Forks

MAS.S62
3/5/2018 Lecture 8
Neha Narula
Can a block point to two prev blocks?

No! Only one spot for prev hash
Can two blocks point to one?

Yes! Known as a FORK.
What does this mean?
What does a fork mean?

- Two versions of history
- Possible double spends
- Two currencies!
How do we fix it?

Which is the “right” one?
Over time, one will win
Over time, one will win
prev: 00ce
txns
nonce: 5ffc

prev: 00db
txns
nonce: 582c

prev: 0092
txns
nonce: fd1a

prev: 002b
txns
nonce: 34a8

hash: 00db

hash: 0092

hash: 002b

hash: 001c
Validation Rules

• < 1 MB blocks
• Valid transactions
  – For each input, scriptPubKey + scriptSig evaluates to true (entire script interpreter)
  – nLockTime
• Proof of work
• No double spends
• Block timestamps
• Prev block hash pointers
Changing the validation rules

- Fix bugs
- Major security issues
- New features

Can’t get everyone to upgrade at the same time!
Soft forks

• Backwards compatible
• Only adding new rules: Old-rule nodes will see new-rule blocks as valid
Miners who don’t upgrade might produce invalid blocks, but they will be orphaned.
Hard forks

• Not backwards compatible
• Removing rules: Old-rule nodes will NOT see new-rule blocks as valid
Two chains, possibly forever.
Hard fork vs. Soft fork

• Hard forks are NOT backwards compatible
• Can do combination hard/soft forks
Who controls forks?

• Miners create blocks
• Nodes validate blocks
What happens if a soft fork doesn’t obtain > 50% of hash rate?
Depends on the soft fork! If old-rule blocks are still valid, soft fork gets reorg’d out.
If old-rule blocks are now invalid, fork will persist
If soft fork > 50%, old-rule blocks will follow new fork automatically
What happens if a hard fork doesn’t obtain > 50% of the hash rate?
Again depends, but if old-rule blocks are still valid, new-rule nodes will follow along
What happens if a hard fork does obtain > 50% of the hash rate?
SPV wallets and forks

• SPV wallets see:
  – Block headers: prev, nonce, merkle root, ts
  – Merkle paths

• What happens during a fork?
Soft forks in practice

• Lots! P2SH, Segwit, OP_CHECKSEQUVERIFY
Hard forks in practice

• New Bitcoins (Bitcoin Cash, Bitcoin Gold, Bitcoin Diamond)
• Ethereum DAO hard fork
• Some cryptocurrencies hard fork frequently (Monero, every 6 months)
Ethereum DAO hard fork

• Block 1920000 transferred ~12M ETH from one set of accounts to another for reclamation
• 85% of mining power went along with it
• Two currencies: ETH and ETC (~30:1 today)
Summary

- Forks are extremely challenging
- Quite different than traditional consensus
- Next class: Sharon Goldberg on P2P network