UNIVERSITY of NICOSIA

Session 5

Bitcoin in Practice – Part 2

Bitcoin Core, MultiSig, SegWit, CoinJoin, Lightning Network and Forks

DFIN 511: Introduction to Digital Currencies

Session 5: Objectives

Objectives

- Learn about Bitcoin Core, its history and current version
- Understand the functionality of Multi-Signature Transactions
- Introduce the concepts of Segregated Witness and Transaction Malleability
- Understand the Lightning Network and its purpose
- Learn about Soft and Hard Forks

Session 5: Agenda

1. Bitcoin Core
2. Multi-Signature Transactions
3. Segregated Witness
4. CoinJoin
5. Lightning Network
6. A Fork in the Road (a primer)
7. Conclusions
8. Further Reading

Session 5: Bitcoin in Practice – Part 2

1. Bitcoin Core

Nodes and Bitcoin Core

- Any computer that connects to the Bitcoin network is called a **node**.
- Some nodes that maintain only a subset of the blockchain and verify transactions using a method called simplified payment verification (SPV) are called SPV or **lightweight nodes.** Mobile wallets almost always are lightweight nodes.
- Other nodes that maintain a complete and up-to-date copy of the blockchain, and can fully verify transactions against all the consensus rules of Bitcoin are called **full nodes**.
- "A full node is a program that fully validates transactions and blocks. Almost all full nodes also help the network by accepting transactions and blocks from other full nodes, validating those transactions and blocks, and then relaying them to further full nodes."
- The most popular implementation of full nodes is the reference client Bitcoin Core.
- "Bitcoin Core is programmed to decide which blockchain contains valid transactions."

Learn more: See No.1 on the further reading list, located at the end of the document.

Source: https://bitcoin.org/en/full-node

Source: https://bitcoin.org/en/bitcoin-core/

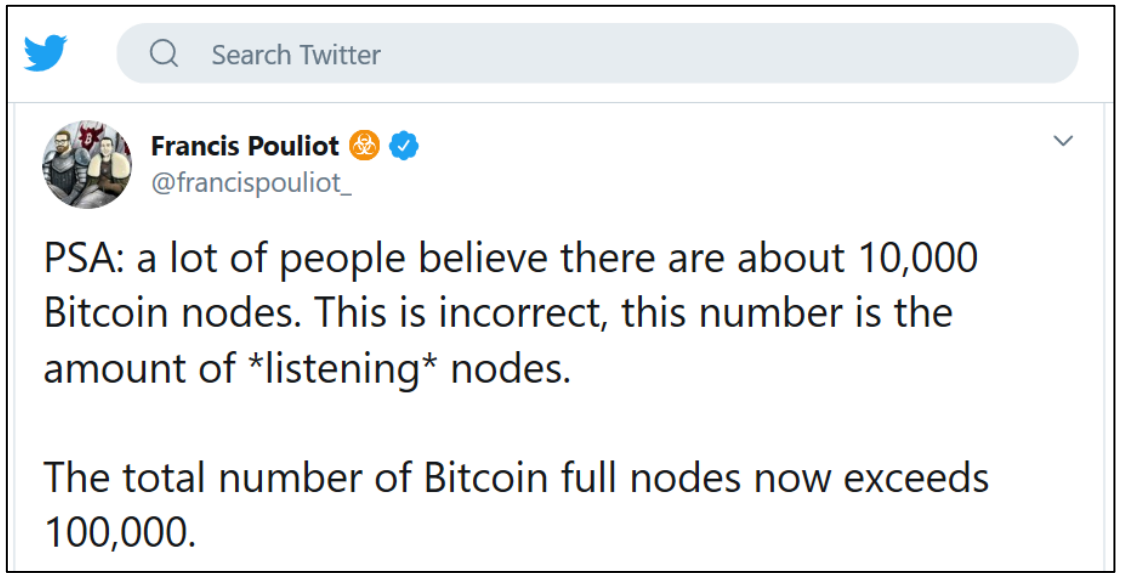
Bitcoin Core

- The current version of Bitcoin Core is 0.21.1.
- New versions of Bitcoin Core are typically released every 2-3 months.
- A notable change in version 0.21.1 compared to previous versions is how "miner block templates produced by this version of Bitcoin Core will signal readiness to enforce taproot during the roughly three month period specified by BIP341."
- Besides Bitcoin Core, other implementations include:
  - btcd, Bitcore, Bitcoinj

