IT486 v3.0: Blockchains and Cryptocurrencies

Hard and soft forks, Cross-blockchain swaps

Software changes - Hard forks

- Suppose a software change is proposed that will produce blocks that will not be accepted as valid under the old version
- Consider, for example, a change that increases the block size limit from 1 MB to 9 MB
- This is called *hard fork*

Hard fork

- Call the miners running old version legacy miners and the miners running new version upgraded miners

Hard fork

- Call the miners running old version legacy miners and the miners running new version upgraded miners
- Assume an upgraded miner mines a 9 MB block

Hard fork

- Call the miners running old version legacy miners and the miners running new version upgraded miners
- Assume an upgraded miner mines a 9 MB block
    - legacy miners will reject the block
        - continue working on the longest branch which contains only blocks that abide by the old rules

Hard fork

- Call the miners running old version legacy miners and the miners running new version upgraded miners
- Assume an upgraded miner mines a 9 MB block
    - legacy miners will reject the block
        - continue working on the longest branch which contains only blocks that abide by the old rules
    - upgraded miners will accept the block
- This results in a blockchain fork

Hard fork

- Two branches will exist:
  - one branch containing the 9 MB block and
  - the other branch containing only blocks that abide by the old rules

Hard fork

- Two branches will exist:
    - one branch containing the 9 MB block and
    - the other branch containing only blocks that abide by the old rules
- upgraded miners will consider both branches as valid

Hard fork

- Two branches will exist:
  - one branch containing the 9 MB block and
  - the other branch containing only blocks that abide by the old rules
- upgraded miners will consider both branches as valid
- legacy miners see only the branch not containing the 9 MB block

Case 1

- Assume the legacy miners control the majority of the network hashrate
- Then any branch containing blocks which violate the old size limit will eventually be abandoned by the upgraded miners (why?)

Case 2

- Assume the upgraded miners control the majority of the network hashrate
- Then they will abandon the branch not containing the 9 MB block, but this branch will not be abandoned by the legacy miners as it is the only valid branch they see

Case 2

- Assume the upgraded miners control the majority of the network hashrate
- Then they will abandon the branch not containing the 9 MB block, but this branch will not be abandoned by the legacy miners as it is the only valid branch they see
- The fork remains, with both chains being extended forever

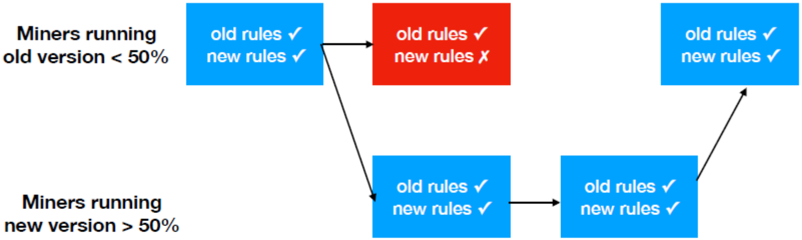
Software changes - Soft forks

- A software change can be effected by a *soft fork* if it restricts the ruleset enforced by miners
- Consider, for example, a change that decreases the block size limit from 1 MB to 500 KB

Software changes - Soft forks

- A software change can be effected by a *soft fork* if it restricts the ruleset enforced by miners
- Consider, for example, a change that decreases the block size limit from 1 MB to 500 KB
- A majority of miners running the new version can outpace the legacy miners, who will accept the longer branch constructed by the miners using the new version
    - there is no risk of two distinct branches emerging when some miners continue to use the old software

Soft fork



Miners running old version < 50%

Miners running new version > 50%

old rules ✓
new rules ✓

old rules ✓
new rules ✗

old rules ✓
new rules ✓

old rules ✓
new rules ✓

old rules ✓
new rules ✓

(red = not accepted by the other camp)

