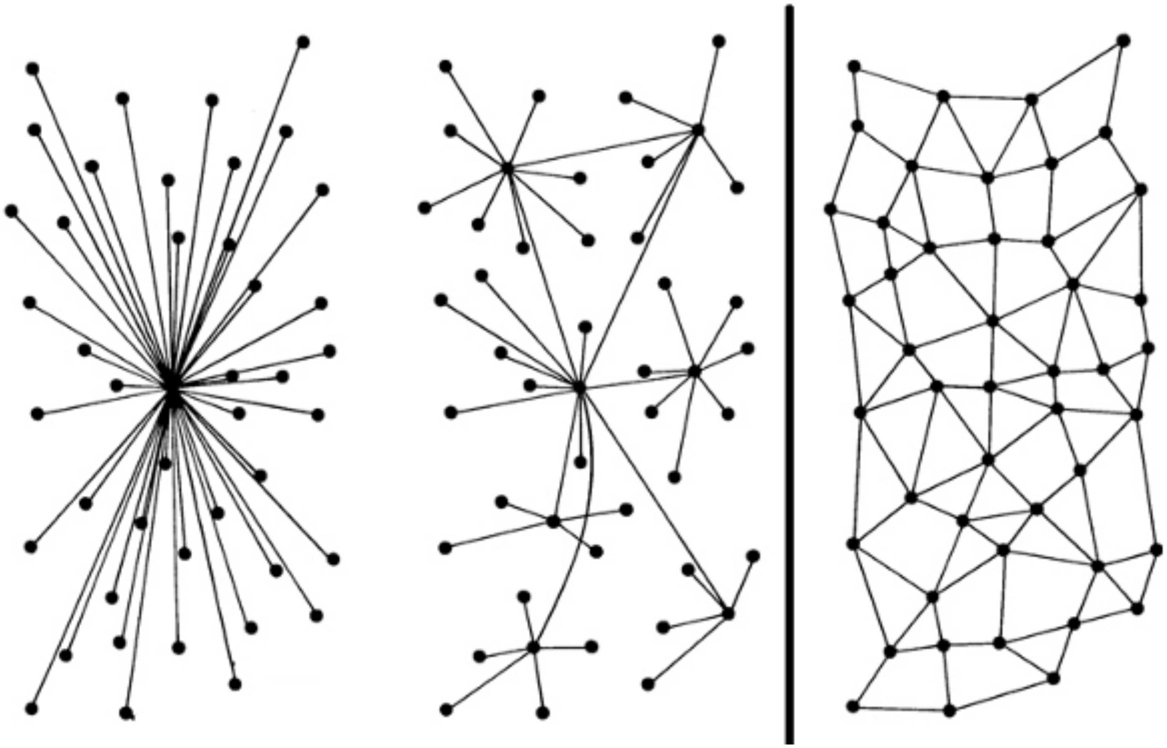
Decentralized

Secure

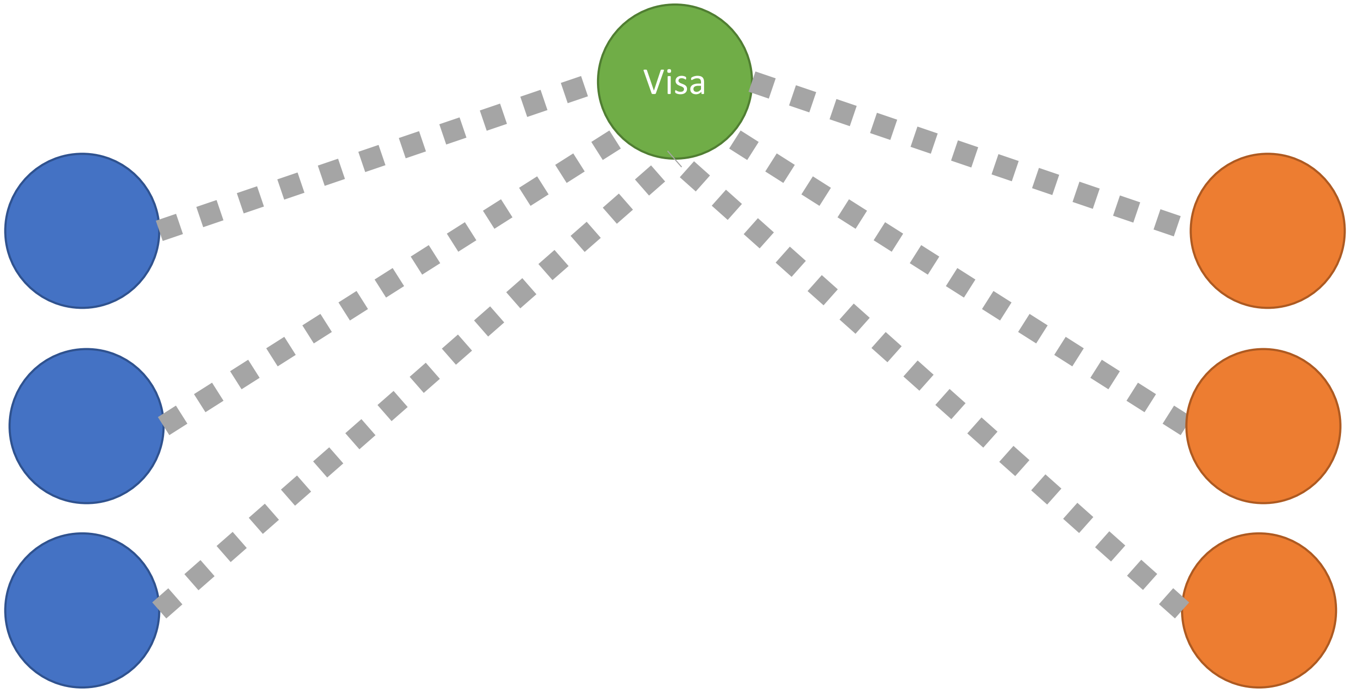
Private?

