The Lightning Network

Machine-to-machine Payments

Leonhard A. Weese
Co-founder, Bitcoin Association of Hong Kong
leo@bitcoin.org.hk

Hong Kong, 7 November, 2020

Bitcoin

Decentralized, open and free global financial network

- Slow (~10 min block intervals)
- Expensive (~HK$2-30)
- Limited capacity (~4-7 tx/s)
- Volatile exchange rate (~2% per hour)

Blockchain

- Does not scale
- Broadcast model
- High external costs (Memory, bandwidth, computing power)

  - > Dangerous conflicts between throughput and decentralization

A New Network

- Bitcoin as the settlement layer
- Lightning as the payment layer
- Scaling without compromising the security of the base layer
- Lightning is not a Blockchain!

Bitcoin Transaction

2018-10-10 16:40

tx: **hgb710f470dd3df348fc99fbf9c148b**

from: **fb9c6b8dad6094a9b7bf0438eb223e**

to: **12CJg4sxZHgPLrVHxk7p7o4s5f286G9iim**

amount: 12.5 Bitcoin signature: *Alice*

The Signatures of Alice and Bob are needed to spend these outputs

- Every transaction references a previous transaction
- Every transaction is signed
- Complicated rules can be defined
  (→ Smart Contracts)

UTXO

c5794a0cb767da69c40e3a5c1f6c91f148093e414817235bb96cf5fdb6989e79

DETAILS +

#0 0b904cb40312ac64fca38b3153888ce4ebc0c31e297b0c9458235942310a1282:1 0.02565229 BTC

#0 1JFKkqMPMYYphtuQ6vE2DFB5badAMadWZj 0.00965673 BTC

#1 1PfjwEH8qLX9zERnWCYn9Jk8pDuHLxs5Jg 0.01592806 BTC

1 CONFIRMATION 0.02558479 BTC

19a7e5a6c732f804afb8bef8873cdab34da718997a256d081f700f5cebbbac99

DETAILS +

#0 f2e605501203ca46f42e8f072e2de73376ce89638da8bb6d0b1fa893877a0e95:2 0.0002772 BTC

#1 bf257408f3af2c64612b03a46d237c2a7dd41303c63e40ec559c66194d4365bc:0 0.00890611 BTC

#0 32zPw8474HqYvnjRNRCbS7XQ3BL9YrW4oC 0.00914613 BTC

1 CONFIRMATION 0.00914613 BTC

Payment Channel

2018-10-10 16:40

tx: **hgb710f470dd3df348fc99fbf9c148b**

from: **fb9c6b8dad6094a9b7bf0438eb223e**

to: **bc1qtnsyw9d78dnf9j8p2rhnvj2fx6ukmya6xqfcxl**

amount: 1 Bitcoin signature: ~~~

The Signatures of Alice and Bob are needed to spend these outputs

1) Payment Channel is being opened
1 BTC is sent to a 'multisig' address
Alice and Bob control this address together

Payment Channel

2018-10-10 16:40

tx: **hgb710f470dd3df348fc99fbf9c148b**

from: **fb9c6b8dad6094a9b7bf0438eb223e**

to: **bc1qtnsyw9d78dnf9j8p2rhnvj2fx6ukmya6xqfcxl**

amount: 1 Bitcoin

signature: ~~~

The Signatures of Alice and Bob are needed to spend these outputs

2) Alice only signs her transaction after she receives Bob's signature on a refund transaction. This way her funds can't be stuck.

2018-10-10 16:40

tx: **283e4f581e1bb73d8d47a5072471f7**

from: **hgb710f470dd3df348fc99fbf9c148b**

to: **bc1qsrr3pv86v8ftxh8nmgrdt9rda7vl4p6ts2nzcg**
amount: **1 Bitcoin**

to: **bc1qj93n553npnsumygn4sqfch9qlkv54u82sjxzdf**
amount: **0 Bitcoin**

signature: *Bob*

The Signatures of Alice and Bob are needed to spend these outputs. This money can only be spent two days after this transaction is confirmed unless the secret to hash 2325005714a7 is revealed.

