Theory of Blockchain

Session 8:

Bitcoin – Part 3

Module 2 – Bitcoin Lightning Network

Bitcoin's Blockchain Unscalability

1,700 TXs per Second

7 TXs per Second

Bitcoin's TPS = 7

Block size = 1MB

Average transaction size = 250 B

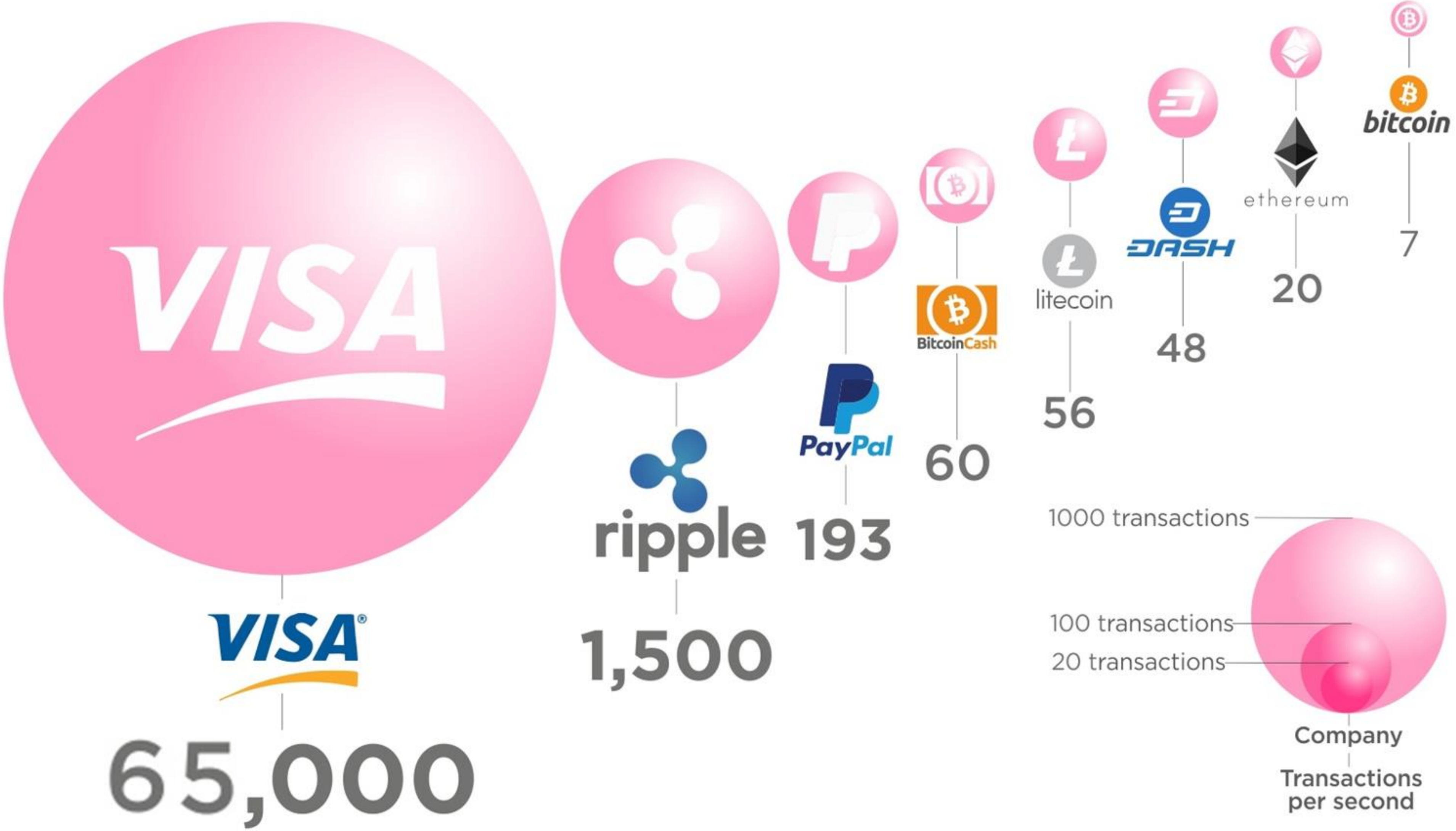
1 block every 10 mins in average

The VISANet transaction rate could reach up to 47 thousand per second before the Christmas holidays.

