

# Bitcoin and Lightning

# Agenda

- Bitcoin
  - Taproot
- Lightning

```

00000000 f9 be b4 d9 1d 01 00 00 01 00 00 00 00 00 00 |.....|
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000020 00 00 00 00 00 00 00 00 00 00 00 3b a3 ed fd |.....;...|
00000030 7a 7b 12 b2 7a c7 2c 3e 67 76 8f 61 7f c8 1b c3 |z{..z.,>gv.a...|
00000040 88 8a 51 32 3a 9f b8 aa 4b 1e 5e 4a 29 ab 5f 49 |..Q2:...K.^J)._I|
00000050 ff ff 00 1d 1d ac 2b 7c 01 01 00 00 00 01 00 00 |.....+|.....|
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000070 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff |.....|
00000080 ff ff 4d 04 ff ff 00 1d 01 04 45 54 68 65 20 54 |..M.....EThe T|
00000090 69 6d 65 73 20 30 33 2f 4a 61 6e 2f 32 30 30 39 |imes 03/Jan/2009|
000000a0 20 43 68 61 6e 63 65 6c 6c 6f 72 20 6f 6e 20 62 | Chancellor on b|
000000b0 72 69 6e 6b 20 6f 66 20 73 65 63 6f 6e 64 20 62 |rink of second b|
000000c0 61 69 6c 6f 75 74 20 66 6f 72 20 62 61 6e 6b 73 |ailout for banks|
000000d0 ff ff ff ff 01 00 f2 05 2a 01 00 00 00 43 41 04 |.....*....CA.|
000000e0 67 8a fd b0 fe 55 48 27 19 67 f1 a6 71 30 b7 10 |g....UH'.g..q0..|
000000f0 5c d6 a8 28 e0 39 09 a6 79 62 e0 ea 1f 61 de |\\..(.9..yb...a.|
000000ff

```

January 3rd 2009

# Early days

- Software developed before whitepaper released
- Effectively solves The Byzantine Generals problem (double spending) via proof-of-work.

*“The proof-of-work chain is how all the synchronisation, distributed database and global view problems you've asked about are solved.”*