Upgrade your client to the **latest version (0.21.1) using this detailed guide**: https://bitcoincore.org/en/2021/05/01/release-0.21.1/

Bitcoin Core Nodes

- On May 5, 2019, the CEO of Bull Bitcoin declared that the total number of Bitcoin Core full nodes now exceeds 100,000. (the highest number of nodes since the 2017 peak displayed in next slide). Also notice (to your right) how many users still operate on oldest versions of Bitcoin).



Source: https://twitter.com/francispouliot_/status/1125139855313387520

```
   40442 /Satoshi:0.16.1/ Bitcoin Core
   21072 /Satoshi:0.17.1/ Bitcoin Core
   11576 /bread:2.1/ bread
    6587 /Satoshi:0.15.1/ Bitcoin Core
    5375 /breadwallet:0.6.2/ bread
    5102 /Satoshi:0.17.0/ Bitcoin Core
    3950 /Satoshi:0.17.0.1/ Bitcoin Core
    3839 /Satoshi:0.16.0/ Bitcoin Core
    2748 /Satoshi:0.18.0/ Bitcoin Core
    2409 /Satoshi:0.13.2/ Bitcoin Core
    2049 /Satoshi:0.14.2/ Bitcoin Core
    1954 VDS 0.9.3 other (excluded)
    1759 VDS 0.9.4 other (excluded)
    1567 /Satoshi:0.15.0.1/ Bitcoin Core
    1442 /Satoshi:0.16.3/ Bitcoin Core
    1331 VDS 0.9.8 other (excluded)
    1321 VDS 0.9.6 other (excluded)
    1210 /bitcore:1.1.0/ bitcore
    1191 /bitcoinj:0.15.1/Bitcoin Wallet:7.07/
Bitcoin Wallet for Android
    1126 VDS 0.9.7 other (excluded)
    1124 /bitcoinj:0.15.1/Bitcoin Wallet:7.06/
Bitcoin Wallet for Android
    1034 /Satoshi:0.16.2/ Bitcoin Core
     800 /Satoshi:0.14.1/ Bitcoin Core
     583 VDS 0.9.2 other (excluded)
     578 VDS 0.9.5 other (excluded)
     528 /Satoshi:0.13.1/ Bitcoin Core
     428 /bitcoincashj:0.15-SNAPSHOT/ other
(excluded)
     407 /bitcoinj:0.15-SNAPSHOT/ other
(excluded)
     382 /Bither1.6.1/ Bither
     360 /Satoshi:0.15.0/ Bitcoin Core
     323 /bitcoinj:0.15-SNAPSHOT/BCM:1.2/
```

Number of Bitcoin Core Nodes (Full & Listening) for the last $2^{1/2}$ years

In GREEN: the total number of nodes

~55,000

In BLUE: the number of listening nodes, thus full nodes that are publicly visible.

~4,500

Bitcoin Nodes over time: https://luke.dashjr.org/programs/bitcoin/files/charts/historical.html

Session 5: Bitcoin in Practice – Part 2

2. Multi-Signature Transactions

Multi-Signature (MultiSig)Transactions

- Bitcoin has "multi-signature" (shorthand 'multisig') functionality, in which the spending of funds can be set to require more than one signature / a quorum of signatures for authorizing transactions, thus enhancing security.
- MultiSig wallets can be useful within a corporate environment, where multiple people need to approve the movement of funds. They may also be used to facilitate escrow services, especially when it comes to larger transactions with unknown entities.
- A single individual may create a MultiSig setup in which they hold all keys, storing each of the keys on different devices (ex. mobile phone, laptop, and hardware wallet), with a requirement that signatures from two of the three keys will authorize a transaction.
- MultiSig setups can help protect users from phishing attacks and malware infections. Even if one of the above devices is lost, stolen, or compromised, one key will not be sufficient to access the funds; the original owner can still access their funds using the remaining two keys.
- Some popular MultiSig wallets are listed here: https://en.bitcoin.it/wiki/Multisignature#Multisignature_Wallets

https://en.bitcoin.it/wiki/Multisignature https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch07.asciidoc