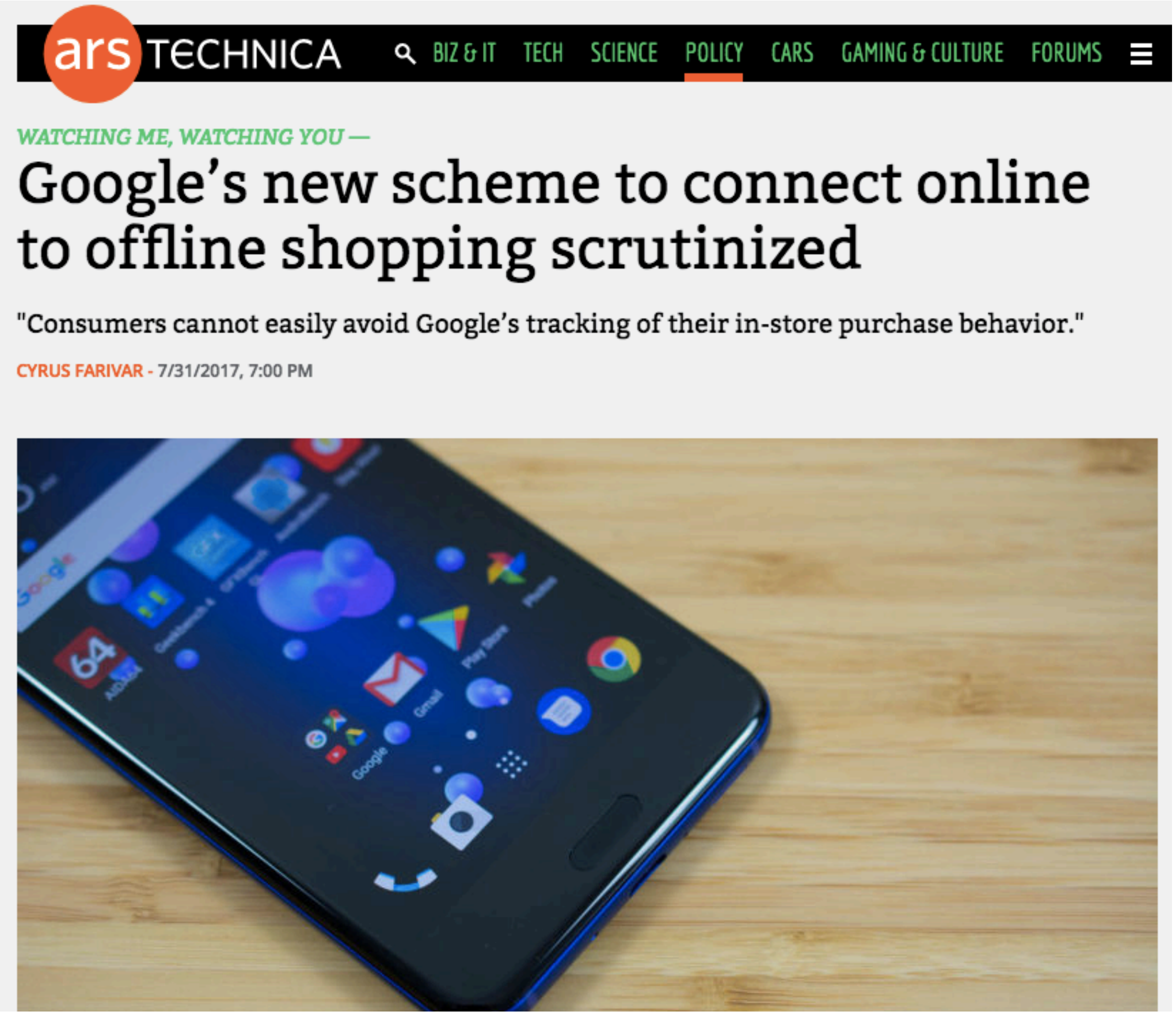
Privacy of payment channels

- For payment channels:
  - Payments on same channel are linkable, so cannot be used for:
    - Micropayments instead of advertising (e.g. Brave)
    - Tolls/subway tickets/WiFi access to avoid location tracking
    - Paying for anonymous messaging
    - Anything where you do not want to be identified to the seller
  - **Aggregate amount of payments leak to the network**
- For channel network:
  - Hub learns participants and amount.
  - Hub hides your identity from recipient and network. If you trust them…



Major issue: centralization





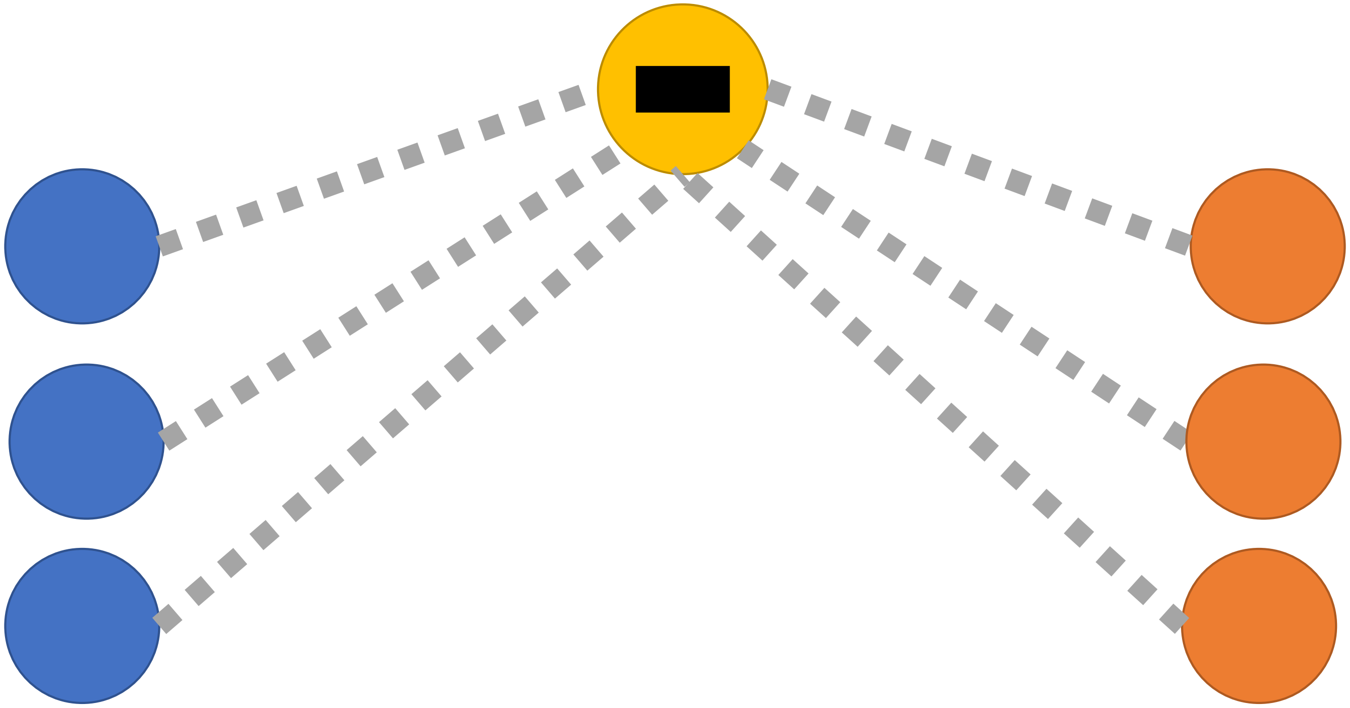
WATCHING ME, WATCHING YOU —

Google’s new scheme to connect online to offline shopping scrutinized

"Consumers cannot easily avoid Google’s tracking of their in-store purchase behavior."