- Satoshi Nakamoto Thu Nov 13 17:56:55 EST 2008

<https://www.metzdowd.com/pipermail/cryptography/2008-November/014849.html>



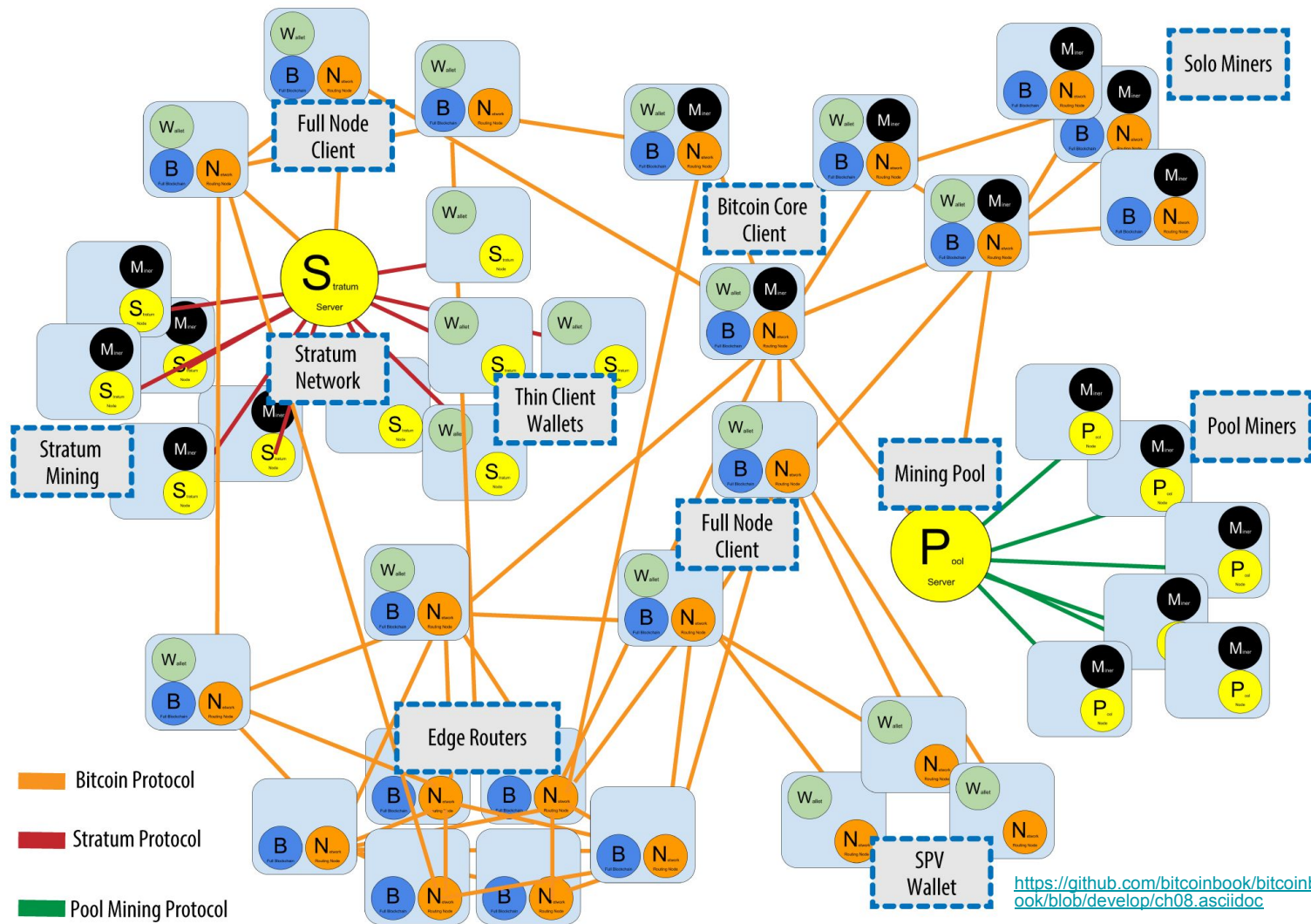
# Satoshi Nakamoto

- Pseudonymous inventor(s) of Bitcoin, not the best coder...

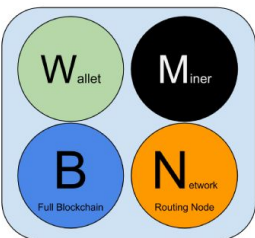
Bug	Resolution	Discovered
Spend coins not owned due to a bug in the transaction handling code.	This was never exploited on the main network, and was fixed by Bitcoin version 0.3.5.	28/7/2010
Overflow error would allow a transaction that creates 184,467,440,737.09551616 bitcoins for three different addresses in block 74638 (16/8/2010).	A new version of the client was published within five hours of the discovery that contained a soft forking change to the consensus rules that rejected output value overflow transactions.	15/8/2010
<p>“The block timestamp is a 32-bit integer. Under the stated assumptions, after 5101541 blocks, that timestamp will overflow and no more blocks can be mined.”</p> <p><a href="https://twitter.com/pwuille/status/1259990906997858304">https://twitter.com/pwuille/status/1259990906997858304</a></p>	 A screenshot of a Twitter thread on a dark background. The top tweet is by Justin Siegel (@JustinSiegel1) dated May 12, 2020, asking "When would the 'appropriate' time to fix this be?". It has 1 reply, 1 retweet, and 1 like. The bottom tweet is by Pieter Wuille (@pwuille) dated May 12, 2020, replying "Somewhere in the next 80 years?". <p>Justin Siegel @JustinSiegel1 · May 12, 2020 When would the “appropriate” time to fix this be?</p> <p>Pieter Wuille @pwuille · May 12, 2020 Somewhere in the next 80 years?</p>	

# Network

Extended:

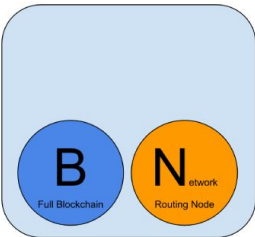


# Nodes



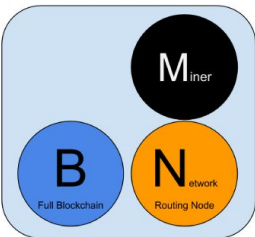
## Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.



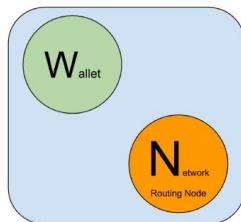
## Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.