LOCAL MEMORY

Payment Channel

2018-10-10 16:40

tx: **hgb710f470dd3df348fc99fbf9c148b**

from: **fb9c6b8dad6094a9b7bf0438eb223e**

to: **bc1qtnsyw9d78dnf9j8p2rhnvj2fx6ukmya6xqfcxl**

SETTLED

amount: 1 Bitcoin

signature: *Alice*

The Signatures of Alice and Bob are needed to spend these outputs

2) Alice signs both transactions, but keeps the second transaction in her local memory

2018-10-10 16:40

tx: **283e4f581e1bb73d8d47a5072471f7**

from: **hgb710f470dd3df348fc99fbf9c148b**

to: **bc1qsrr3pv86v8ftxh8nmgrdt9rda7vl4p6ts2nzcg**
amount: **1 Bitcoin**

to: **bc1qj93n553npnsumygn4sqfch9qlkv54u82sjxzdf**
amount: **0 Bitcoin**

LOCAL MEMORY

signature: *Alice, Bob*

The Signatures of Alice and Bob are needed to spend these outputs. This money can only be spent two days after this transaction is confirmed unless the secret to hash 2325005714a7 is revealed.

Payment Channel

2018-10-10 16:40

tx: **hgb710f470dd3df348fc99fbf9c148b**

from: **fb9c6b8dad6094a9b7bf0438eb223e**

to: **bc1qtnsyw9d78dnf9j8p2rhnvj2fx6ukmya6xqfcxl**

SETTLED

amount: 1 Bitcoin

signature: *Alice*

The Signatures of Alice and Bob are needed to spend these outputs

2018-10-10 16:41

tx: **283e4f581e1bb73d8d47a5072471f7**

from: **hgb710f470dd3df348fc99fbf9c148b**

to: **bc1qsrr3pv86v8ftxh8nmgrdt9rda7vl4p[illegible]ts2nzcg**

amount: 0.9 Bitcoin

to: bc1qj93n553npnsumygn4sqfch9qlkv[illegible]u82sjxzdf

amount: 0.1 Bitcoin

LOCAL MEMORY

signature: *Alice, Bob*

The Signatures of Alice and Bob are needed to spend these outputs. This money can only be spent two days after this transaction is confirmed unless the secret to hash 2325005714a7 is revealed.

3) Alice pays 0.1 Bitcoin to Bob by signing a new transaction that sends 0.1 BTC to Bob. This transaction is kept in local memory by both.

Payment Channel

2018-10-10 16:40

tx: **hgb710f470dd3df348fc99fbf9c148b**

from: **fb9c6b8dad6094a9b7bf0438eb223e**

to: **bc1qtnsyw9d78dnf9j8p2rhnvj2fx6ukmya6xqfcxl**

SETTLED

amount: 1 Bitcoin

signature: *Alice*

The Signatures of Alice and Bob are needed to spend these outputs

2018-10-10 16:42

tx: **283e4f581e1bb73d8d47a5072471f7**

from: **hgb710f470dd3df348fc99fbf9c148b**

to: **bc1qsrr3pv86v8ftxh8nmgrdt9rda7vl4p6ts2nzcg**

amount: 0.95 Bitcoin

to: bc1qj93n553npnsumygn4sqfch9qlkv54u82sjxzdf

amount: 0.05 Bitcoin

LOCAL MEMORY

signature: *Alice, Bob*

The Signatures of Alice and Bob are needed to spend these outputs. This money can only be spent two days after this transaction is confirmed unless the secret to hash 2325005714a7 is revealed.

4) Bob can also send funds this way.

Payment Channel

2018-10-10 16:40

tx: **hgb710f470dd3df348fc99fbf9c148b**

from: **fb9c6b8dad6094a9b7bf0438eb223e**

to: **bc1qtnsyw9d78dnf9j8p2rhnvj2fx6ukmya6xqfcxl**

amount: 1 Bitcoin

signature: *Alice*

The Signatures of Alice and Bob are needed t

SETTLED

2018-10-10 16:43

tx: **283e4f581e1bb73d8d47a5072471f7**

from: **hgb710f470dd3df348fc99fbf9c148b**

to: **bc1qsrr3pv86v8ftxh8nmgrdt9rda7vl4p0ts2nzcg**
amount: 0.85 Bitcoin

to: bc1qj93n553npnsumygn4sqfch9qlkv54u82sjxzdf
amount: 0.15 Bitcoin

signature: *Alice, Bob*

The Signatures of Alice and Bob are needed to spend these outputs. This money can only be spent two days after this transaction is confirmed unless the secret to hash 2325005714a7 is revealed.

