Litecoin:
SegWit and the Future

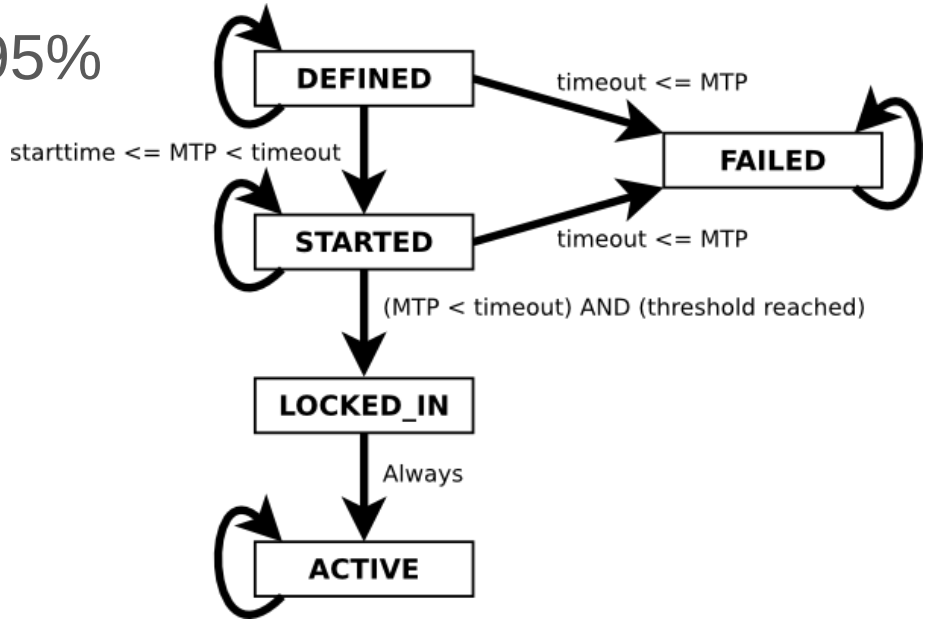
Charlie Lee
10/23/2017

Segregated Witness (SegWit)

- Fixes transaction malleability
- Fixes quadratic signature hashing bug
- Makes signatures prunable
- Makes future upgrades soft forks
  - Schnorr Sigs
  - Confidential Transactions
- Increase block size ~2x
- Just a soft fork

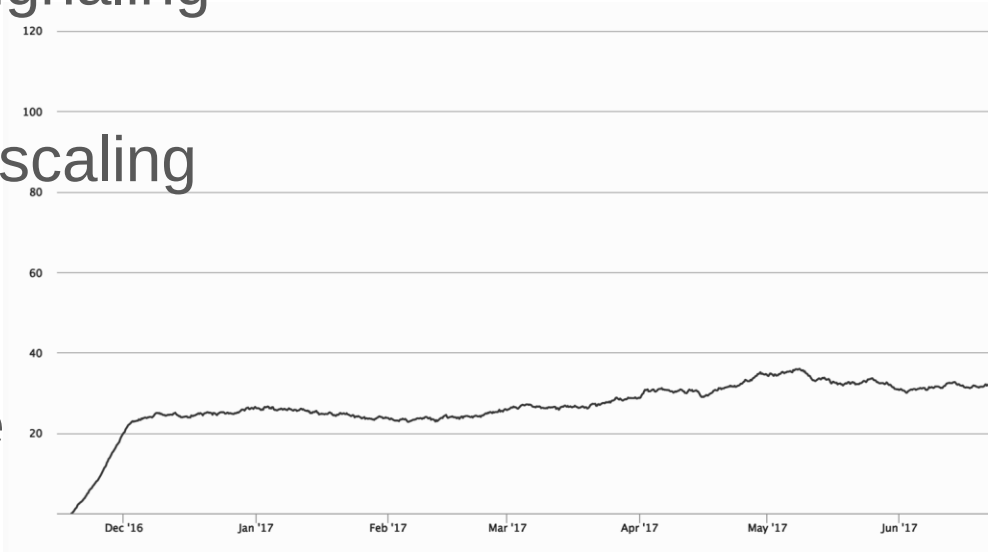
Miner Activation Soft Fork (BIP9)

- Non-controversial soft fork upgrade
- Speed up activation
- Safest way to upgrade at 95%
- Signaling, not voting



Scaling Stalled

- Miner voting instead of signaling
- SegWit stalled
  - Miners want onchain scaling
  - Threatened by LN
  - Asicboost useless
- Community held hostage



SegWit derailed by FUD

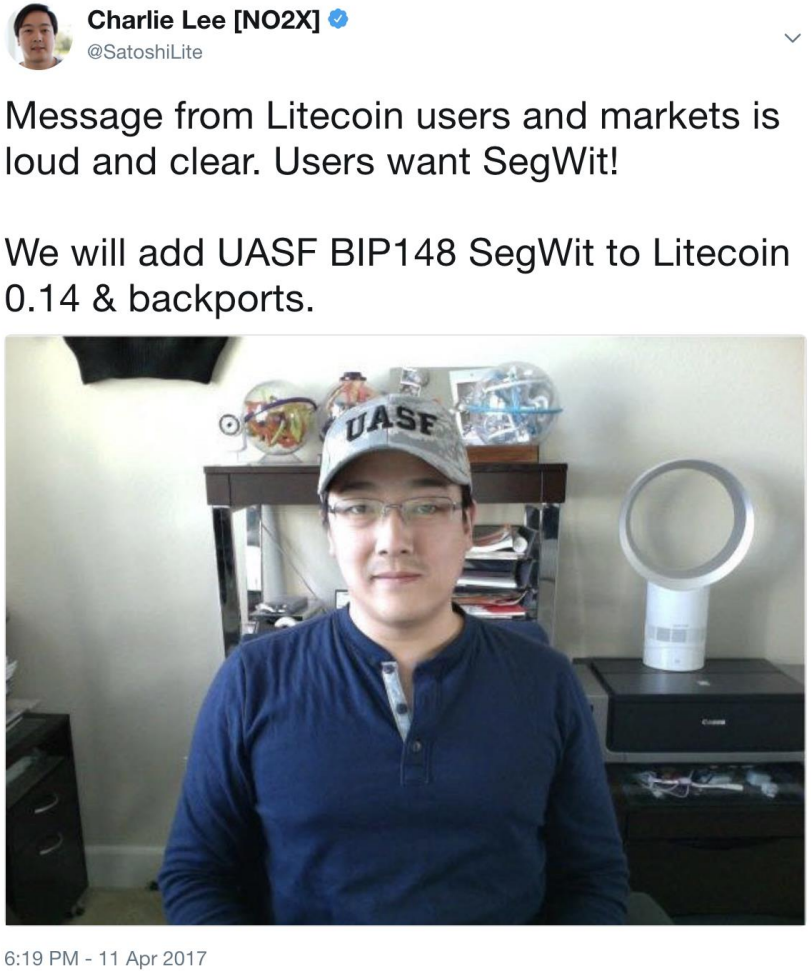
- Anyone-can-spend
- No longer a chain of signatures
- Patent lawsuits
- SegWit is not a blocksize increase

Opportunity for Litecoin

- Benevolent dictator
- Test SegWit on Litecoin
  - Market wants SegWit
  - SegWit is safe
  - Lightning Network

User Activated Soft Fork

- Miner blocking activation
- UASF threat
- Compromise



Future

- BIP8 activation
- Lightning Networks
- RootStock EVM sidechain
- MAST
- Confidential Transactions
- Schnorr signatures
    - Signature aggregation

Q&A