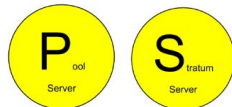
## Solo Miner

Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.



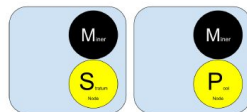
## Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.



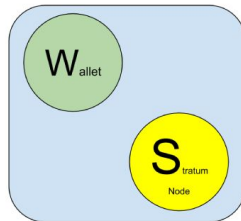
## Pool Protocol Servers

Gateway routers connecting the bitcoin P2P network to nodes running other protocols such as pool mining nodes or Stratum nodes.



## Mining Nodes

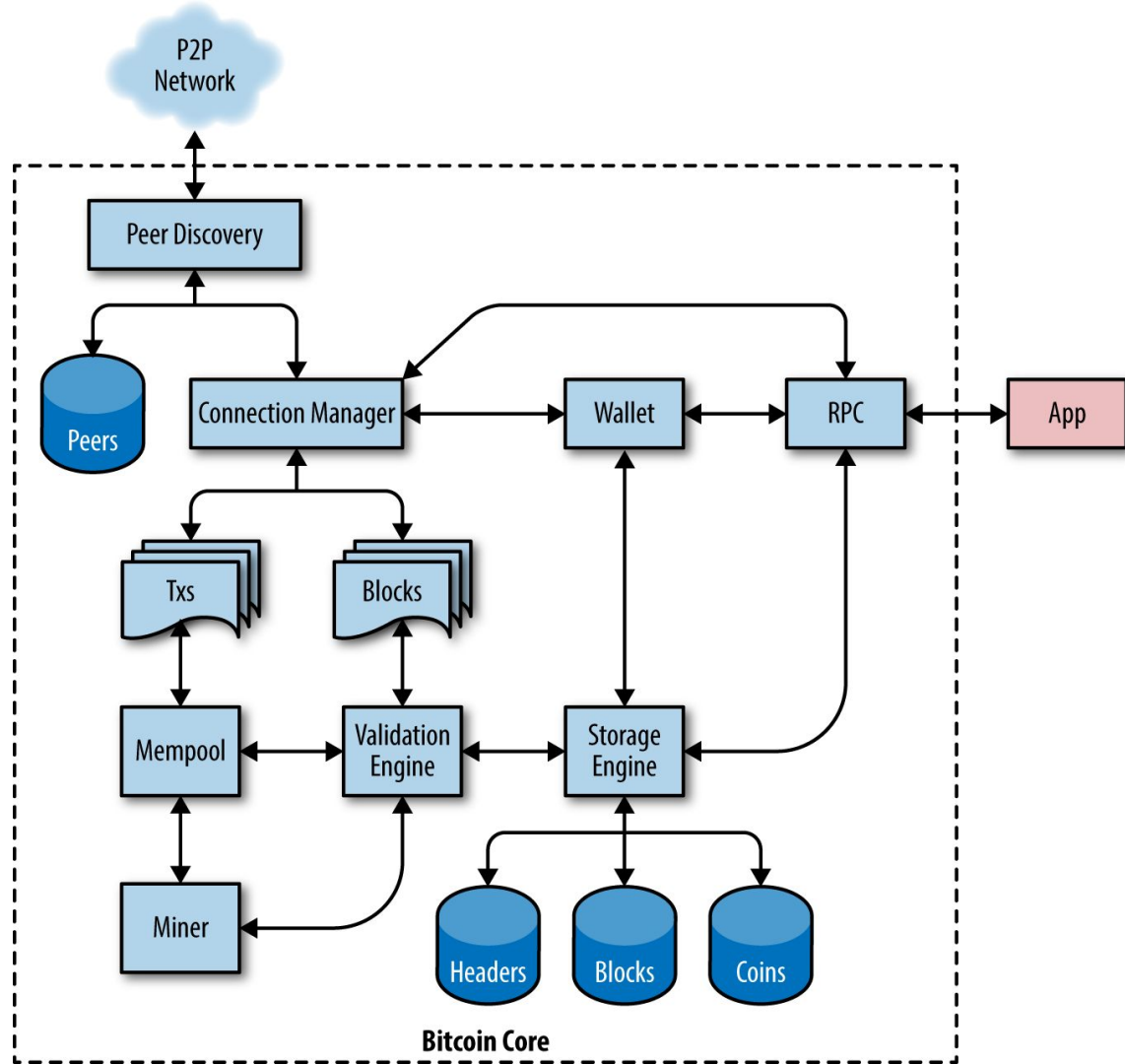
Contain a mining function, without a blockchain, with the Stratum protocol node (S) or other pool (P) mining protocol node.