Block size wars

- Proposals to increase the block size limit have led to heated debate

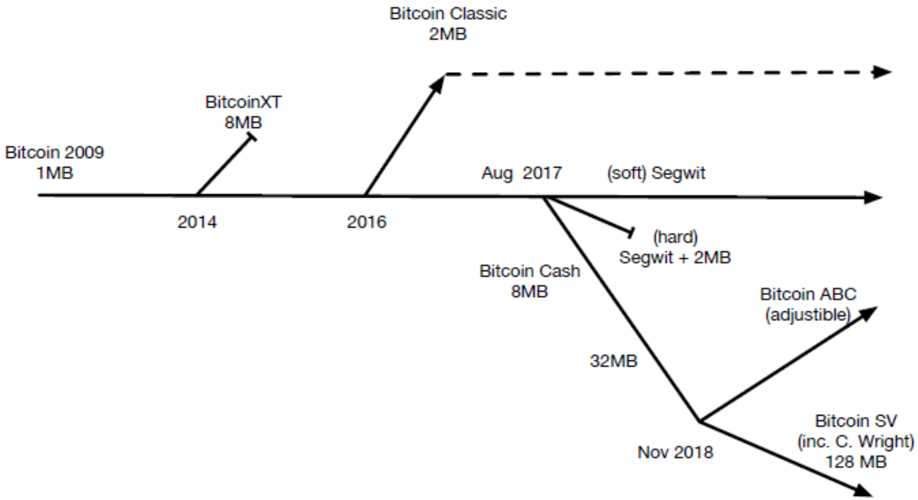
Block size wars

- Proposals to increase the block size limit have led to heated debate
- Argument for:
    - it increases the txn throughput

Block size wars

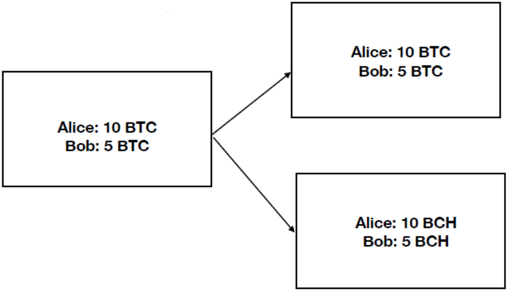
- Proposals to increase the block size limit have led to heated debate
- Argument for:
  - it increases the txn throughput
- Argument against:
  - it requires a hard fork, which risks splitting the community

Prominent blocksize-motivated forks



What happens to money in a hard fork?

- In a hard fork, currency holdings split into two distinct holdings on the two branches



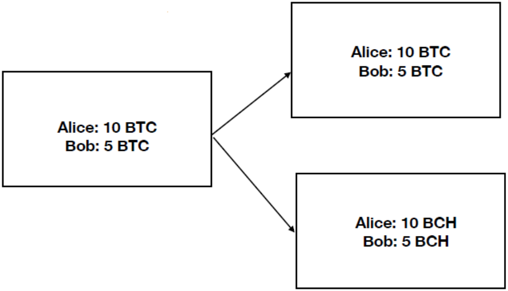
Alice: 10 BTC
Bob: 5 BTC

Alice: 10 BTC
Bob: 5 BTC

Alice: 10 BCH
Bob: 5 BCH

What happens to money in a hard fork?

- In a hard fork, currency holdings split into two distinct holdings on the two branches



Alice: 10 BTC
Bob: 5 BTC

Alice: 10 BTC
Bob: 5 BTC

Alice: 10 BCH
Bob: 5 BCH

- when an exchange controls the private key, it may not distribute the forked value to its users
  - sometimes the exchange collects it for itself!

Exchange value of a forked currency holding

- If a holding forks into two, then:
  - holding → original holding + holding on forked chain
  - total value = value(original holding) + value(holding on forked chain)

Exchange value of a forked currency holding

- If a holding forks into two, then:
    - holding → original holding + holding on forked chain
    - total value = value(original holding) + value(holding on forked chain)
- What is the total value held, in some other currency (e.g. INR)?

Exchange value of a forked currency holding

- Subject to fluctuations, anything can happen to the total value!

