SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Prep. Talk

Blockchain Language Made Simple

Dr. Lo Swee Won

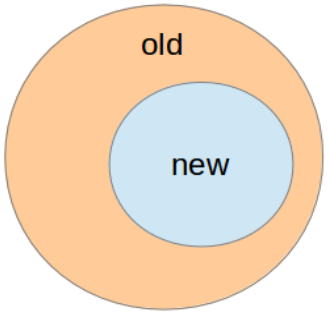
Assisted by Wang Yu

SUSS Blockchain and Fintech Group

Soft and Hard Fork

Soft Fork

- A change to the protocol where only previous valid blocks/transactions are made invalid

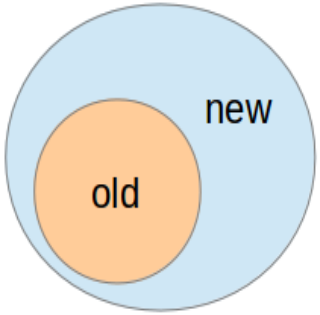


old: 1MB
new: 500kB

- Backwards compatible
- Requires a majority of the miners to upgrade to enforce the new rules

Hard Fork

- A change to the protocol where previous invalid blocks/transactions are made valid (or vice versa)



old: 1MB
new: 2MB

- Not backwards compatible
- Requires all nodes to upgrade and agree on the new version

UASF and UAHF

User Activated Soft Fork (UASF)

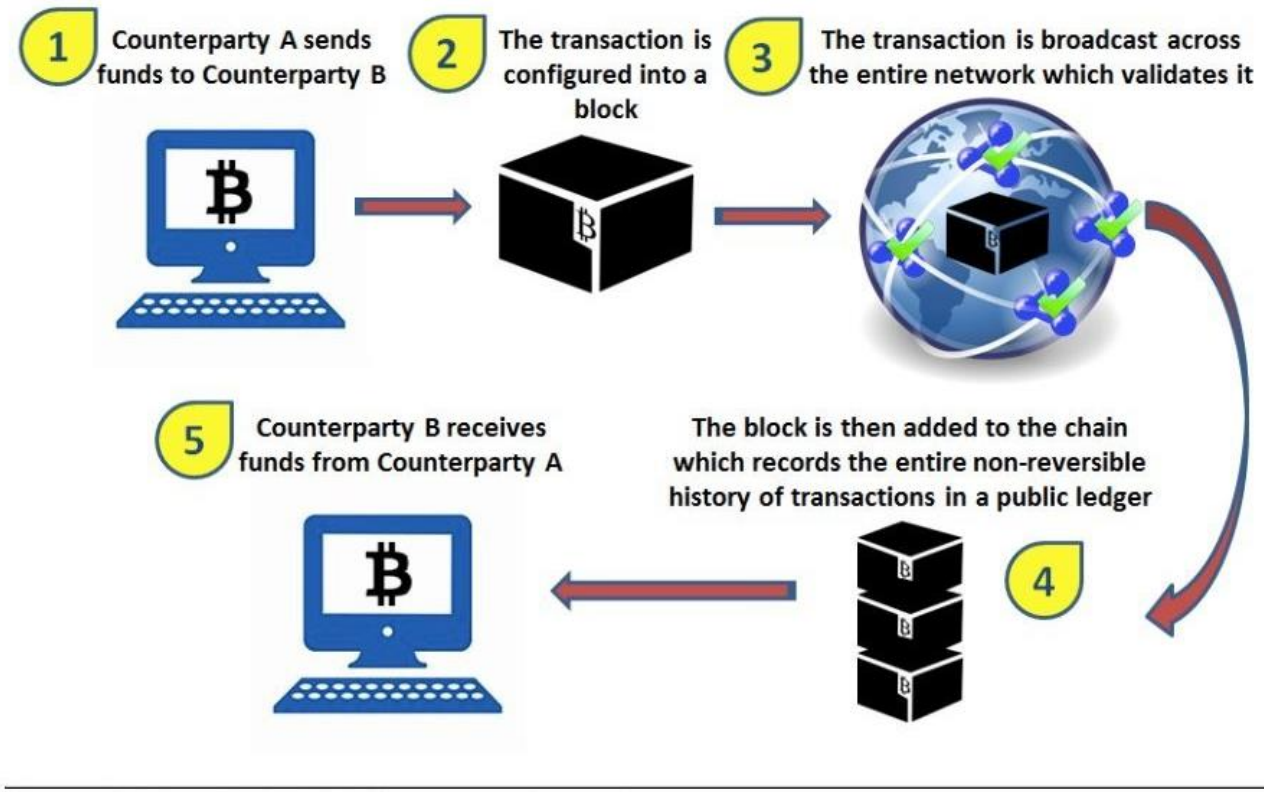
- A Soft Fork activated by flag day and enforced by full nodes instead of miner signalling
- Same features as Soft Fork