## Lightweight (SPV) Stratum wallet

Contains a Wallet and a Network node on the Stratum protocol, without a blockchain.

# Reference Client





# Full Node

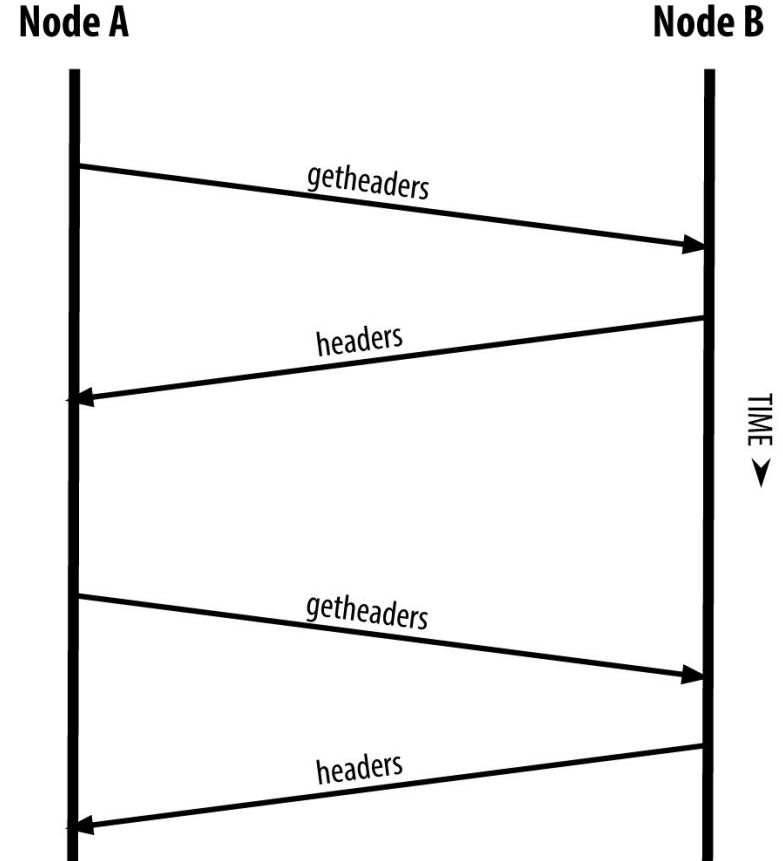
- RaspberryPi 4 4GB
- 1TB SSD
- Micro SDCard 32GB
- LCD - 3.5" RPi Display





# Simplified Payment Verification (SPV) Nodes

- Becoming most prominent nodes on the network.
- Can run on resource-constrained devices e.g. smartphones, embedded systems
- Downloads only block headers - 1000x smaller than full chain.
- Verifies transactions via merkle path after 6 additional blocks.
- Balance between resource needs, practicality, and security.