Blockchain: 1 TB (Daily)

Live Transactions (May 24, 2016) – blockchain.info (blockchain.com now)

Cryptocurrencies Transaction Speeds Compared to Visa & Paypal

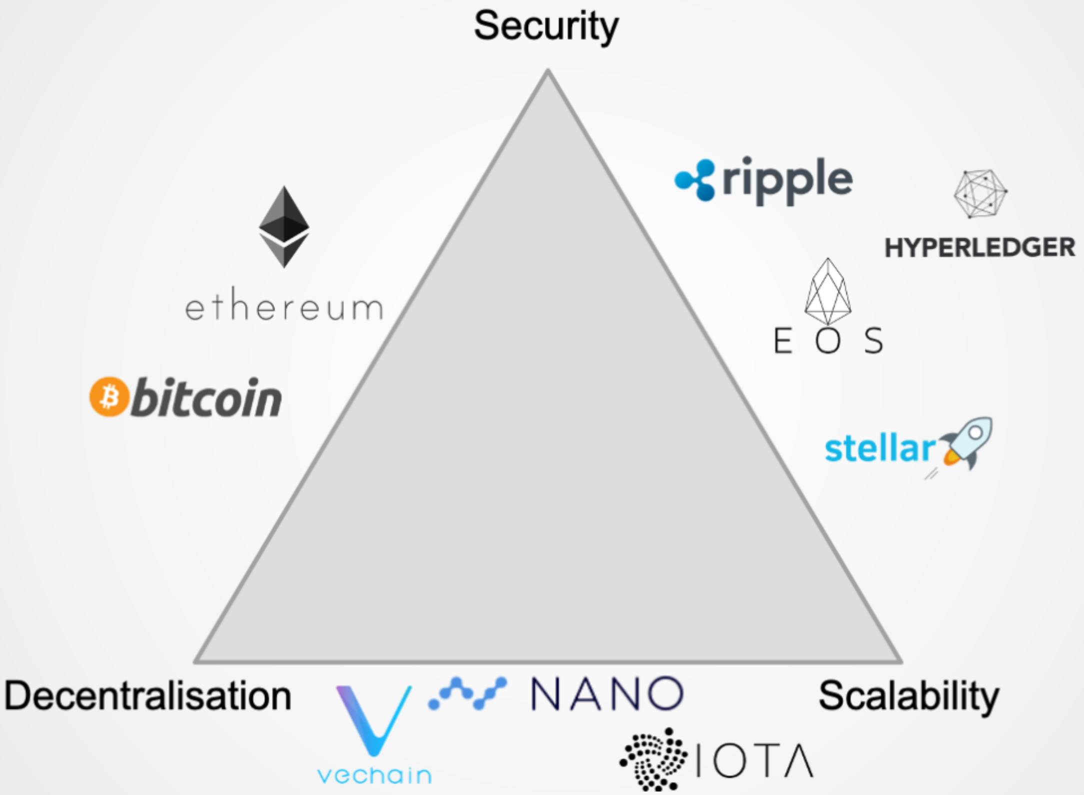


Article & Sources:
https://howmuch.net/articles/crypto-transaction-speeds-compared
https://howmuch.net/sources/crypto-transaction-speeds-compared