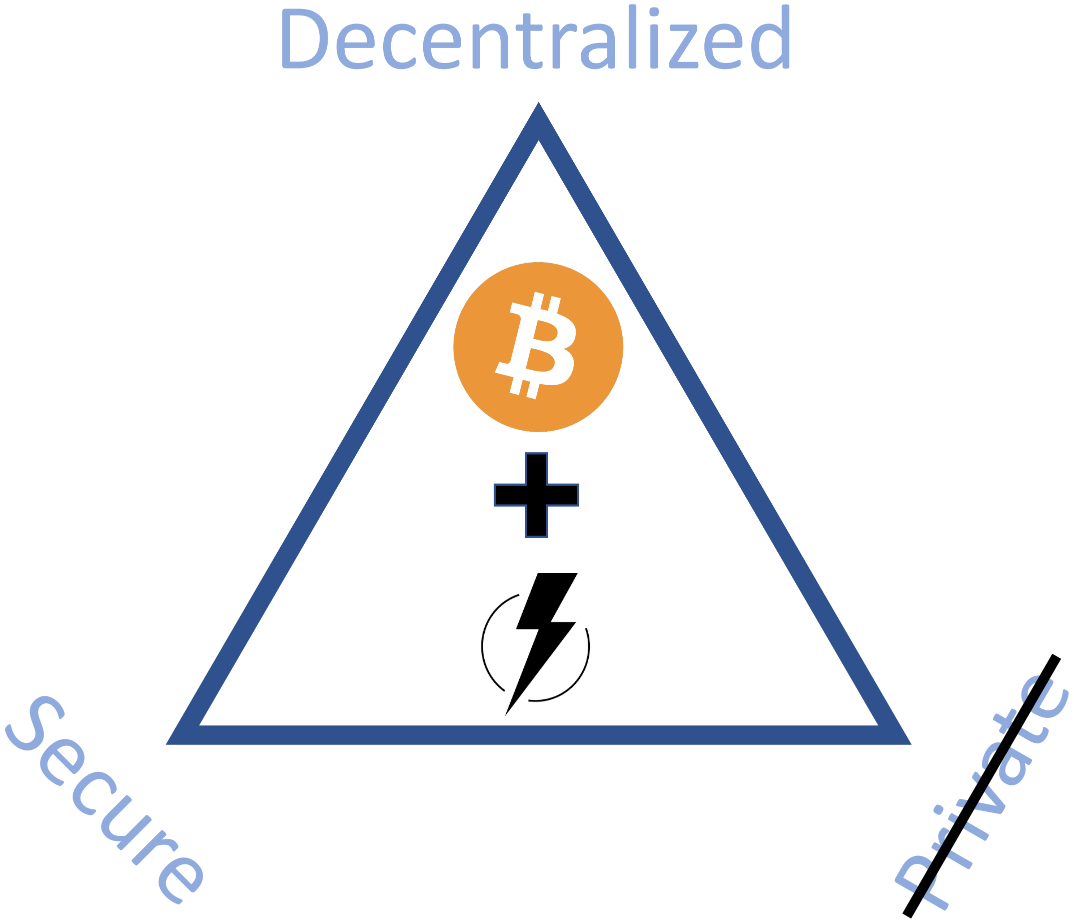
CYRUS FARIVAR - 7/31/2017, 7:00 PM

Major issue: centralization



Centralized lightning may be worse than Bitcoin privacy wise

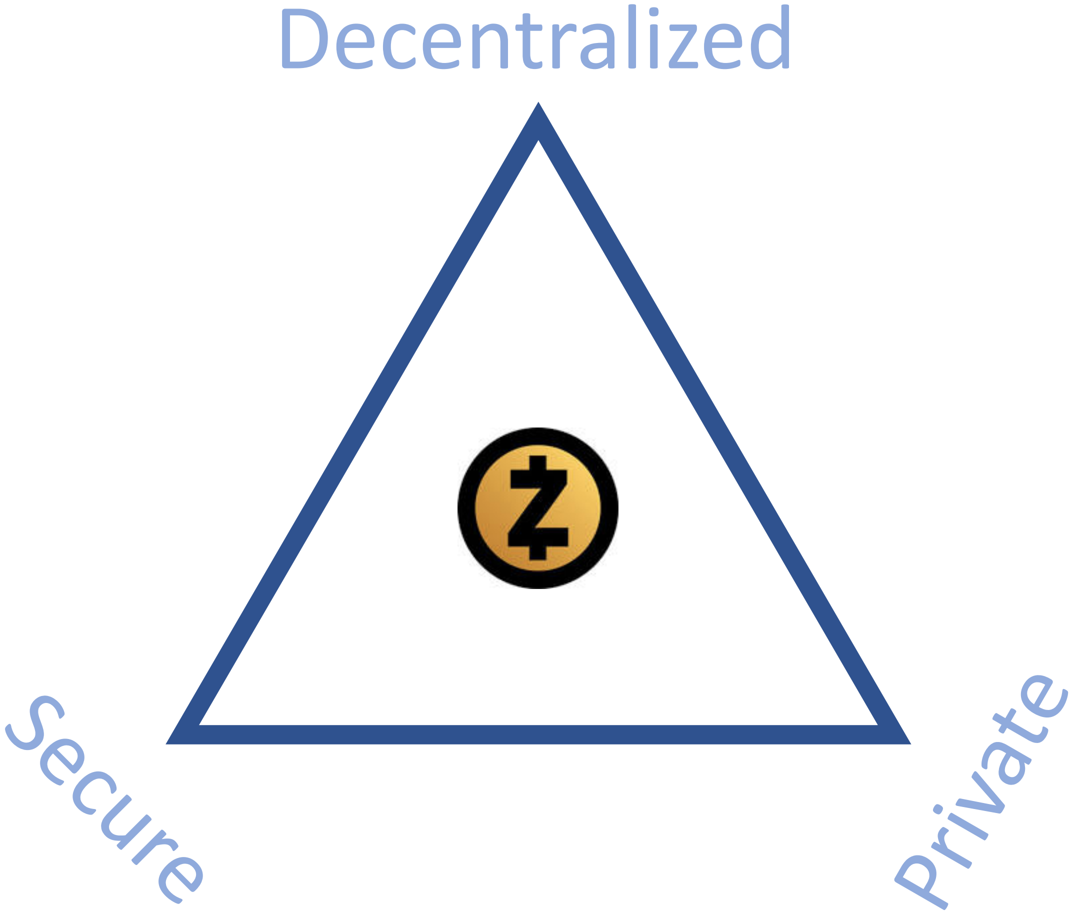
- Bitcoin:
  - Multiple identities for free
  - Identities are ephemeral
- Lightning:
  - Identities are costly (need to open new channel with escrowed money)
  - Identities are long lived
  - Hubs may have your real identity for AML/KYC
- Opening channels with anonymous funds does not solve this.