# Blockchain

<https://mempool.space/tv>



# Expensive, Slow and Boring

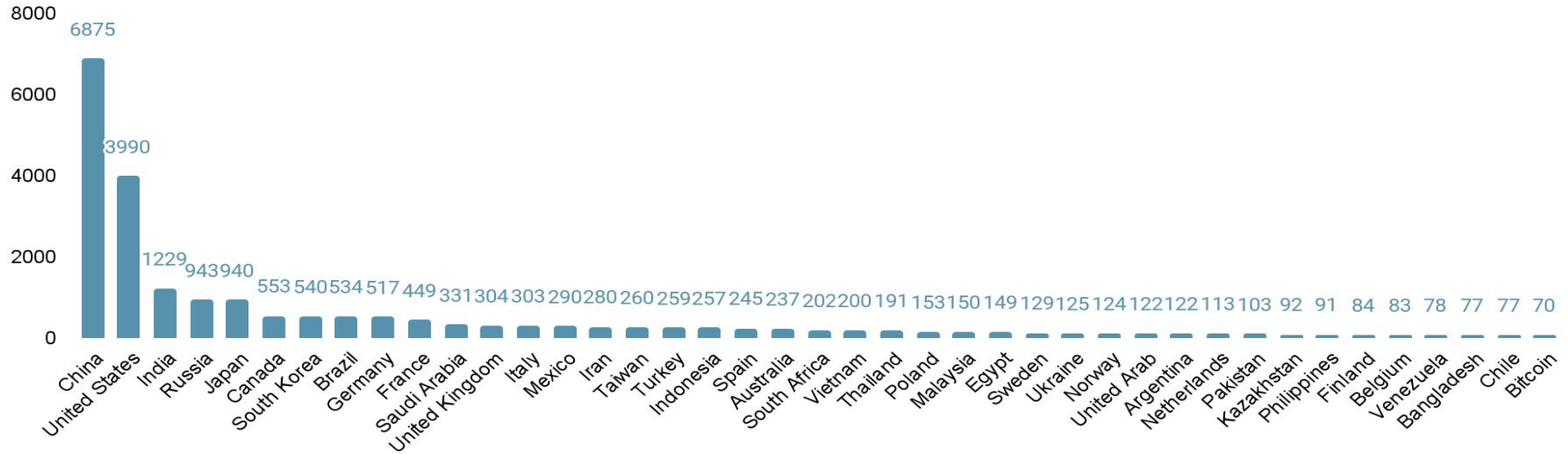
- Distributed ledger
- Store of value
- Slow 'n' steady
  - Dev and tx (~4 tx / second)
- Power intensive
  - <https://endthefud.org/>