User Activated Hard Fork (UAHF)

- Developers add a mandatory rule set to change the node software on a flag day.
- Same features as Hard Fork

Bitcoin Blockchain (1)

Exhibit 1: The Blockchain is a distributed, public ledger, most commonly known as the core underlying technology for Bitcoin



Source: Goldman Sachs Global Investment Research, [Business Insider UK]

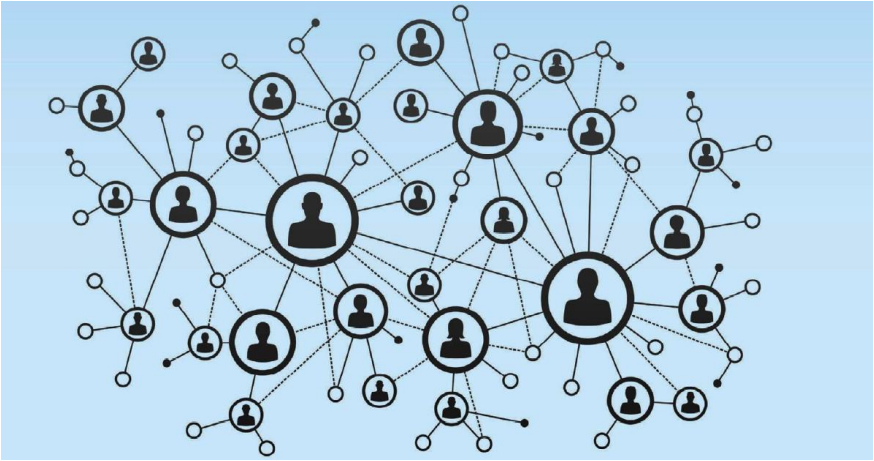
Bitcoin Blockchain (2)

Block Size Limit

- Bitcoin is limited in the number of transactions it can process: 1MB block size, confirmation every 10 min

Consequences

- Longer transaction time
- Higher fees



Segregated Witness (SegWit)

What is SegWit

- A soft fork change in the transaction format of Bitcoin, short for Segregated Witnesses
- The process by which the block size limit on a blockchain is increased by removing signature data from Bitcoin transactions
- Activated on the Bitcoin network on 24 Aug, 2017

Key things that SegWit enables

- It rearranges how data is stored in Bitcoin blocks
- It eliminates transaction malleability, a well-known weak spot in Bitcoin software, making Lightning Network possible

Transaction Malleability

What is Transaction Malleability

- An attack where someone changes the unique ID of a bitcoin transaction before it is confirmed on the bitcoin network.
- The change makes it possible for someone to pretend that a transaction didn't happen, if all the right conditions are in place.

Consequence

- Bookkeeping nightmare
- Paying twice, thrice …
- Longer delay in processing transactions

Segregated Witness (SegWit)

What is SegWit

- A soft fork change in the transaction format of Bitcoin, short for Segregated Witnesses
- The process by which the block size limit on a blockchain is increased by removing signature data from Bitcoin transactions
- Activated on the Bitcoin network on 24 Aug, 2017

Key things that SegWit enables

- It rearranges how data is stored in Bitcoin blocks
- It eliminates transaction malleability, a well-known weak spot in Bitcoin software, making Lightning Network possible

Lightning Network

What is Lightning Network

- A decentralized network using smart contract functionality in the blockchain to enable instant payments across a network of participants
- Implementation of Hashed Timelock Contracts (HTLCs) with bi-directional payment channels which allows payments to be securely routed across multiple peer-to-peer payment channels.

Transactions for the Future

- Instant Payments
- Scalability
- Low Cost
- Cross Blockchains

Bitcoin Improvement Proposal (BIP)

What Is BIP

- Short for Bitcoin Improvement Proposal, a technical document that addresses issues for change in the Bitcoin core client

BIP141 - SegWit

- The original plan for activating SegWit that requires a 95% acceptance rate from the miners to be implemented

BIP91 - SegWit2x

- Looks to lock-in SegWit2x's SegWit update before August 1 and can get activated using 80% of network agreement

UASF BIP148

- A UASF that requires that miners signal for SegWit, which means on the flag date, nodes will start to reject blocks that don't show readiness for BIP141 if BIP148 is supported by a majority of the miners

SegWit2x and Bitcoin Cash

SegWit2x

- Also referred to as the “New York Agreement” or “Silbert Accord”
- Activates SegWit through BIP91 followed by a hard fork to increase the block size to 2MB