howmuch net

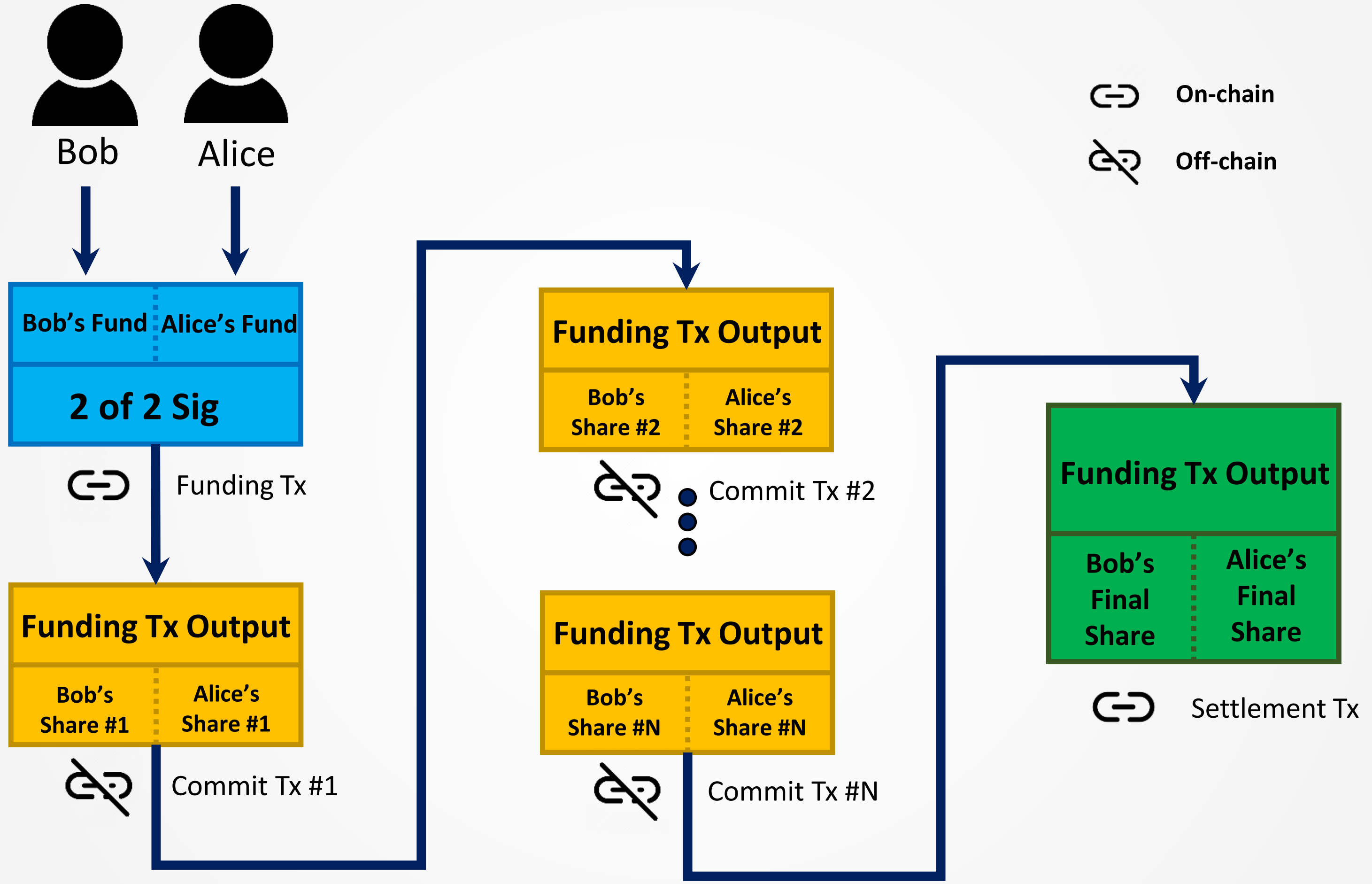
Source: howmuch.net

Blockchain Scalability Trilemma



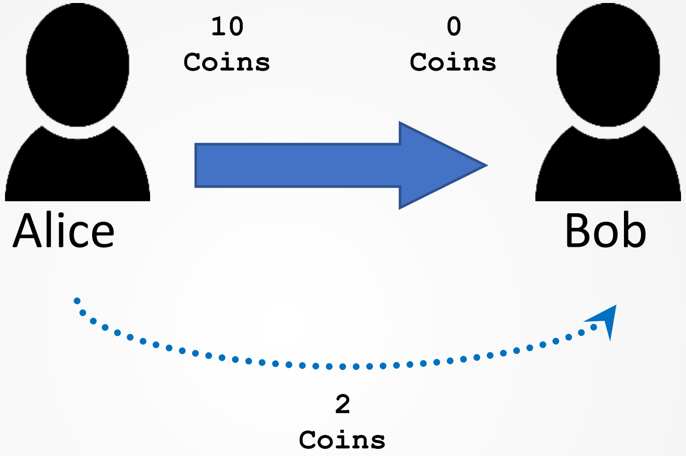
Source: fingo.net

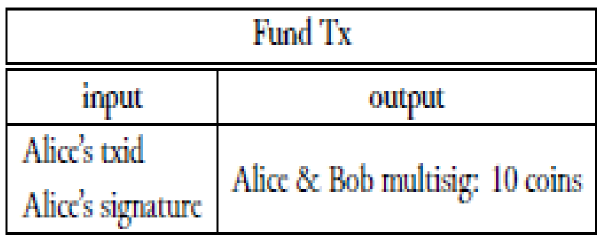
Off-chain Payment Channel



The input of all commitment transactions is the output of "Fund" Trans.