Multi-Signature Transactions

The most common condition for multi-signature transactions is to employ an “M-of-N scheme." In a 2-of-3 scheme, "three public keys are listed as potential signers and at least two of those must be used to create signatures for a valid transaction to spend the funds."

MuSig, a new Schnorr-based multi-signature scheme in development, "is designed to make multi-signature Bitcoin transactions less complex without sacrificing privacy."

"Due to MuSig’s innovative key-aggregation feature, this signature is a regular Schnorr signature that can be processed by Bitcoin once Taproot is activated. When used to create multisig wallets, MuSig reduces transaction fees and increases privacy compared to the traditional way of using the CHECKMULTISIG opcode for `n`-of-`n` signatures, which needs `n` public keys and `n` ECDSA signatures on the blockchain." (Jonas Nick, Tim Ruffing)

Multi-Signature Transactions

The general form of a multisig (“M-of-N”) transaction script looks like:

“M <Public Key 1> <Public Key 2> … <Public Key N> N OP_CHECKMULTISIG”

In the case of a “2-of-3” multisig transaction the script looks like:

“2 <Public Key A> <Public Key B> <Public Key C> 3 OP_CHECKMULTISIG”

The above forms a “locking script”, which can only be unlocked by an equivalent “unlocking script" containing 2 or more signatures computed from the signers' private keys, corresponding to the listed public keys:

“OP_0 <Signature B> <Signature C>”

The above “locking” and “unlocking” script, together form a “validation script”:

“OP_0 <Signature B> <Signature C>

2 <Public Key A> <Public Key B> <Public Key C> 3 OP_CHECKMULTISIG”

(Validation script)

Session 5: Bitcoin in Practice – Part 2

3. Transaction Malleability and Segregated Witness (SegWit)

Transaction Malleability: What is the Problem?

- Transaction malleability is a weakness that would allow a malicious actor to modify ("malleate") a transaction by modifying the "witness data" in such a way that it changes the transaction ID. (Remember that after confirmation, the digital signature, and therefore the transaction ID, are immutable).
- What has now been produced, is a second transaction that signs the same amount, to the same destination address, but with a changed transaction ID.
- This attack does not allow the attacker to steal funds or change where they are being sent to. However, it could be used to defraud the sender by tricking them into sending a second payment after the original did not appear to be confirmed.

Read more about transaction malleability: https://www.mycryptopedia.com/transaction-malleability-explained/

Fun fact: Mt.Gox, the biggest exchange in Japan collapsed in Feb 2014, suspended all withdrawals and blamed transaction malleability for suspending withdrawals.

Segregated Witness and how it addresses Transaction Malleability

- Segregated Witness (SegWit) is an architectural change that was activated in Bitcoin on August 1st, 2017. It moves the witness data of transactions from the scriptSig (unlocking script) field of a transaction into a separate witness data structure that accompanies a transaction.
- The majority of space in a transaction (around 65% or more) can be taken up by signature data.
- By moving the witness outside the transaction, the transaction hash used as an identifier no longer includes the witness data.
- SegWit makes it easier and safer to implement payment channels, the Lightning Network, and other more advanced scripting capabilities that will be introduced in the future.

Learn more: See No. 3 on the further reading list for an introduction to Segwit, located at the end of the presentation.

Further explanation of Segwit: https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch07.asciidoc#segregated-witness

Segregated Witness: Short History and Benefits

Short History:

- 7 December 2015: Pieter Wuille first presented the idea of "Segregated Witness" at the Scaling Bitcoin workshops in Hong Kong as a solution of Bitcoin's scalability problems.
- 23 August 2017: Segregated Witness was fully activated as a soft fork on the Bitcoin network.