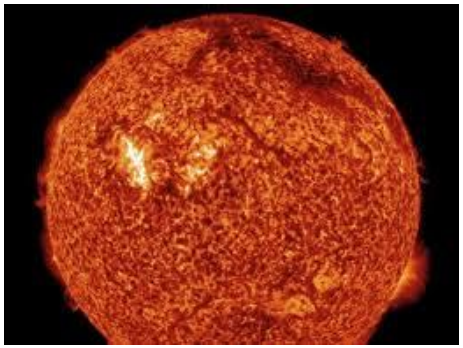
Bitcoin Cash (BCC)

- A token - a user-activated hard fork (UAHF) that bifurcated the Bitcoin blockchain into two branches
- A fork of the Bitcoin blockchain ledger, with upgraded consensus rules that allow it to grow and scale
- It increases the block size to 8 MB and removes SegWit, compared to BTC

The Plasma Framework

What Is Plasma

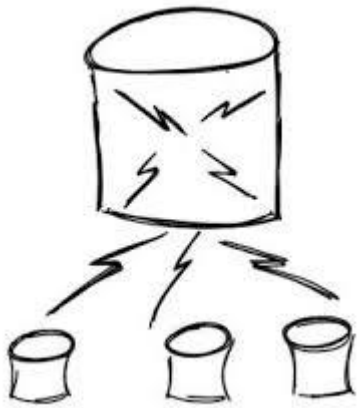
- Ethereum's SegWit
- Eliminates unnecessary data in smart contracts and only broadcast merkelised commitments to the public Ethereum Blockchain



Sharding

What Is Sharding

- An alternative form of validation aiming to solve the labor-intensive or scalability problem associated with Ethereum blockchain, where all nodes on the network store and process all transactions taking place on the network



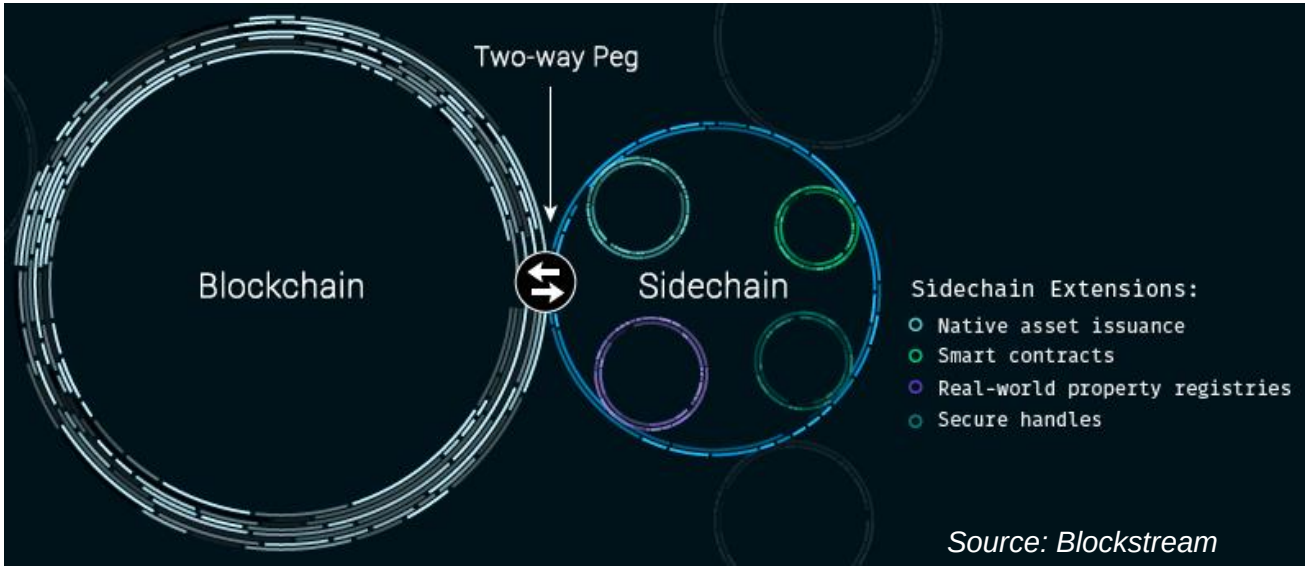
How It Works

- A small subset of network nodes will validate every single transaction

Sidechain

What Is Sidechain

- A innovation of blockchain developed by the startup Blockstream
- A sidechain is a blockchain that validates data from other blockchains and enables transfer between blockchains
- The use of a two-way peg enables coins or other assets to be interchangeable between chains at a fixed or otherwise deterministic exchange rate



RSK

What Is RSK

- Rootstock (RSK) – uses a compatible version of the Lightning Network, known as “Lumino”
- “The first open-source smart contract platform with a 2-way peg to Bitcoin that also rewards the Bitcoin miners via merge-mining”
- RSK is a Bitcoin Sidechain – it carries a separate token pegged to Bitcoin

SUSS
SINGAPORE UNIVERSITY
OF SOCIAL SCIENCES

Thank You.