Decentralized

Secure

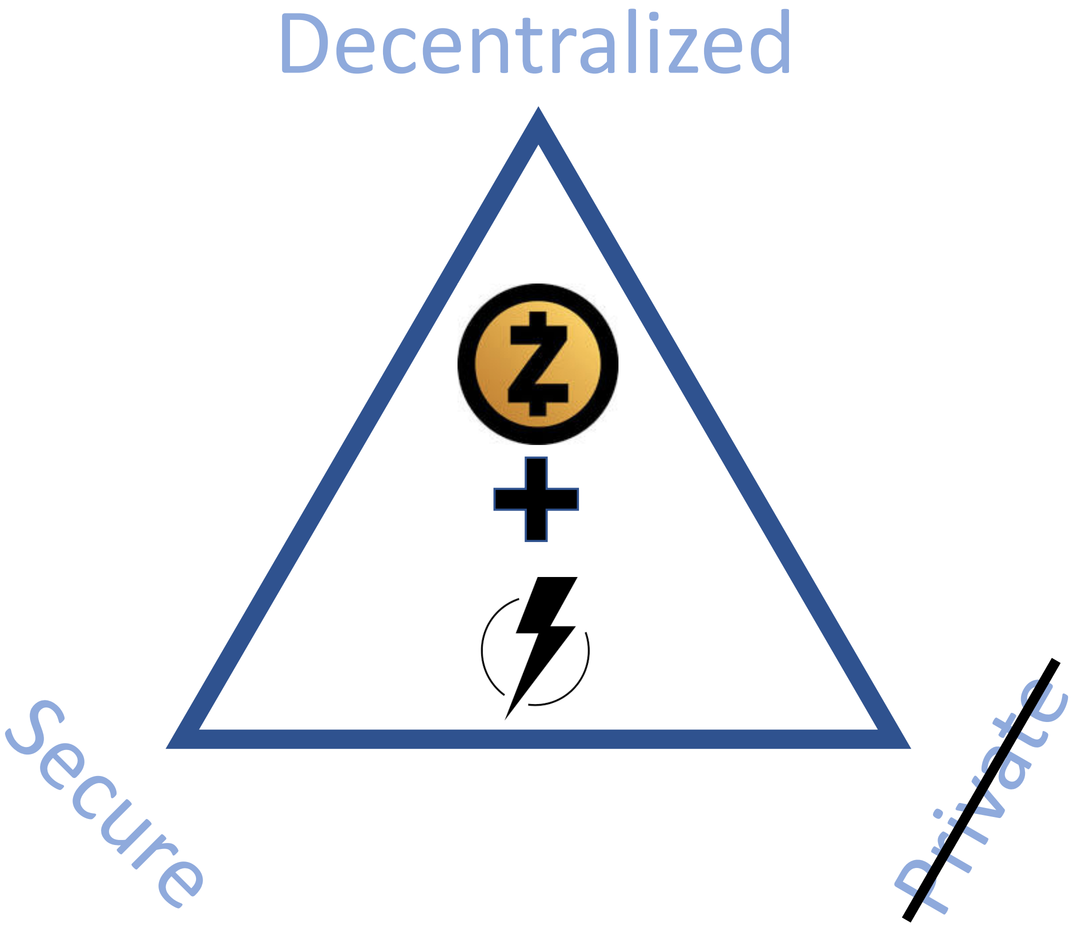
~~Private~~



Decentralized

Secure

Private



Decentralized

Secure

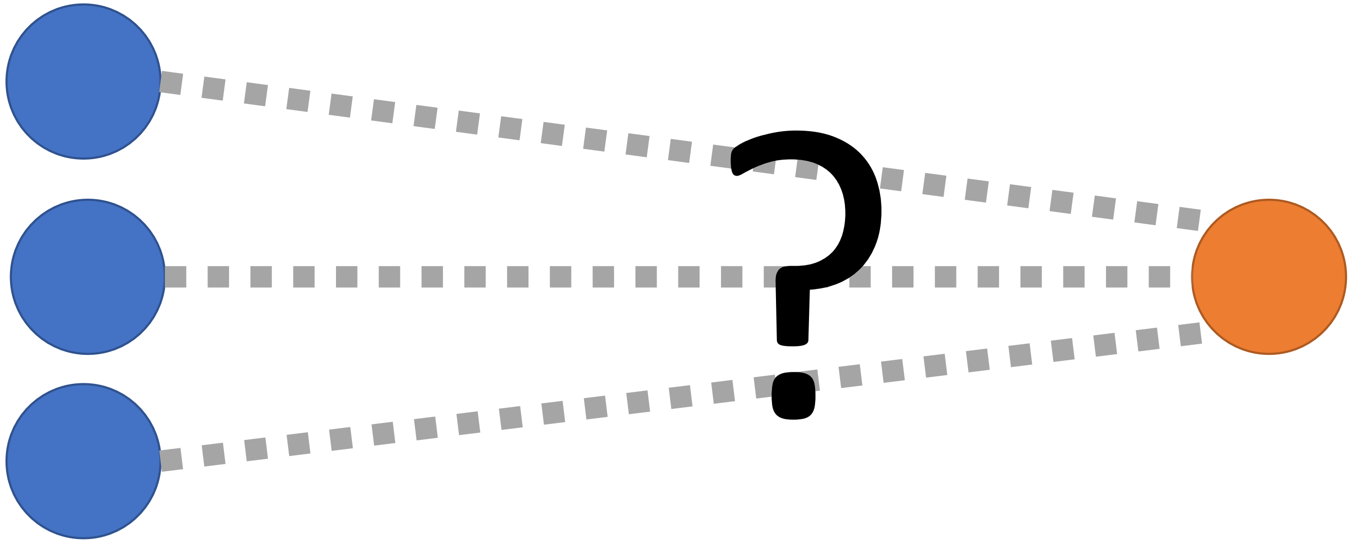
~~Private~~

Bolt: privacy for payment channels

A set of protocols for private payment channels:

- Unidirectional channels:
  - Alice can send fixed denominations of money to Bob after establishing a channel and escrowing funds
  - Based on compact e-cash
- Bidirectional channels:
  - Alice and Bob can exchange arbitrary values
  - Based on fair exchange, blind signatures, and zero-knowledge proofs
- Third party payments:
  - Bidirectional payments can be made indirectly
  - May hide payment value from intermediary

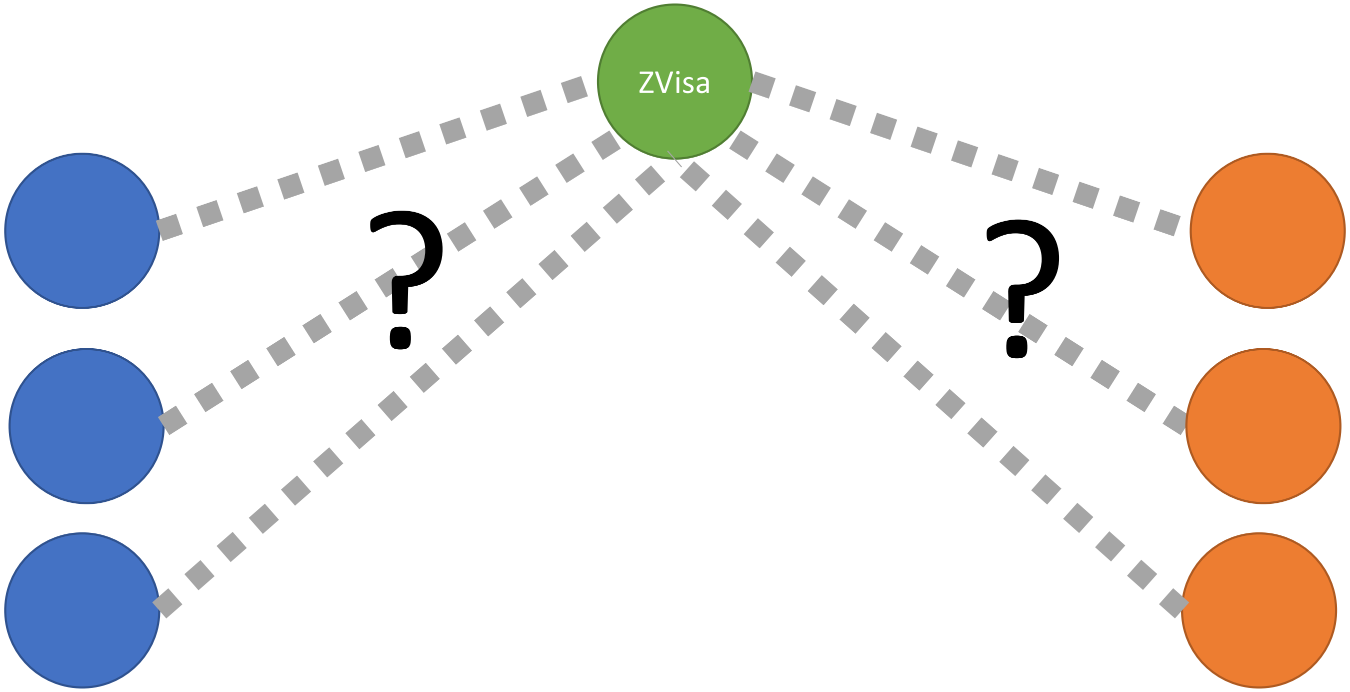
Privacy for channels



Customers

Merchant

Privacy for channel networks



The problem:

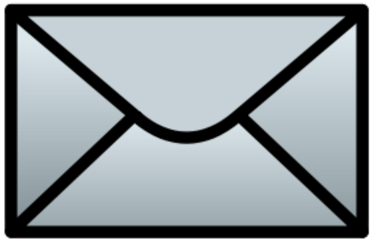
Exchange an IOU worth $100 for one worth $95 (and one beer). But:

- We cannot tell you the current IOU is worth $100
- We cannot tell you the new IOU is worth $95
- We cannot show you the IOU
- Yet somehow we must prove:
  - We do really have an IOU
  - The new one really is $5 less
- And that’s not even the hard part…..

Commitments

- Cryptographically opaque envelope
- Content cannot be opened by anyone but creator
- Cannot be changed by anyone