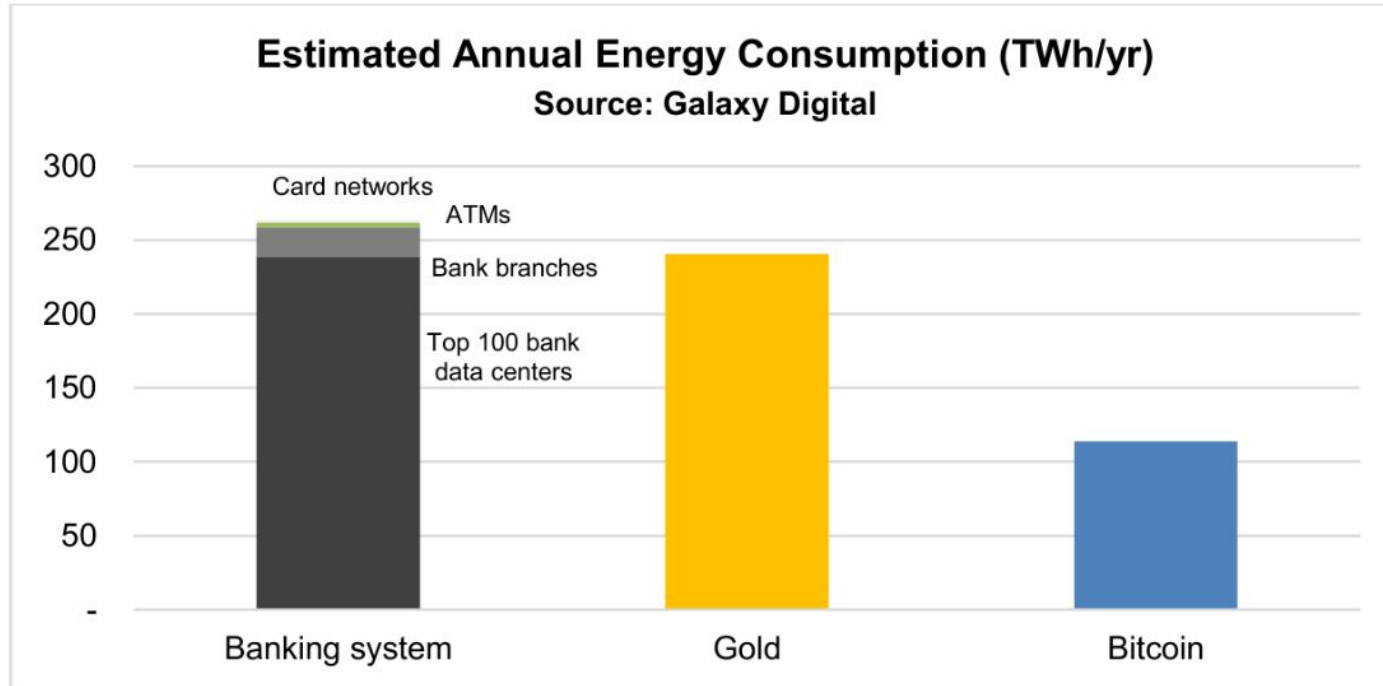
# FUD

- Power  $\neq$  Carbon  $\neq$  Emissions
- Electronic waste

2019 Annual Energy Consumption (in TWh)



# “BitGold Coin”

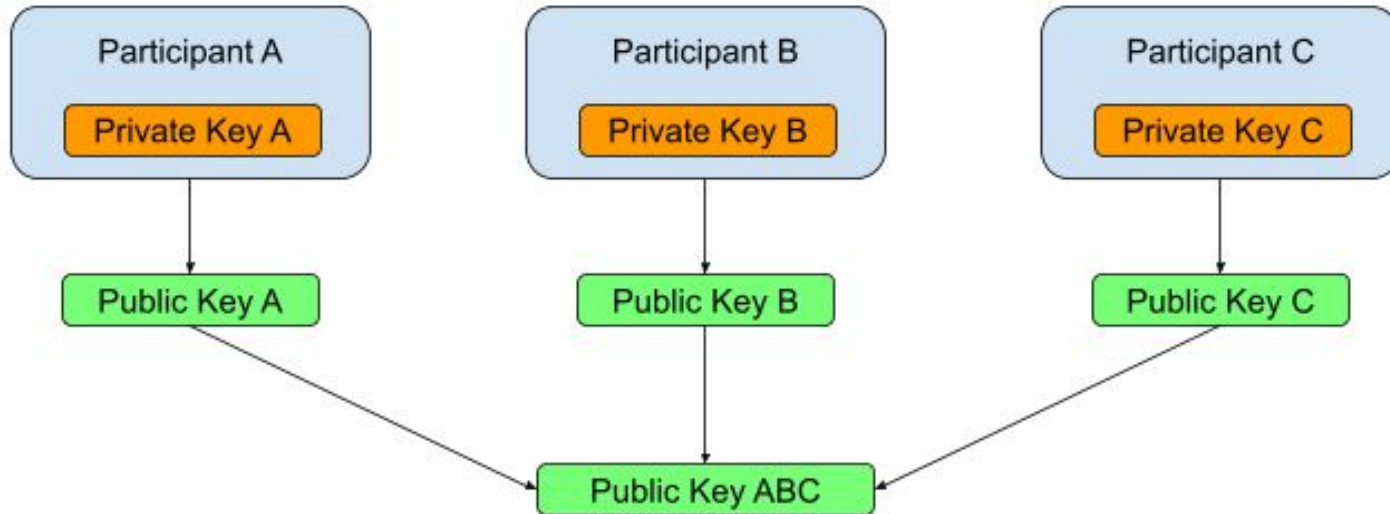


\*2021



# “BIP Taproot”

- 340 Schnorr Signatures
- 341 Pay-to-Taproot (P2TR)
- 342 Tapscript



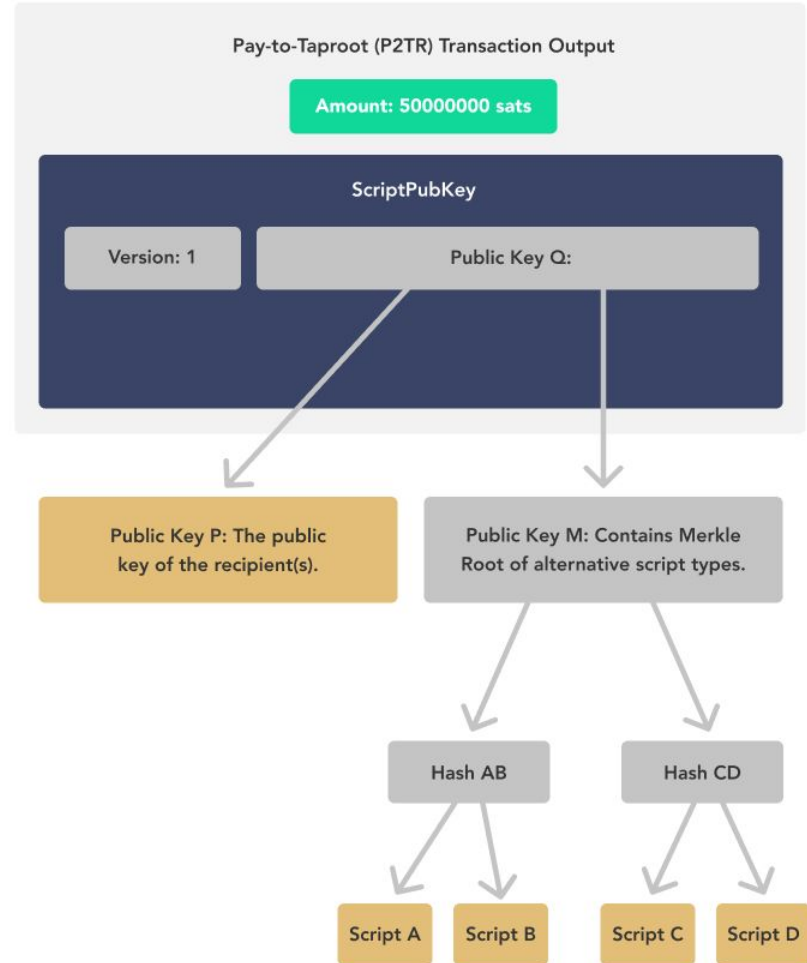
# BIP 340 - Schnorr Signatures

- A type of digital signature scheme similar to the ECDSA scheme
- Increased privacy
- Smaller on-chain size thus lower fees
- More complex spending policies e.g. k-of-n multisig, represented as a single signature for a single key
- Faster validation