Exchange value of a forked currency holding

- Subject to fluctuations, anything can happen to the total value!
- May remain constant

Exchange value of a forked currency holding

- Subject to fluctuations, anything can happen to the total value!
- May remain constant
    - community splits, value follows number of members using currency

Exchange value of a forked currency holding

- Subject to fluctuations, anything can happen to the total value!
- May remain constant
  - community splits, value follows number of members using currency
- May decrease

Exchange value of a forked currency holding

- Subject to fluctuations, anything can happen to the total value!
- May remain constant
  - community splits, value follows number of members using currency
- May decrease
  - overall loss of confidence in cryptocurrency due to fork

Exchange value of a forked currency holding

- Subject to fluctuations, anything can happen to the total value!
- May remain constant
  - community splits, value follows number of members using currency
- May decrease
  - overall loss of confidence in cryptocurrency due to fork
- May increase

Exchange value of a forked currency holding

- Subject to fluctuations, anything can happen to the total value!
- May remain constant
    - community splits, value follows number of members using currency
- May decrease
    - overall loss of confidence in cryptocurrency due to fork
- May increase
    - fork brings in new capabilities / new users

User response to a hard fork

- Options
  - quickly sell off or spend one of the holdings
  - hold both

User response to a hard fork

- Options
  - quickly sell off or spend one of the holdings
  - hold both
- Possible reasons for sell off
  - loss of confidence in crypto-currency
  - expecting a drop in value of what you are selling
  - philosophical opposition/support for a chain's ambition/philosophy
  - speculation

Miner response to a fork

- Options
  - Keep working on the chain you were on
  - Switch to the new chain
  - Distribute your mining power across the two chains
  - Switch your mining power back and forth across the two chains

Miner response to a fork

- Reasons
  - You support the philosophy/ambition of one chain more than the other
  - The majority of the users have gravitated to one of the chains
  - The choice is the one that maximises your profit

Network effect

- The value of an application enabling interactions between users derives in large part from the number of users of that application
- Example: Social media
- The same effect applies to cryptocurrencies
    - the currency/blockchain fork with the larger number of users will tend to be more attractive, so win out in the end

Cross-chain Swap

- Alice has Bitcoin, wants Litecoin
- Bob has Litecoin, wants Bitcoin

Cross-chain Swap

- Alice has Bitcoin, wants Litecoin
- Bob has Litecoin, wants Bitcoin
- Alice trades Bob 1 Bitcoin 1 BTC for 10 LTC

What is an Atomic Swap?

Enables Alice and Bob to trade cryptocurrency, e.g. Bitcoin, such that:

What is an Atomic Swap?

Enables Alice and Bob to trade cryptocurrency, e.g. Bitcoin, such that:

- Atomic:
  - The exchange happens or does not happen, neither party can cheat the other by taking coins without sending coins

What is an Atomic Swap?

Enables Alice and Bob to trade cryptocurrency, e.g. Bitcoin, such that:

- Atomic:
  - The exchange happens or does not happen, neither party can cheat the other by taking coins without sending coins

  Untrusted:
  - No trusted third party is needed

Is this swap atomic?

- Alice as initiator sends Bob her 1 BTC
- Bob as responder sends Alice his 10 LTC

Is this swap atomic?

- Alice as initiator sends Bob her 1 BTC
- Bob as responder sends Alice his 10 LTC
- No! How can Alice be sure that Bob will send 10 LTC to her?

Is this swap atomic?

- Alice as initiator sends Bob her 1 BTC
- Bob as responder sends Alice his 10 LTC
- No! How can Alice be sure that Bob will send 10 LTC to her?
- Note: Bob can cheat Alice, but Alice can't cheat Bob

Atomic Swaps

- What if somehow they could exchange “exactly at the same time”?

Atomic Swaps

- What if somehow they could exchange “exactly at the same time”?
- Create transactions, on both chains
- Add a spending condition, which only can get true on both chains simultaneously (even if chains are totally unrelated)

Step 1: Secret Generation

- Initiator (i.e. Alice) thinks of a random secret S, example:

  correct horse battery staple

- She calculates the hash H of the secret S:

  2259 . . .