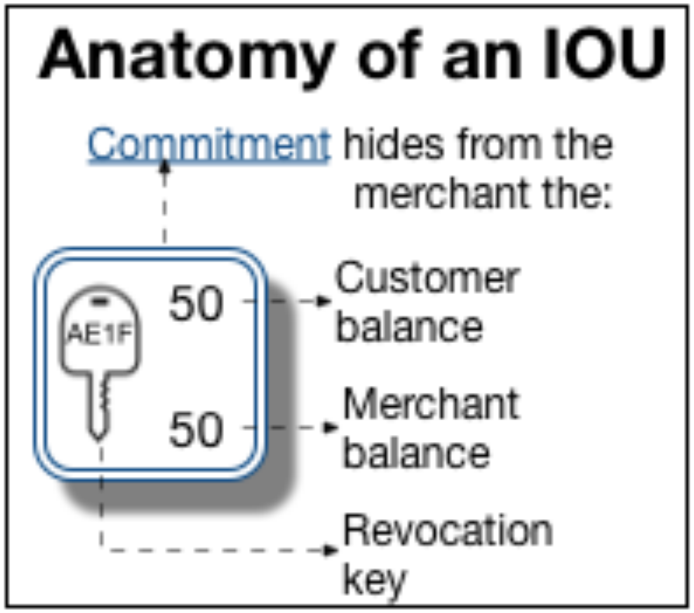
$$Comm(x; r) = g^x h^r$$



Zero-knowledge proofs π

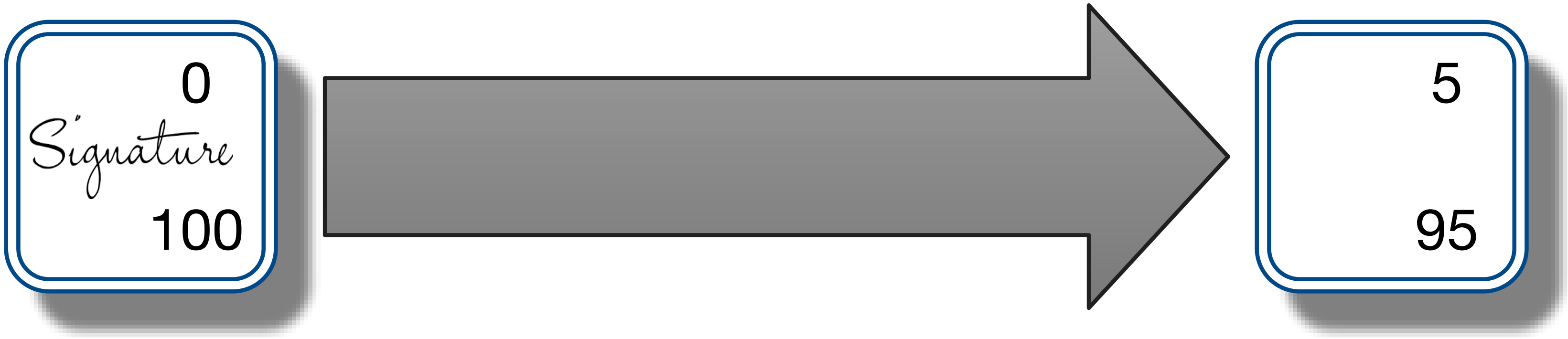
- Zero-knowledge [Goldwasser, Micali, & Rackof 1985]
- Lets you make statements about the content of commitments
- Sound: cannot be forged
- Zero knowledge: can keep secrets

The easy part: hiding the IOU

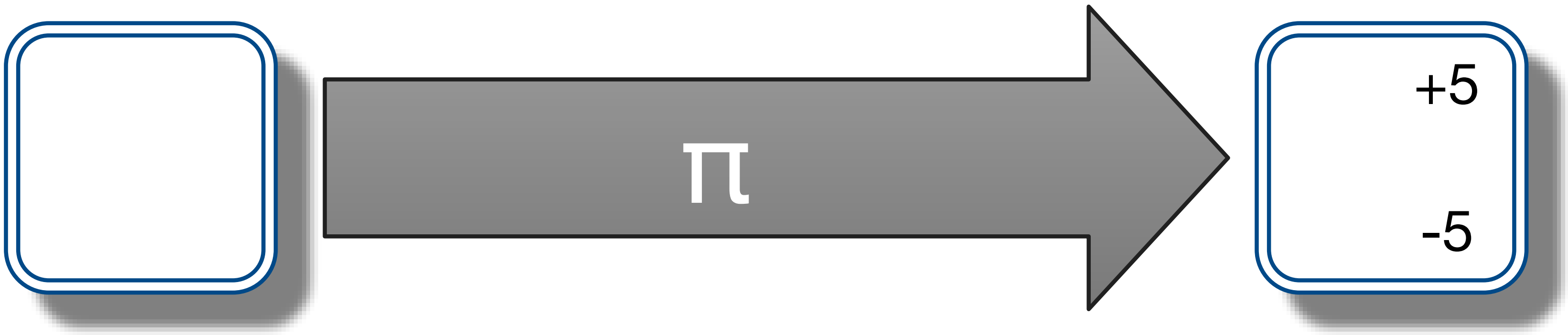

Anatomy of an IOU

Commitment hides from the merchant the:

- IOU is a commitment to
  - The customer’s balance
  - The merchant’s balance
  - A revocation key used to revoke the IOU
  - Signature by the merchant for validity
- Use zero-knowledge proof to prove:
  - You have a commitment/IOU
  - It is signed by the merchant
  - Your new IOU is for Δ more/less e.g. $4 less for a beer



Can you
please sign?



“This is signed”

“Can you
please sign this
related thing?”

The hard part

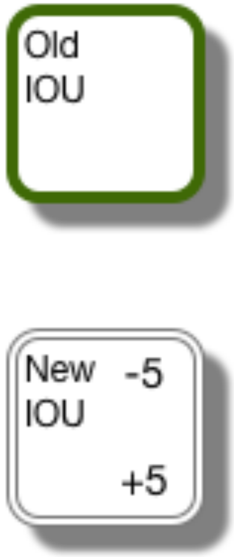
- Both IOUs cannot be valid at same time
  - If Moe issues new IOU and beer first, Homer can cash out old IOU. Free beer.
  - If Homer invalidates old IOU, Moe can not issue a new one and keep the money.
- Seemingly need to atomically swap
  1. Moe’s signature on the new IOU
  2. Homer’s signature revoking the old IOU
- Fair exchange of signatures is impossible!!!!

Solution: all IOUs are not the same

- IOU serves two functions:
  - A way to cash out and get your money from the blockchain
  - A way to make another purchase
- An IOU need not always be valid for both roles at the same time
- Alice can safely give up her ability to buy more using an IOU
- Bob can safely sign a new IOU for $95 even if Alice holds an IOU for $100 (he just can’t give her the beer yet)

