

Blockchain Forks

How to upgrade a network

Leonhard A. Weese

President, Bitcoin Association of Hong Kong

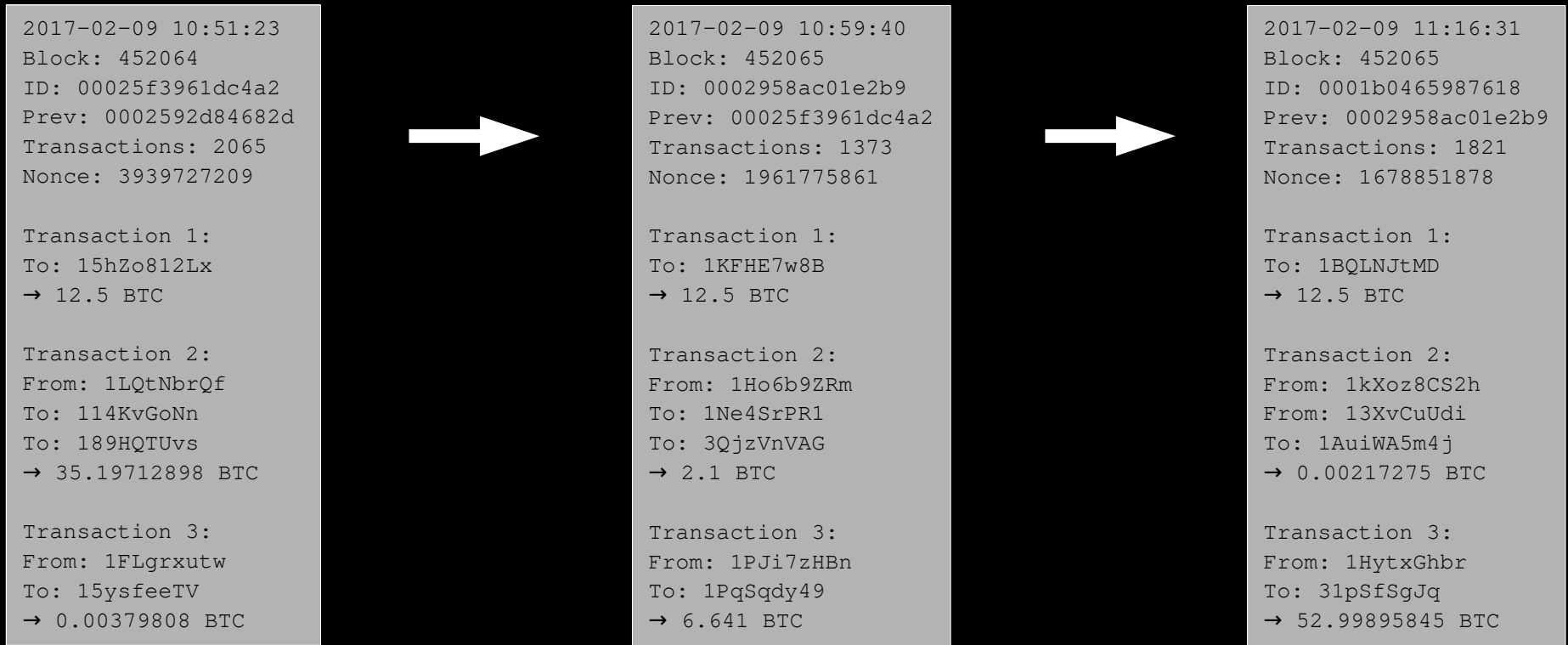
leo@bitcoinhk.org

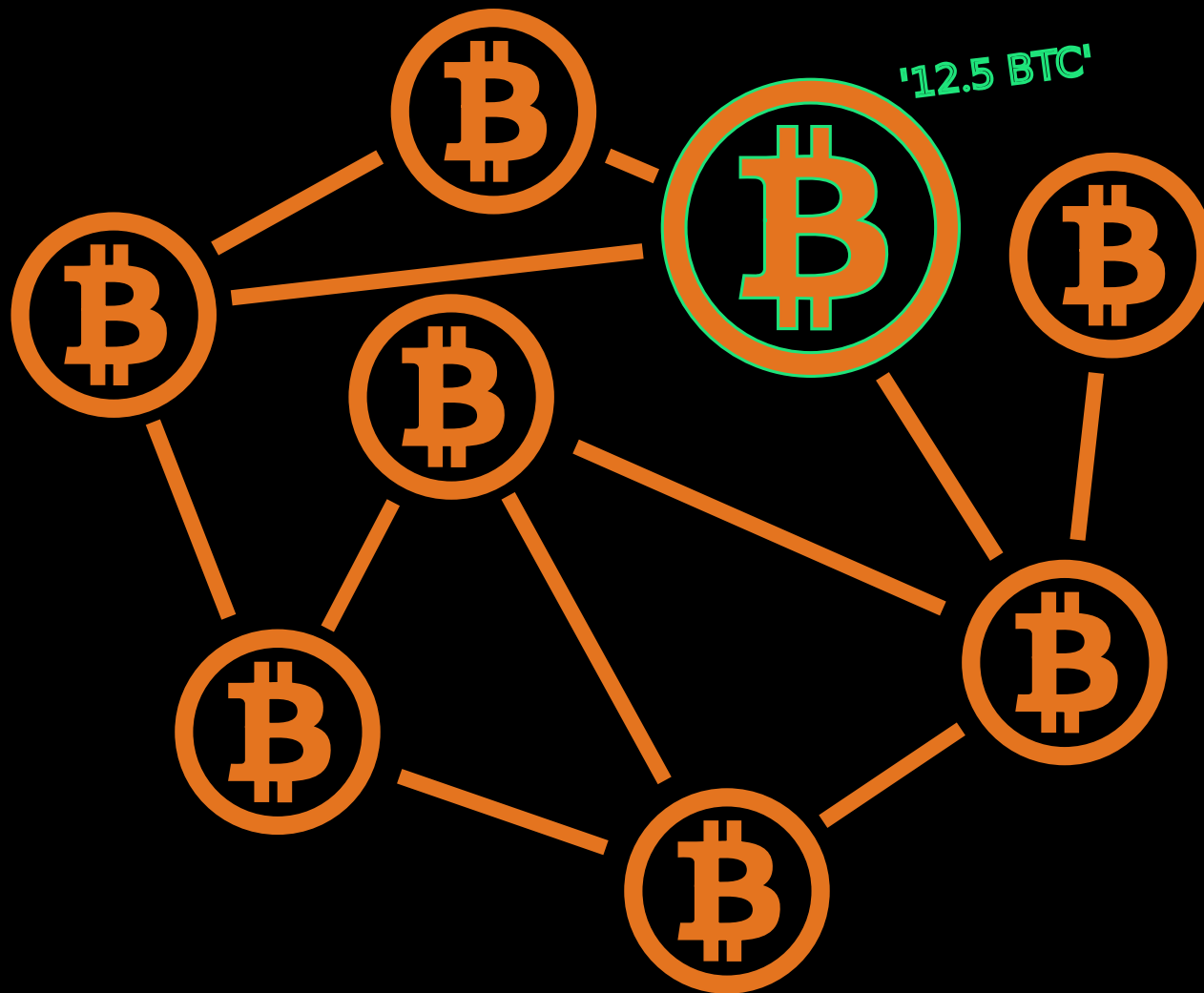
Blockchain forks

- 1) Consensus
- 2) Software forks
- 3) Consensus rule forks
- 4) Chain splits/forks
- 5) How to activate a fork
- 6) History of forks
- 7) Practical Advice

1) Consensus

- Every 10 mins a new block is added to the chain





Validating nodes

- Anybody can run a validating node at low cost
- Your node will accept or reject blocks & transactions
- A miner can theoretically put anything into a block
- But will it get accepted?

2) Software forks

- A software upgrade under a different name, or released by a different team
 - Development branch (forks later are merged)
 - Schisms
 - Often compatible
 - Different from new implementations
- eg: Wikitravel → Wikivoyage

Articles of Association

3) Consensus rule fork

- Are the **new blocks** accepted by old nodes?
- Are the old blocks accepted by **new nodes**?
- Tightening rules (Soft Fork)
- Broadening or removing rules (Hard Fork)
- Software forks **proposing consensus rule forks**:
Bitcoin Unlimited, Bitcoin Classic, Bitcoin XT

Problems with forks

- Require a high degree of consensus
- Require a high degree of testing
- Who is accepted to take the political lead?
- Can result in chain splits/forks