LOCAL MEMORY

5) An infinite number of transactions can be sent between Alice and Bob.

Payment Channel

2018-10-10 16:40

tx: **hgb710f470dd3df348fc99fbf9c148b**

from: **fb9c6b8dad6094a9b7bf0438eb223e**

to: **bc1qtnsyw9d78dnf9j8p2rhnvj2fx6ukmya6xqfcxl**

amount: 1 Bitcoin

signature: *Alice*

The Signatures of Alice and Bob are needed t

SETTLED

2018-10-10 16:43

tx: **283e4f581e1bb73d8d47a5072471f7**

from: **hgb710f470dd3df348fc99fbf9c148b**

to: **bc1qsrr3pv86v8ftxh8nmgrdt9rda7vl4p6tsxnzcg**
amount: **0.85 Bitcoin**

to: **bc1qj93n553npnsumygn4sqfch9qlkv94a82sjxzdf**
amount: **0.15 Bitcoin**

signature: *Alice, Bob*

The Signatures of Alice and Bob are needed to spend these outputs. This money can only be spent two days after this transaction is confirmed unless the secret to hash 2325005714a7 is revealed.

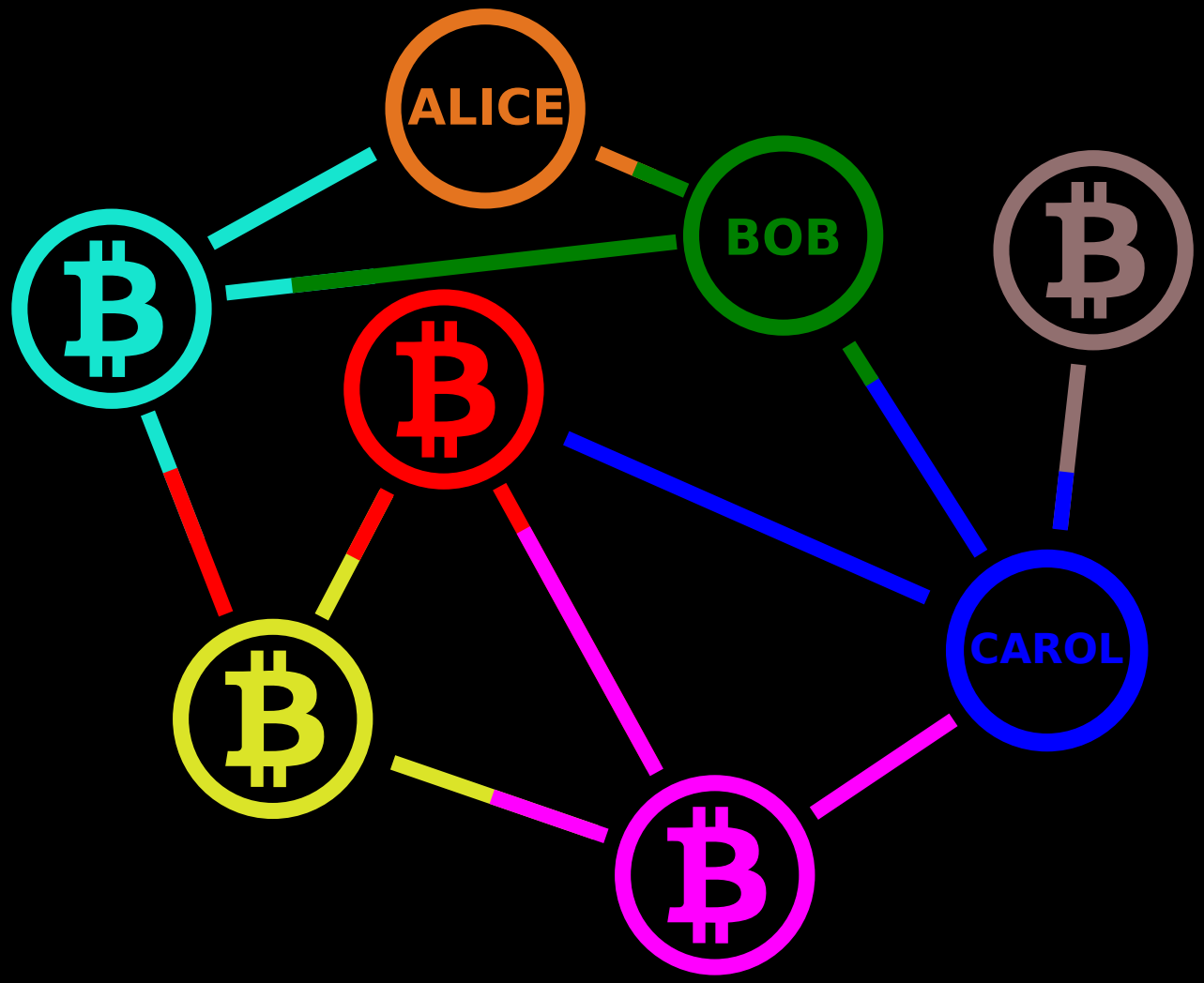
SETTLED

6) Alice and Bob can close their Payment Channel anytime, even if the other party is unavailable.

A Network of Channels

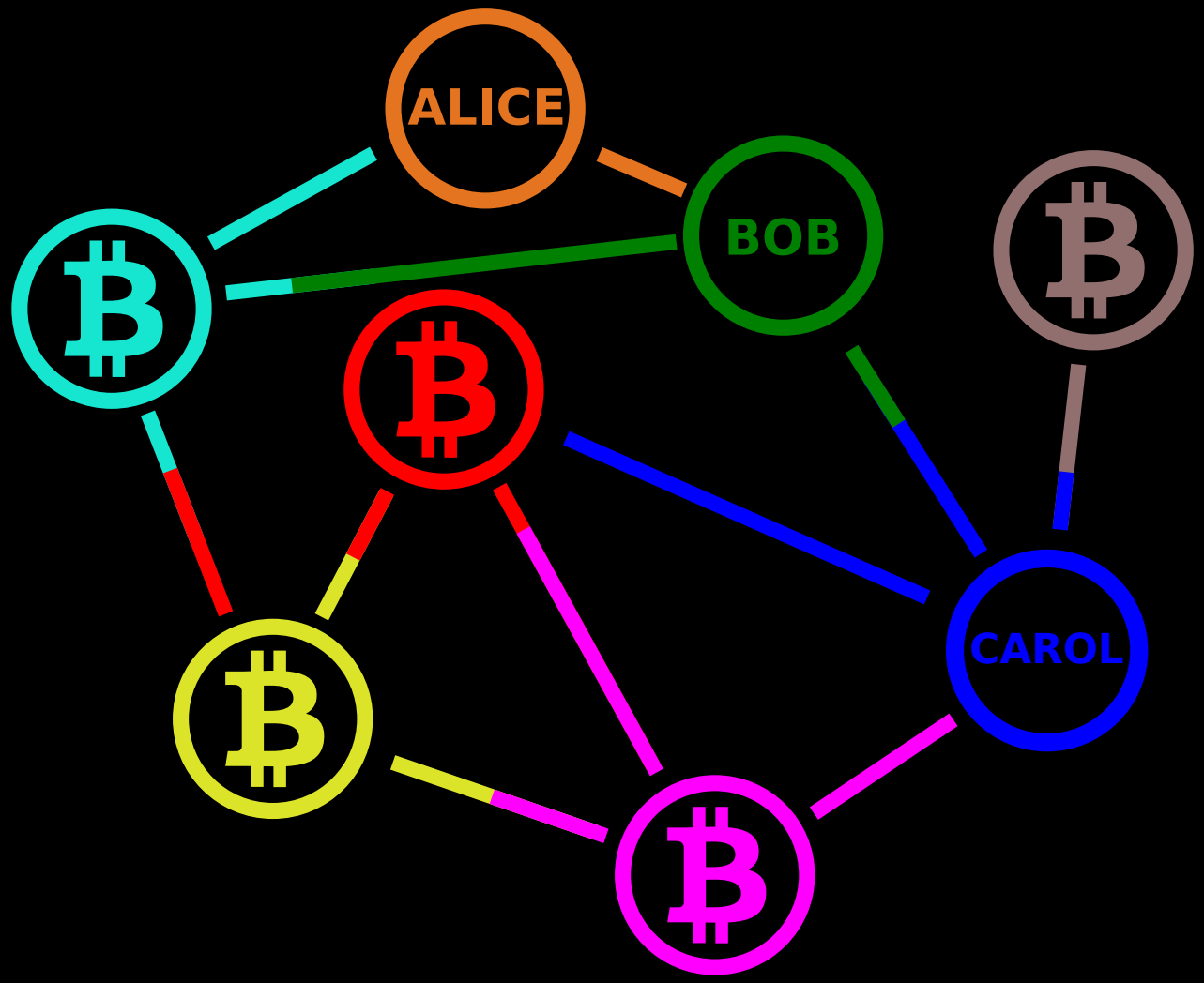
- Hash Time-Locked Contracts (HTLC)
  - Alice sends Bitcoin to a HTLC address
  - Bob only receives the funds if he reveals a secret 'key'
  - Otherwise the payment does not become valid
- Alice → Bob → Carol
  - Carol generates secret key
  - Alice makes payment to Bob dependent on this key
  - Bob makes payment to Carol dependent on the same key
  - Carol needs to reveal her key to receive the payment
- The transfer is made atomically. Either it succeeds completely, or it never happens