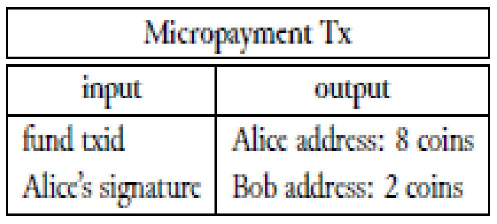
One-way Channel Example





Fund Tx	
input	output
Alice's txid Alice's signature	Alice & Bob multisig: 10 coins

Funding Tx

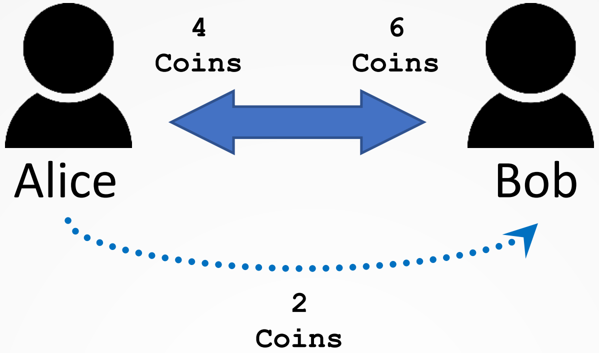


Micropayment Tx	
input	output
fund txid	Alice address: 8 coins
Alice's signature	Bob address: 2 coins

Micropayment Tx

Source: MAS.S62, Thaddeus Dryja

Two-way Channel



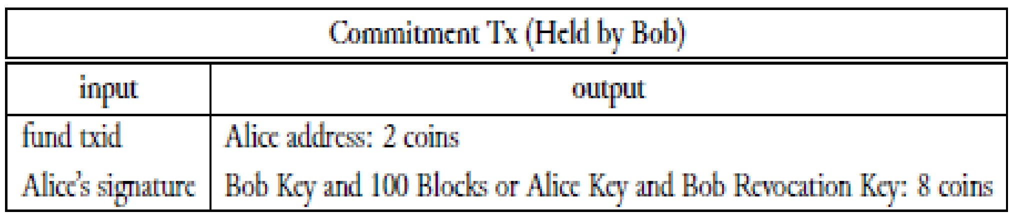
4 Coins

6 Coins

Alice

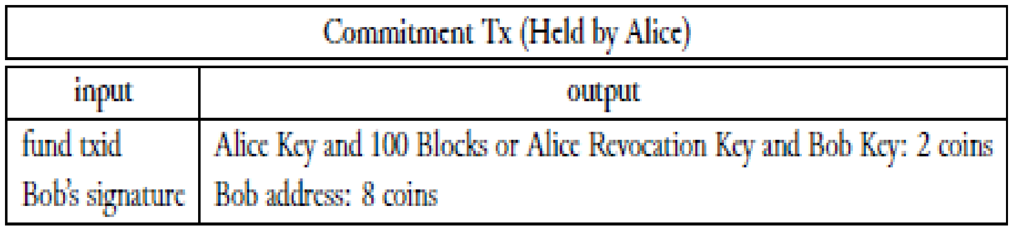
Bob

2 Coins



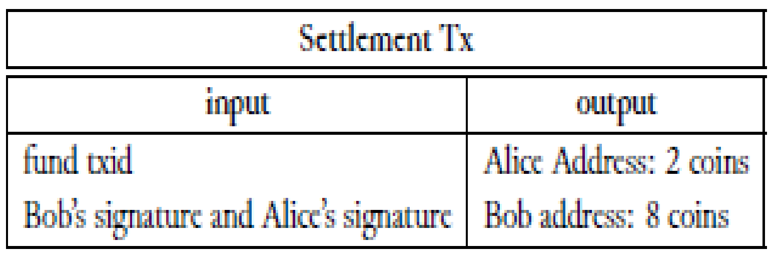
Commitment Tx (Held by Bob)	
input	output
fund txid	Alice address: 2 coins
Alice's signature	Bob Key and 100 Blocks or Alice Key and Bob Revocation Key: 8 coins

Commitment Tx Held by Bob



Commitment Tx (Held by Alice)	
input	output
fund txid	Alice Key and 100 Blocks or Alice Revocation Key and Bob Key: 2 coins
Bob's signature	Bob address: 8 coins