# BIP 341 - Pay-to-Taproot (P2TR)

- Allows Bitcoin to be spent via pub-key (key path) or **Merkelized Alternative Script Tree** (script path)
  - MAST can represent multiple scripts
- A significant improvement to privacy
- The spender of a MAST output need not reveal all of the scripts, only the one they used

<https://river.com/learn/terms/p/pay-to-taproot-p2tr/>

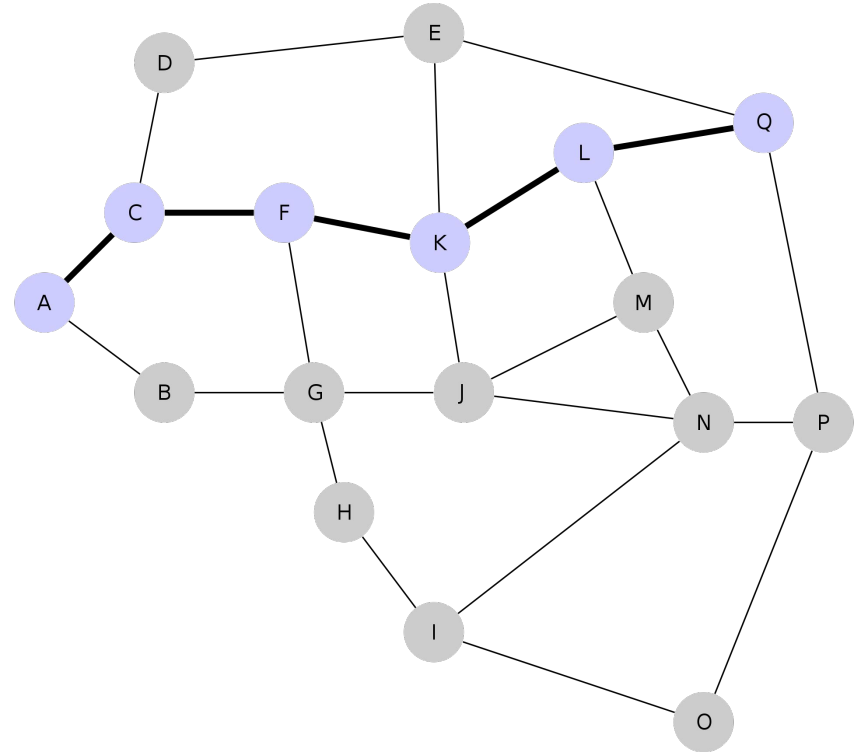


# BIP 342 - Tapscript

- Scripting language used to enable new transaction types with several opcodes
- Verify Taproot spends and Schnorr signatures
- Designed to maximize future flexibility of P2TR spending in order to allow for upgrades which are not yet foreseen