Benefits:

- Increases block capacity from 1MB to a theoretical, maximally efficient 4MB. More transactions can fit into each block, and transaction fees decrease.
- "Nodes can prune the witness data after validating the signatures or ignore it altogether when doing simplified payment verification." (Mastering Bitcoin)
- Prevents transaction malleability attacks.
- Enables more complex scripting possibilities.
- Is backward compatible – it is a soft fork.

Learn more: See No. 3 on the further reading list for an introduction to Segwit.

Segregated Witness: Short History and Benefits

Adoption of Segregated Witness since its activation in 2017:

- The majority of wallets and cryptocurrency exchanges now support SegWit.
- Bitcoin Core versions from 0.16.0 onwards include full SegWit support.
- The percentage of bitcoin transactions using SegWit has exceeded 50% in September 2019, and as of August 2021 it has exceeded 75%.

Why is SegWit not fully adopted?

- Since it was not a mandatory upgrade, wallets and exchanges adopt at their own pace.
- Users had to become familiar with new address formats (wrapped and native SegWit).
- Misconceptions about how SegWit worked led to its scaling and fee benefits being overlooked.

Source: https://blog.coinbase.com/announcing-segwit-support-on-coinbase-4e51117857c7

https://captainaltcoin.com/bitcoin-segwit-wallets/

https://cointelegraph.com/news/share-of-segwit-spending-bitcoin-transactions-now-over-50

Session 5: Bitcoin in Practice – Part 2

4. CoinJoin

CoinJoin: Short History

CoinJoin is a Bitcoin transaction where multiple users combine their UTXOs, improving privacy.

- **August 2013:** Greg Maxwell proposes "CoinJoin: Bitcoin Privacy for the Real World."
- **May 2014:** A browser extension called DarkWallet is released, which implements CoinJoin.
- **December 2015:** JoinMarket v0.1.0, another CoinJoin client, is released.
- **August 2017:** The Zerolink Framework, a specification for CoinJoin wallets, is launched.
- **August 2018:** The Chaumian CoinJoin wallet Wasabi is launched.
- **June 2019:** Wasabi coordinates the first 100-party CoinJoin, the largest at the time.
- **August 2019:** Samourai Wallet, launched in early 2015, introduces collaborative mini-CoinJoins.
- **May 2020:** Chris Belcher publishes design sketch for CoinSwap, also conceived by Maxwell.
- **January 2021:** PayJoin adoption is tracked as more compatible implementations emerge.

https://blog.wasabiwallet.io/what-is-a-coinjoin/

CoinJoin: Implications and Regulatory Response

Blockchain analysis firms have cited difficulties with tracing and deanonymising transactions using CoinJoin, as well as on the Lightning Network. Tom Robinson, co-founder of **Elliptic**, also stated: "I believe Schnorr and Taproot are actually going to make that very difficult to do."

While law enforcement in the United States and Europe have cited concerns regarding the possibility for money laundering, terrorism financing, and moved to take down centralised, custodial 'tumblers', non custodial mixers like Wasabi, Samourai, and JoinMarket have not been considered "obliged entities" under anti-money laundering regulations.

- **May 2019:** FinCEN distinguishes between "service providers" and "software providers."
- **April 2020:** A Europol report on Wasabi Wallet states that the software is "popular enough to spark our interest," attempts to de-mix transactions are "realistically speaking, in most cases" not possible, and AMLD5 "does not apply to this service."

https://bitcoinmagazine.com/what-is-bitcoin/what-are-bitcoin-mixers

Session 5: Bitcoin in Practice – Part 2

5. Lightning Network

Lightning Network (Routed Payment Channels)

The Lightning Network is a peer-to-peer routed payment protocol of bi-directional channels that works as a second layer on top of a blockchain, designed to improve enable smaller, faster, and cheaper transactions.