Customer

① Prove new IOU pays merchant $5 more than some signed old IOU

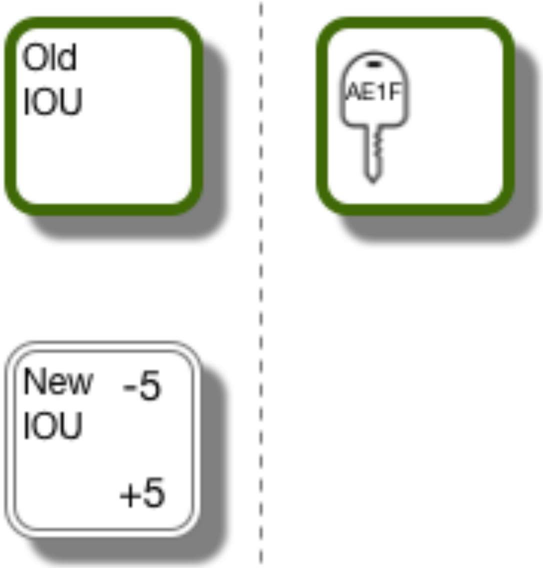


merchant

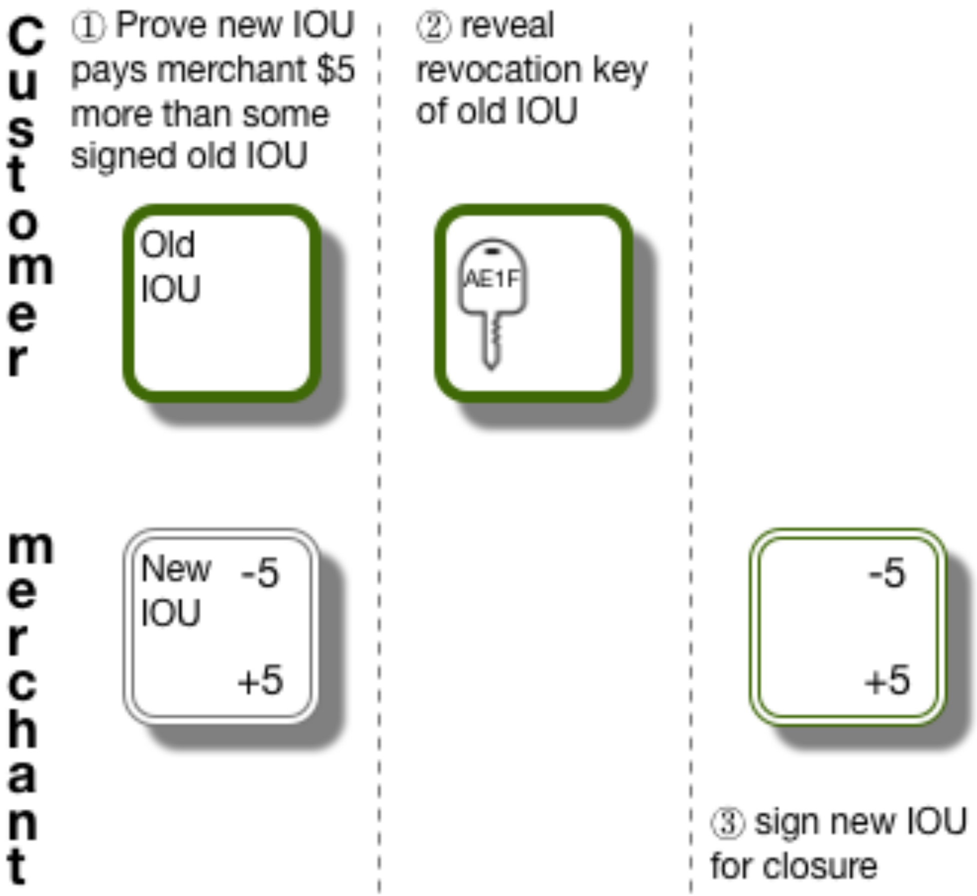
Customer

① Prove new IOU pays merchant $5 more than some signed old IOU

② reveal revocation key of old IOU



merchant



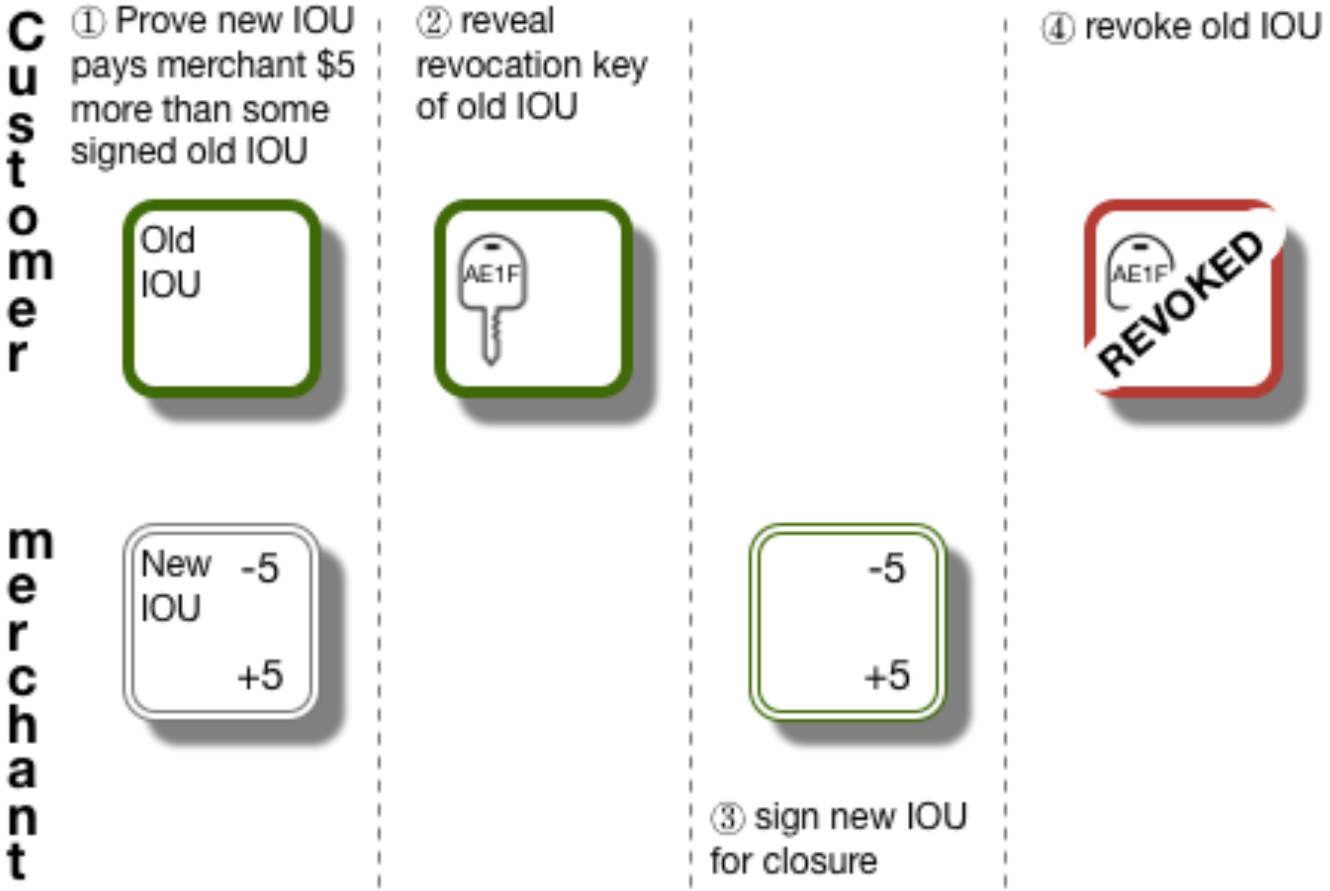
Customer

merchant

① Prove new IOU pays merchant $5 more than some signed old IOU

② reveal revocation key of old IOU

③ sign new IOU for closure



Customer

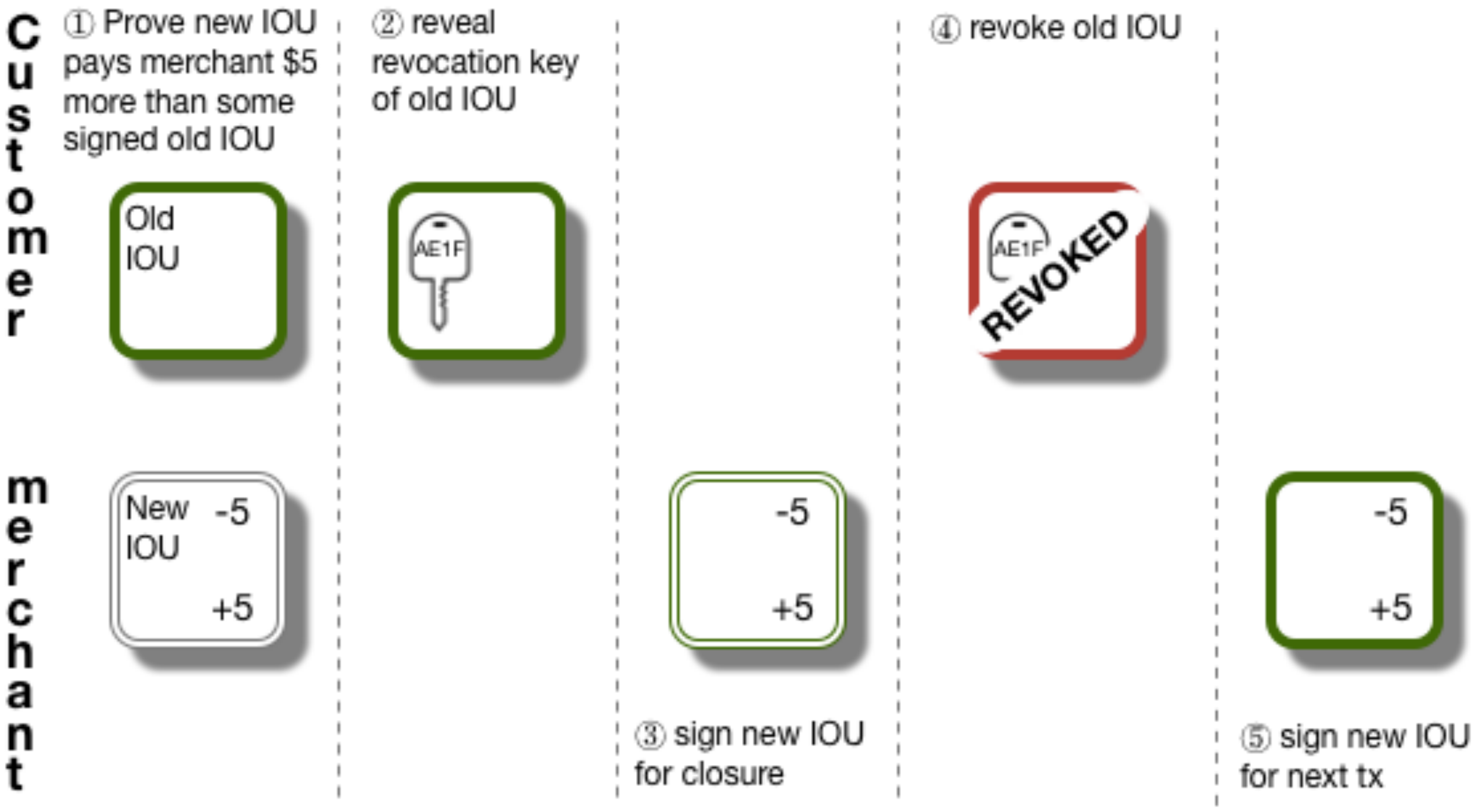
merchant

① Prove new IOU pays merchant $5 more than some signed old IOU

② reveal revocation key of old IOU

③ sign new IOU for closure

④ revoke old IOU



① Prove new IOU pays merchant $5 more than some signed old IOU

② reveal revocation key of old IOU

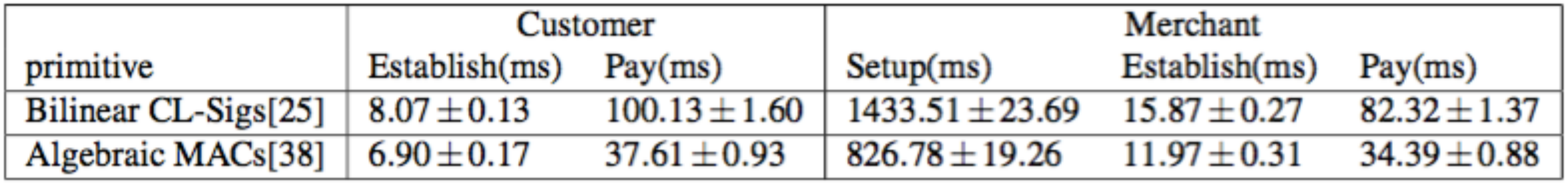
③ sign new IOU for closure

④ revoke old IOU

⑤ sign new IOU for next tx

Some performance numbers

- Various primitives can be used.
- One time setup to establish a channel can take 1 to 2 seconds.
- But payments take less than 100ms per hop.
- No zkSNARK style trusted setup.
- Can be done with well established cryptography.



	Customer		Merchant		
primitive	Establish(ms)	Pay(ms)	Setup(ms)	Establish(ms)	Pay(ms)