Commitment Tx Held by Alice

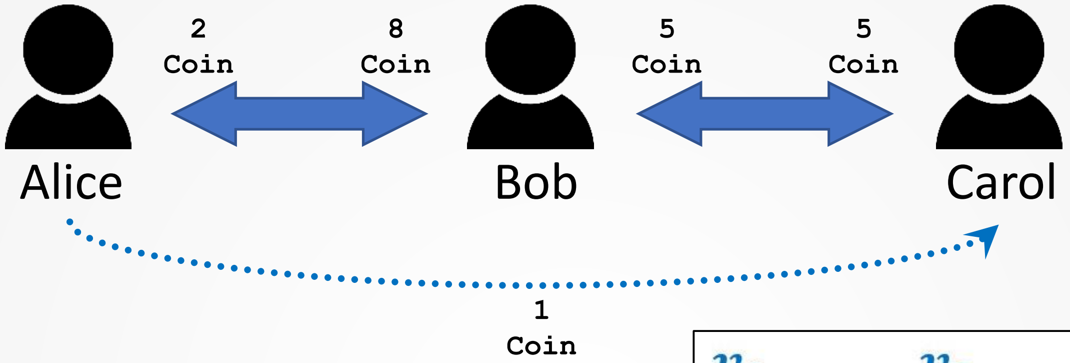


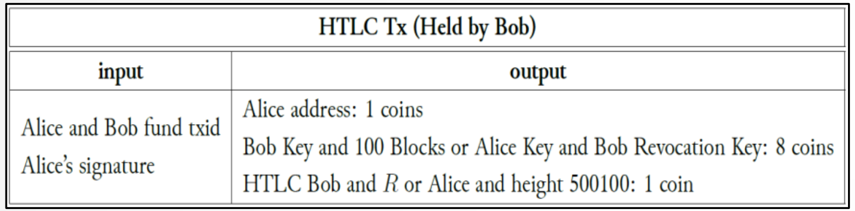
Settlement Tx	
input	output
fund txid	Alice Address: 2 coins
Bob's signature and Alice's signature	Bob address: 8 coins

Settlement Tx Held by Bob

Source: MAS.S62, Thaddeus Dryja

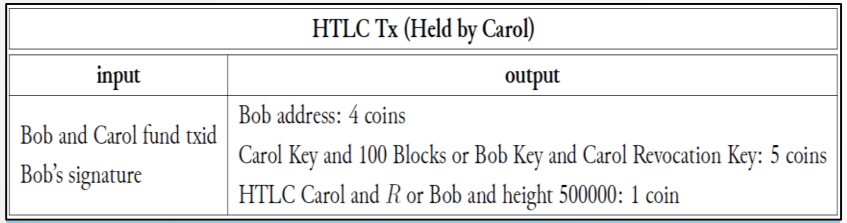
Multi-hop Channel via HTLC





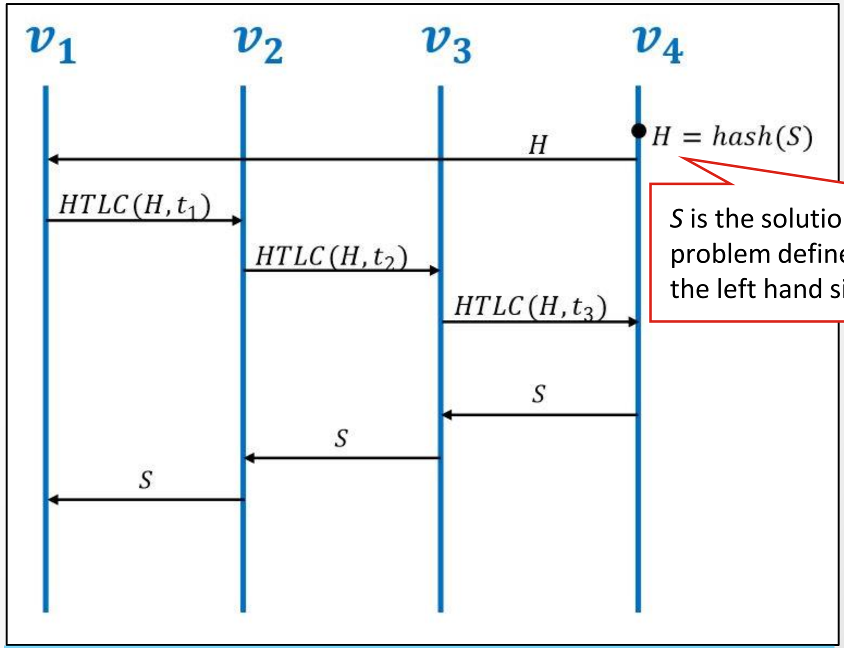
HTLC Tx (Held by Bob)	
input	output
Alice and Bob fund txid Alice's signature	Alice address: 1 coins Bob Key and 100 Blocks or Alice Key and Bob Revocation Key: 8 coins HTLC Bob and R or Alice and height 500100: 1 coin

