Bitcoin Transactions and Lightning Network

Kwinten De Backer

July 28, 2018

Overview

- Bitcoin Transactions
- 2 The double spending problem
- 3 Problems with scalability
- The Lightning Network
- 5 The real mindblowing stuff

Kwinten De Backer Lightning Network July 28, 2018 2 / 24

General format of a Bitcoin transaction

Kwinten De Backer Lightning Network July 28, 2018 3 / 24

Inputs

Outputs

Verification

Kwinten De Backer Lightning Network July 28, 2018 6 /

What does it mean to own Bitcoin?

Kwinten De Backer Lightning Network July 28, 2018 7 / 24

Pay to public key hash

Kwinten De Backer Lightning Network July 28, 2018 8 / 24

Pay to script hash

Kwinten De Backer Lightning Network July 28, 2018 9 / 24

Mining (short)



Kwinten De Backer Lightning Network July 28, 2018 10 / 2

Transaction fees

Confirmation delay

Kwinten De Backer Lightning Network July 28, 2018 12 / 2

Blockspace and decentralization

Kwinten De Backer Lightning Network July 28, 2018 13 / 24

Lightning on a conceptual level

Kwinten De Backer Lightning Network July 28, 2018 14 / 24

Payment channels

Kwinten De Backer Lightning Network July 28, 2018 15 / 24

Payment channel network (naive)

Kwinten De Backer Lightning Network July 28, 2018 16 / 24

Payment channel network (better)

Kwinten De Backer Lightning Network July 28, 2018 17 / 24

Lightning problems and solutions

Kwinten De Backer Lightning Network July 28, 2018 18 / 24

Cross chain atomic swaps

Kwinten De Backer Lightning Network July 28, 2018 19 / 24

Submarine swaps

Kwinten De Backer Lightning Network July 28, 2018 20 / 24

Oracles



Kwinten De Backer Lightning Network July 28, 2018 21 / 24

Channel Factories



Kwinten De Backer Lightning Network July 28, 2018 22 /

References



John Smith (2012)

Title of the publication

Journal Name 12(3), 45 - 678.

Kwinten De Backer Lightning Network July 28, 2018 23 / 24

The End