Bilinear CL-Sigs[25]	8.07 ± 0.13	100.13 ± 1.60	1433.51 ± 23.69	15.87 ± 0.27	82.32 ± 1.37
Algebraic MACs[38]	6.90 ± 0.17	37.61 ± 0.93	826.78 ± 19.26	11.97 ± 0.31	34.39 ± 0.88

Extensions

- Can do payment networks over multiple hops
  - Hides participants from each other and intermediaries
  - Hides everything from the blockchain
- Can do channels for state beyond monetary balances. Useful for a private version of Ethereum.
- Can remove any exotic cryptography from the blockchain
  - All exotic crypto is off chain
  - Only standard signatures and commitment openings are validated on chain
  - Adds one more round trip in the protocol

Comparison to related work

		Compatibility	Privacy from hub?	Privacy from Counter party?	Payments in either direction?	Variable valued payments?
Lighting + anon HTLCs		Bitcoin	**No**	**No**	Yes	Yes
Tumblebit		Bitcoin	Yes	**No**	**No**	**No**
Bolt	unidirectional	(new opcode) Bitcoin/Zcash	Yes	Yes	**No**	Yes
	Bi directional	**(new opcode) Zcash or Bitcoin + strong privacy**	**Yes**	**Yes**	**Yes**	**Yes**

Deployment options

- Can be deployed by adding an op code to Zcash (or Bitcoin[1])

- [1]Bidirectional channels require strongly anonymous money to fund the channel. (unidirectional channels do not)

Bolt: provably secure strongly private payment channels

Questions?