A Network of Channels

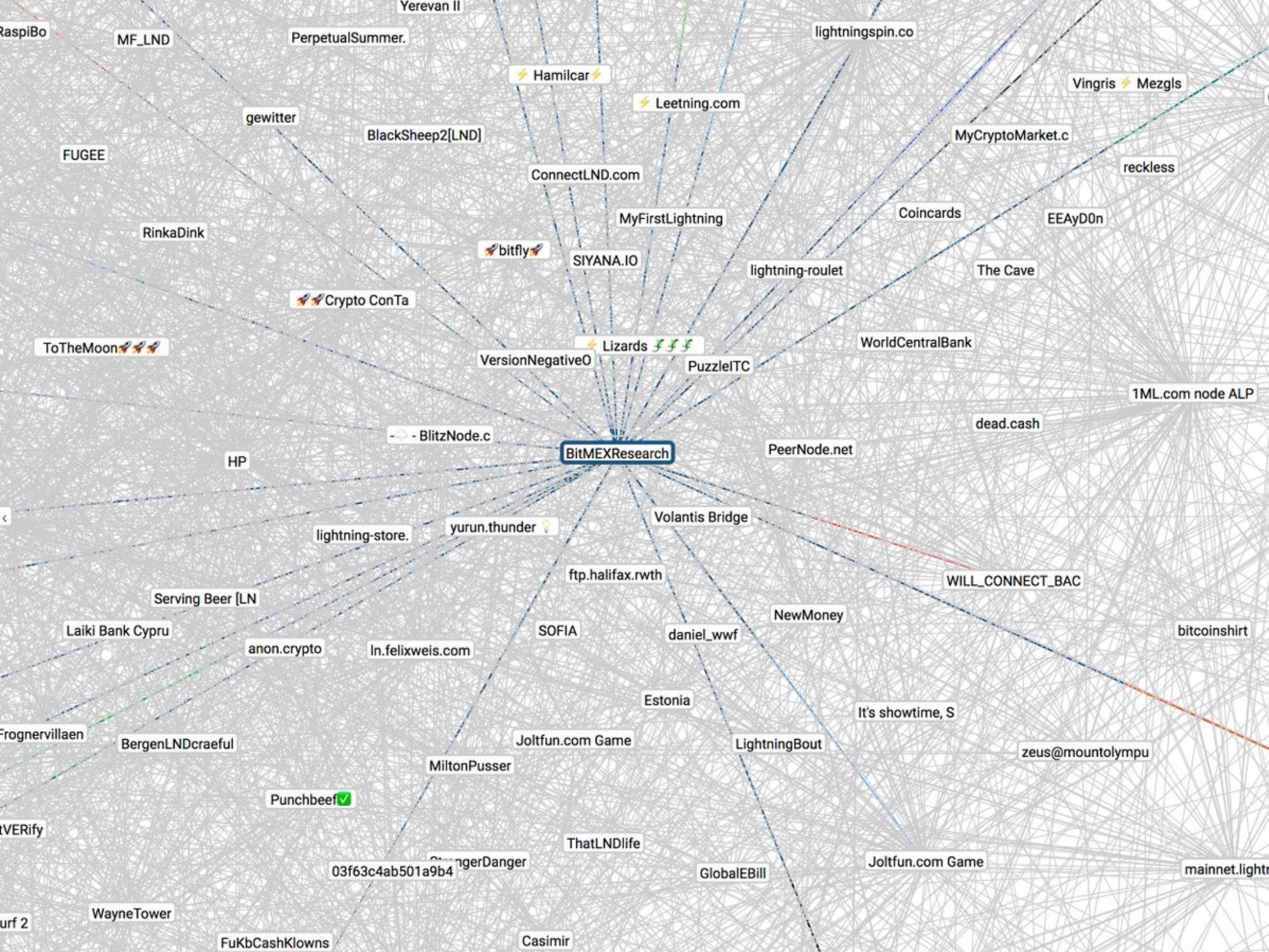


Hong Kong, 7 November, 2020

A Network of Channels



Hong Kong, 7 November, 2020


Yerevan II
RaspiBo
MF_LND
PerpetualSummer.
lightningspin.co
⚡ Hamilcar ⚡
Vingris ⚡ Mezgls
⚡ Leetning.com
gewitter
BlackSheep2[LND]
MyCryptoMarket.c
FUGEE
ConnectLND.com
reckless
MyFirstLightning
Coincards
EEAyD0n
RinkaDink
🚀bitfly🚀
SIYANA.IO
lightning-roulet
The Cave
🚀🚀Crypto ConTa
⚡ Lizards ⚡⚡⚡
WorldCentralBank
ToTheMoon🚀🚀🚀
VersionNegativeO
PuzzleITC
1ML.com node ALP
dead.cash
- - BlitzNode.c
BitMEXResearch
PeerNode.net
HP
Volantis Bridge
lightning-store.
yurun.thunder 💡
ftp.halifax.rwth
WILL_CONNECT_BAC
Serving Beer [LN
NewMoney
Laiki Bank Cypru
SOFIA
daniel_wwf
bitcoinshirt
anon.crypto
ln.felixweis.com
Estonia
It's showtime, S
Frognervillaen
BergenLNDcraeful
Joltfun.com Game
LightningBout
zeus@mountolympu
MiltonPusser
Punchbeef✅
tVERify
ThatLNDlife
StrangerDanger
03f63c4ab501a9b4
GlobalEBill
Joltfun.com Game
mainnet.lightn
WayneTower
urf 2
FuKbCashKlowns
Casimir

Benefits

- Infinite payments within the network
- Payments can be arbitrarily small (<1 Satoshi)
- Instant Payments
- Based on invoices, not addresses
- Easier to protect the users' privacy, as payments aren't public
- Unicast und Anycast are easier to scale
- Bitcoin can be liquidated in real-time

Limitations

- Liquidity of the channels is limited
- Finding routes can be complicated
- Participants have to always be online
- Channels cannot be opened and closed frequently (Bitcoin ~7 tx/s)

Applications

- Efficient market for microservices
  - APIs (e.g. Time tables, ticket sales)
  - AI (e.g. Routing, image recognition)
  - Sensors (e.g. Traffic, weather)
  - Computing power (e.g. CGI animations)
  - Memory (z.B. Amazon S3)
- No Accounts necessary
  - Security
  - Privacy
  - Identification through asymmetric keys

Leonhard A. Weese
Co-founder, Bitcoin Association of Hong Kong
leo@bitcoin.org.hk
@LeoAW

https://www.bitcoin.org.hk

PGP: 9185 B1FD 625A 1AD0 CCFE F451 C073 56F5 BB4D D1B7

Hong Kong, 7 November, 2020