- The idea behind Lightning Network is that not all transactions need to be recorded on-chain; instead, they can be handled through a series of scalable off-chain commitments, while still being backed by the underlying security of the Bitcoin network.
- In its basic form, "a payment channel is simply a 2-of-2 multisignature address on Bitcoin, for which you hold one key, and your channel partner holds the other key."
- "Once several participants have channels from one party to another, payment can also be 'forwarded' from payment channel to payment channel, by setting up a path across the network connecting several payment channels together."

Learn More: See No. 2 on our further reading list, located at the end of the presentation.

https://github.com/lnbook/lnbook/blob/develop/03_how_ln_works.asciidoc#payment-channels-basics

Payment Channels

- Payment channels are built on top of 2-of-2 multi-signature addresses, timelocks and Segregated Witness transaction outputs.
- A channel is opened after the multi-signature address receives an initial on-chain funding transaction.
- Parties in the channel can then make off-chain payments between each other, updating the channel balance along the way, as much as they wish.
- Either of the participants may decide to close the channel, cooperatively or uncooperatively, at any time.
- When the channel is closed, the balance will be settled through a transaction recorded on-chain.
- A hypothetical scenario with three parties (A, B, C) routing:
  - There are two payment channels. A has a payment channel with B, and B has a payment channel with C.
  - If A wants to send a payment to C, then A will first update their balance in the payment channel with B, and then B will update the balance in their payment channel with C.
  - Vice versa, if C wants to send a payment to A, then C will first pay B, and then B will pay A.

Source: https://1ml.com/statistics

Payment Channels

Benefits:

- Privacy: Payments on Lightning are more private than transactions on the public Bitcoin blockchain.
- Speed: Payments on Lightning are received and spendable in milliseconds, rather than minutes or hours.
- Capacity: The Lightning Network can handle more payments per second by several orders of magnitude.

Status:

- In January 2021, the Lightning Network exceeded 16,000 nodes and 1,000 BTC in capacity. As of September 2021, there are more than 25,000 nodes and over 2,000 BTC in capacity.
- See here and here for Lightning wallets and here for recent updates.

Source: https://1ml.com/statistics

Basics of Lightning Technology (BOLT)

The **Basics of Lightning Technology** (BOLT) is the standardized technical specification for the Lightning Network, defining how various implementations can interoperate with each other over the same network. The drafting has been in progress since at least November 2016, when the Lightning request-for-comment (RFC) repository was initialized.

- BOLT #4: Describes the construction of an onion routed packet that is used to route a payment from an origin node to a final node. Onion routing is a method for anonymous data transmission.
- BOLT #5: Describes how channels can be co-operatively or non co-operatively closed, to settle on-chain.
- BOLT #10: Describes a node discovery mechanism.

As with the BIPs and EIPs we covered in Session 3, anyone can contribute. The BOLTs are managed by maintainers of the fully compliant Lightning Network daemon (LND); developers of other clients such as Éclair and c-lightning also contribute and are standard compliant.

Use Case: Streaming Money

October 2016: In 'Bitcoin, Lightning, and Streaming Money,' Andreas M. Antonopoulos talked about "what happens when we start streaming money," and how it will "open up a completely new dimension to money."

November 2020: Adam Curry, popularly known as the "father of podcasting," announced that he would be integrating Bitcoin into his podcasting platform. It utilizes a Lightning-based messenger app called Sphinx to facilitate conversation and micropayments between hosts and their listeners.

December 2020: RaspiBlitz, a project developing Lightning-focused hardware devices and an application suite, noted that they were now supporting "Sphinx Relay Server to join the Podcast 2.0 experiment."

January 2021: Strike Global, a new Lightning-based payment application and service spearheaded by Jack Mallers, launches, with "beta" testing in El Salvador. Bitcoin is later declared legal tender.

Session 5: Bitcoin in Practice – Part 2

6. Forks

Forks come in different types

It would take a whole session to go into detail about forks, and so the topic is currently beyond the scope of this course. The short answer: a fork is a change or divergence in software, a blockchain, or network consensus.

> "They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism"- Satoshi Nakamoto

Note: This week is Bitcoin-centric. Other scalability proposals, including Bitcoin Cash and Ethereum sharding, will be discussed in later sessions.