HTLC Tx Held by Bob



HTLC Tx (Held by Carol)	
input	output
Bob and Carol fund txid Bob's signature	Bob address: 4 coins Carol Key and 100 Blocks or Bob Key and Carol Revocation Key: 5 coins HTLC Carol and R or Bob and height 500000: 1 coin

HTLC Tx Held by Carol

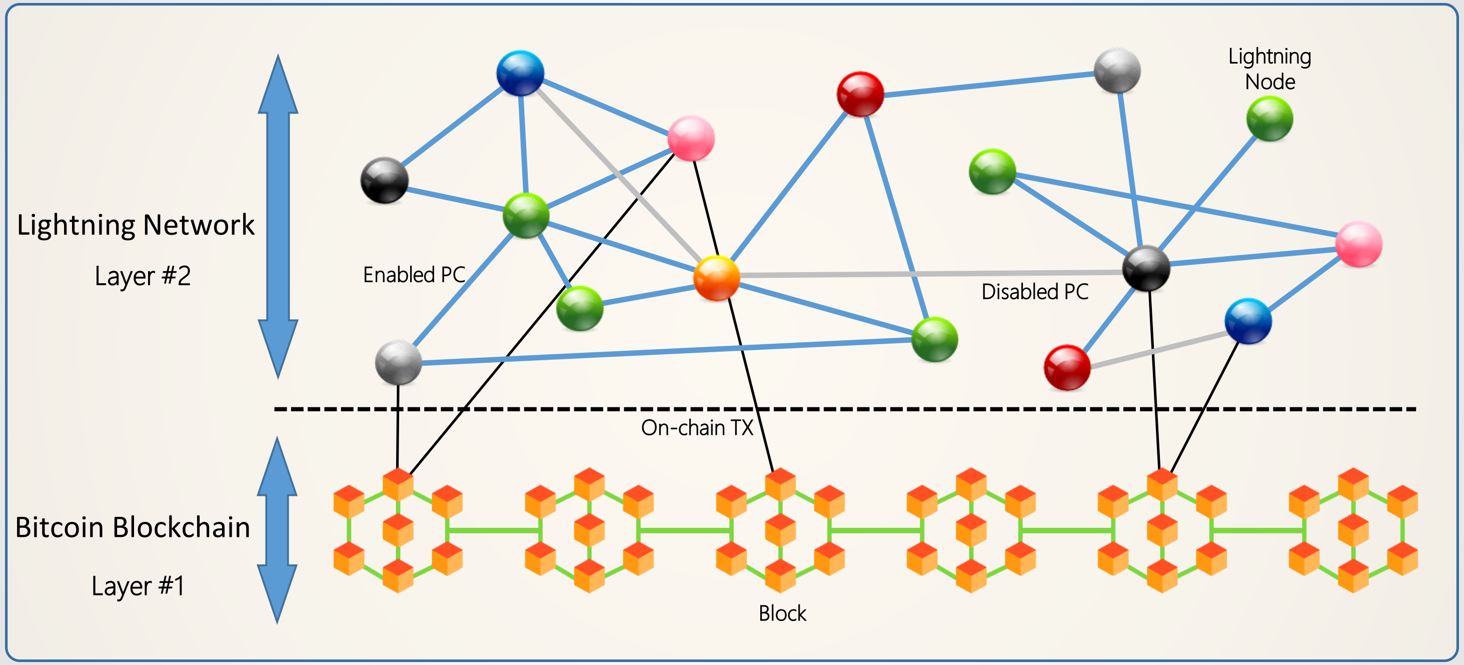


S is the solution to the preimage problem defined by *H* (similar to *R* in the left hand side transaction)

Multi-hop Payment Settlement Process

Source: MAS.S62, Thaddeus Dryja

The Lightning Network



Use Cases

New revenue models for content creators in the media industry

Tipping in social media

More privacy in online payment and sending money to friends

Source: Medium, Lucas Tatge

Use Cases

Vending machines

Car-to-X communication

API services payments

Source: Medium, Lucas Tatge

What Comes Next …

- We saw how off the chain transactions are handled in Bitcoin Lightning Network.

- We listed some potential applications of Lightning Network.

- We introduce wallets in the next module.

See you in the next module …