4) Chain splits/forks

- Also called:
 - Network split/fork
 - **Coin split**
- Occurs when two chains are built on the same block
- Biggest risks:
 - Naming conventions
 - Replay attacks
 - Exchanges not releasing your 'other' coins
 - Intransparent SPV software
 - **General confusion**

Soft vs hard forks

- Soft Forks:
 - Tighten the rules
 - New blocks accepted by old nodes
 - Old blocks may be accepted by new nodes
 - Coercive, little way to oppose them for minority
- Hard Forks
 - Broaden the rules
 - New blocks not accepted by old nodes
 - Old blocks accepted by new nodes
 - Trivial to oppose, easily lead to chain splits

5) How to fork

- “Economic Majority”
- Flag day
- User voting
- Miner voting
- Just do it (responsibly)
 - Why do we stay on the same chain?

6) History of Bitcoin forks

- July 15, 2010 (1MB Limit)
- October 2011 (Litecoin)
- April 2012 (BIP 16, Multisig)
- March 2013 (Bitcoin 0.8.0)
- July 2015 (BIP 66, DER Signatures)
- ??? (BIP 148, Segwit)

7) Practical advice

- Keep your coins off an exchange!
- Be careful with block explorer and SPV wallets
- Run a node
- Don't worry

More practical advice

扣好安全帶



扣好安全帶
buckle up

BUCKLE UP

Leonhard A. Weese
President, Bitcoin Association of Hong Kong
leo@bitcoinhk.org
[@LeoAW](#)

<https://www.bitcoinhk.org>

PGP: A087 7877 C0CF E886 1B35 118D 832E 6328 4080 D73A

icons from iconfinder.com