Learn more: See No. 6 on our further reading list located at the end of the presentation to learn more about forks.

Forks come in different types (cont.)

Soft Forks :

A soft fork is a backwards-compatible change to the Bitcoin protocol wherein nodes opt-in to a tightening / restriction of consensus the rules. Nodes which do not update will continue receiving new blocks and recognising them as valid.

Hard Forks :

A hard fork is a non backwards-compatible divergence in the Bitcoin protocol or block history wherein nodes must adopt new / loosened consensus rules. Nodes which do not update will see blocks produced under the new rules as invalid.

Examples of Soft and Hard Forks

Soft Forks :

Segwit: Already explained that it was introduced as a soft fork.

Pay to Script Hash (P2SH): A soft-fork that resulted in multi-signature wallets on the Bitcoin network.

Hard Forks :

17 June 2016: Following a hack of the DAO, which siphoned away 1/3 of its funds, a rollback was proposed to reverse it and reclaim the funds. Not everyone agreed with this decision. As a result, the Ethereum network split into two cryptocurrencies: Ethereum with the rollback (ETH), and Ethereum Classic without the rollback (ETC). We will discuss Ethereum more in the coming weeks.

DAO: Decentralized Autonomous Organization: a decentralized venture capital fund operating on the Ethereum Platform.

1 August 2017: While the Bitcoin network was about to activate Segregated Witness, a portion of the network followed an alternative non backwards-compatible scaling path of increasing the base block size, without SegWit. This resulted in the fork coin known as Bitcoin Cash (BCH).

Session 5: Bitcoin in Practice – Part 2

7. Conclusions

Conclusions

- The Bitcoin Core reference client is one of several compatible client implementations of the Bitcoin protocol.
- Full nodes maintain a complete and up-to-date copy of the blockchain, in order to perform validation and bootstrap other nodes. Pruned nodes and lightweight clients only download and validate a subset of blockchain data.
- Segregated Witness (SegWit) is a soft fork on Bitcoin which addresses transaction malleability and scalability issues while decreasing transaction fees.
- The Lightning Network is a payment protocol that works as a second layer on top of a blockchain. Since the activation of SegWit, the Lightning Network has been developed as one solution for scaling Bitcoin.
- A hard fork is a permanent divergence in the consensus rules that old nodes cannot follow.
- A soft fork is a backwards-compatible change to the Bitcoin protocol. Nodes that don't opt-in to the new features or tightened rules will still continue to recognize transactions and blocks produced by upgraded clients as valid.

Session 5: Bitcoin in Practice – Part 2

8. Further Reading

Further Reading

1. Bitcoin Core

- https://en.bitcoin.it/wiki/Bitcoin_Core

2. Lightning Network Explained and Adoption

- https://cointelegraph.com/explained/lightning-network-explained
- https://www.coindesk.com/merchants-bitcoin-lightning-network/
- https://cointelegraph.com/news/bitcoins-ln-developer-discloses-the-networks-vulnerability
- https://medium.com/@cryptohuntsman/5-popular-wallets-to-experience-bitcoin-lighting-network-dbff2763028
- https://decrypt.co/9662/bitcoin-lightning-network-hits-10000-nodes

3. SegWit Introduction

- https://blockgeeks.com/guides/what-is-segwit/
- https://cointelegraph.com/explained/segwit-explained

Further Reading

4. Bitcoin Core 0.20.1

- https://bitcoincore.org/en/2020/08/01/release-0.20.1/

5. Consensus Rule Changes & Forks

- https://bitcoin.org/en/developer-guide#consensus-rule-changes
- https://99bitcoins.com/bitcoin-forks/

6. SegWit

- https://p2sh.info/dashboard/db/segwit-usage?orgId=1&from=1514747352245&to=1523206850143
- https://bitcointechtalk.com/transaction-malleability-explained-b7e240236fc7

UNIVERSITY of NICOSIA

Questions?

Contact Us:

Twitter: **@mscdigital**
Course Support: **digitalcurrency@unic.ac.cy**
IT & Live Session Support: **dl.it@unic.ac.cy**