Step 2: BTC funding Tx

- Alice sends her funds (1 BTC) into a contract Tx (or funding Tx) on the BTC chain, locking the output

Step 2: BTC funding Tx

- Alice sends her funds (1 BTC) into a contract Tx (or funding Tx) on the BTC chain, locking the output
- Output (i.e. 1 BTC) can be spent EITHER
  - by Bob if he knows S which will hash to the value H
    OR
  - by Alice at some time t_A in future (failsafe refund)

Step 2: BTC funding Tx

- Alice sends her funds (1 BTC) into a contract Tx (or funding Tx) on the BTC chain, locking the output
- Output (i.e. 1 BTC) can be spent EITHER
  - by Bob if he knows S which will hash to the value H
    OR
  - by Alice at some time t_A in future (failsafe refund)
- This type of Tx is called HTLC: hash-time-locked contract

Step 3: LTC funding Tx

- Bob sends his funds (10 LTC) into a contract Tx (or funding Tx) on the LTC chain, locking the output

Step 3: LTC funding Tx

- Bob sends his funds (10 LTC) into a contract Tx (or funding Tx) on the LTC chain, locking the output
- Output (i.e. 10 LTC) can be spent EITHER
  - by Alice if she knows (and provides) the secret S which will hash to the value H
    OR
  - by Bob at some time t_B in future (failsafe refund)

Notes

- What happens if Bob fails to submit his contract Tx?

Notes

- What happens if Bob fails to submit his contract Tx?
- the output from Alice's contract Tx (1 BTC) will be sent back to Alice at time t_A

Steps 4 and 5: LTC/BTC claim Tx

- Alice claims LTC, revealing her secret S

Steps 4 and 5: LTC/BTC claim Tx

- Alice claims LTC, revealing her secret S
- Bob uses S to claim BTC

Notes

- What happens if Alice fails to claim LTC?

Notes

- What happens if Alice fails to claim LTC?
- Output from Bob's contract Tx (10 LTC) will be sent back to Bob at time t_B

What do the two chains need?

- possibility to somehow time-lock funds
- support the same hashing algorithm in the evaluating script
- branching support in scripts (if / else) to realize failsafe path

What do the two chains need?

- possibility to somehow time-lock funds
- support the same hashing algorithm in the evaluating script
- branching support in scripts (if / else) to realize failsafe path
- this is true for most Bitcoin-like chains

Secret size attack

Remember, our secret:

correct horse battery staple

which hashes to:

2259cd5b42ae4d70deaa3d8d2ead2bb32ed3677b

- Is there a limit for the maximum possible length of a secret?
- For Bitcoin: maximum number of bytes pushable to the stack is 520 bytes

Secret size attack

Remember, our secret:

correct horse battery staple

which hashes to:

2259cd5b42ae4d70deaa3d8d2ead2bb32ed3677b

- Is there a limit for the maximum possible length of a secret?
- For Bitcoin: maximum number of bytes pushable to the stack is 520 bytes
- When this limit is different between two chains, an attack is possible

Secret key attack

- Imagine evil attacker Eve owns FantasyCoin FC which allows max. 300 bytes-sized script elements
- Eve and Alice agree to trade 10000 FC against 10 BTC
- Eve creates a secret which is $>$ 300 bytes but $<$ 520 bytes long and hashes it

Secret key attack

- Eve proceeds as discussed before (locks her FC into the Funding TX, informs Alice)
- As soon as Alice has locked her 10 Bitcoin in her Funding TX, Eve can claim them (as planned, because she as initiator knows the secret)

Secret key attack

- Eve proceeds as discussed before (locks her FC into the Funding TX, informs Alice)
- As soon as Alice has locked her 10 Bitcoin in her Funding TX, Eve can claim them (as planned, because she as initiator knows the secret)
- But when Alice now wants to claim her 10000 FC in return, she cannot: although she now knows the secret, she cannot use it, as it's too large to be used in a FC coin script