# Lightning Network

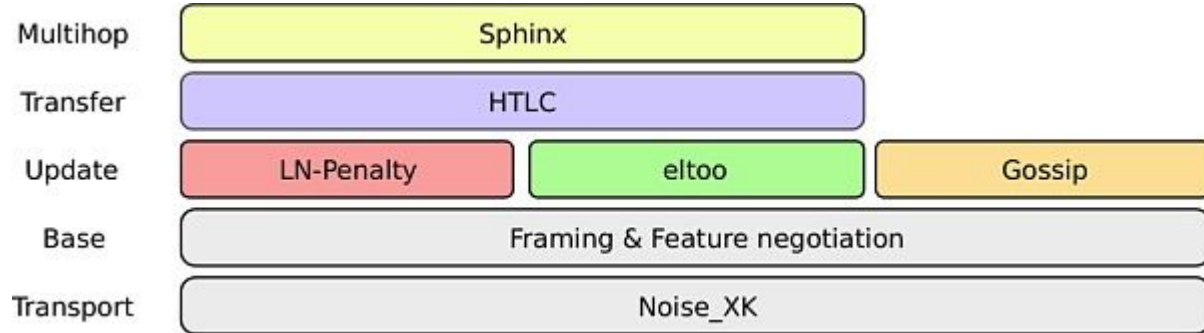
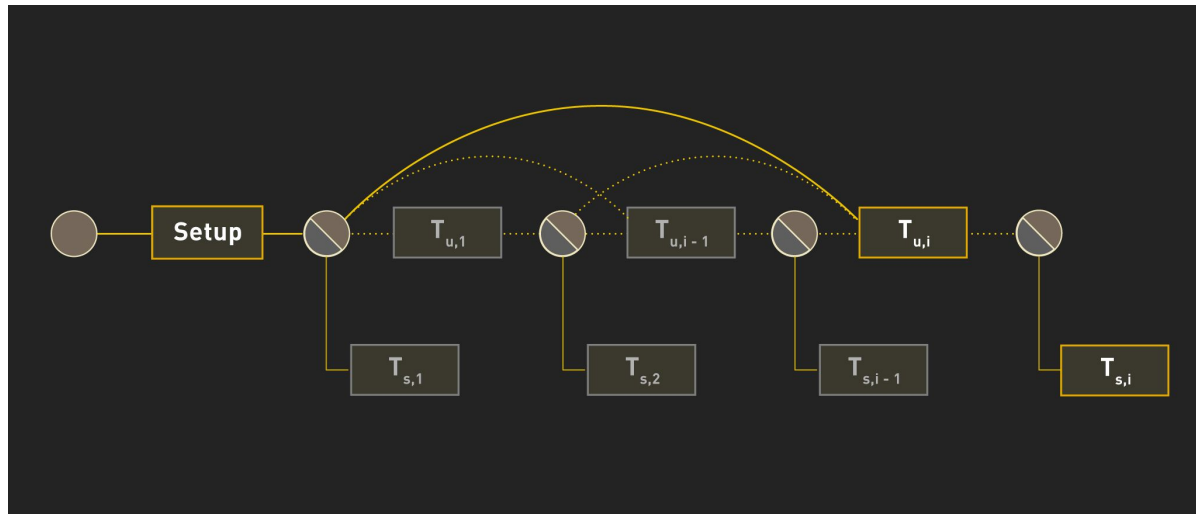
- Mesh network and Bitcoin layer two.
- Allows unlimited near-free p2p transactions without bogging down the BTC blockchain.
- Ramp-on to form channel, ramp-off to settle on the BTC blockchain.
- Channel established by the funding of a 2-of-2 multisignature address.
- Prevents either channel partner from spending the funds unilaterally.
- Watchtowers act as second line of defense.





# Eltoo (L2)

- Allows multiple types of payment channels to operate in parallel.
- Improves fairness of penalty schemes when settling channels.
- Multi-party off-chain contracts.
- Backwards compatible with Lightning.



# Lightning Demo

ssh [root@btcpay939539.Indyn.com](ssh://root@btcpay939539.Indyn.com)

```
bitcoin-lndcli.sh sendpayment --keysend  
--dest=02f4d86b01fb06bb702707bef200e982bd3a71040410ad0d41128f3f6e653d  
d1d6 --amt=1 --final_cltv_delta=40 --data 65537=$(echo -n "It's raining sats" | xxd  
-pu -c 10000)
```

Recipient: <https://btcpay346208.Indyn.com>