SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

Session 5:

Fundamentals of Blockchain

Module 2 – DLT, Transactions Ordering and Authentication

Bitcoin Whitepaper – 2008

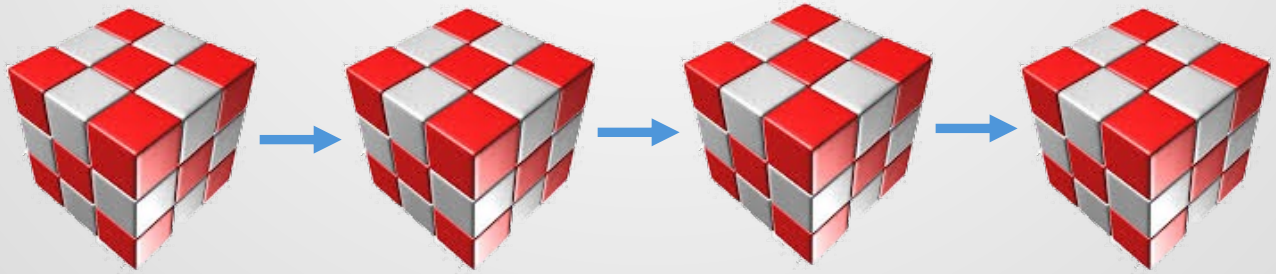
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest

So, What is Blockchain?

Blockchain is a secure transaction ledger database (initially made to facilitate currency exchanges) shared by all the members participating in a distributed network of computers. (LSTA)



What is Bitcoin?

A bank keeps names and account balances
→ The bank wants to know how much one can spend based on his balance

Ledger

Alice	5.3
Bob	100
Frank	700
Carlos	3
Jane	1.3
Charlie	4.645
Scott	.00000001
Kristin	1

Instead of balance, DLTs like Bitcoin keep the transaction records

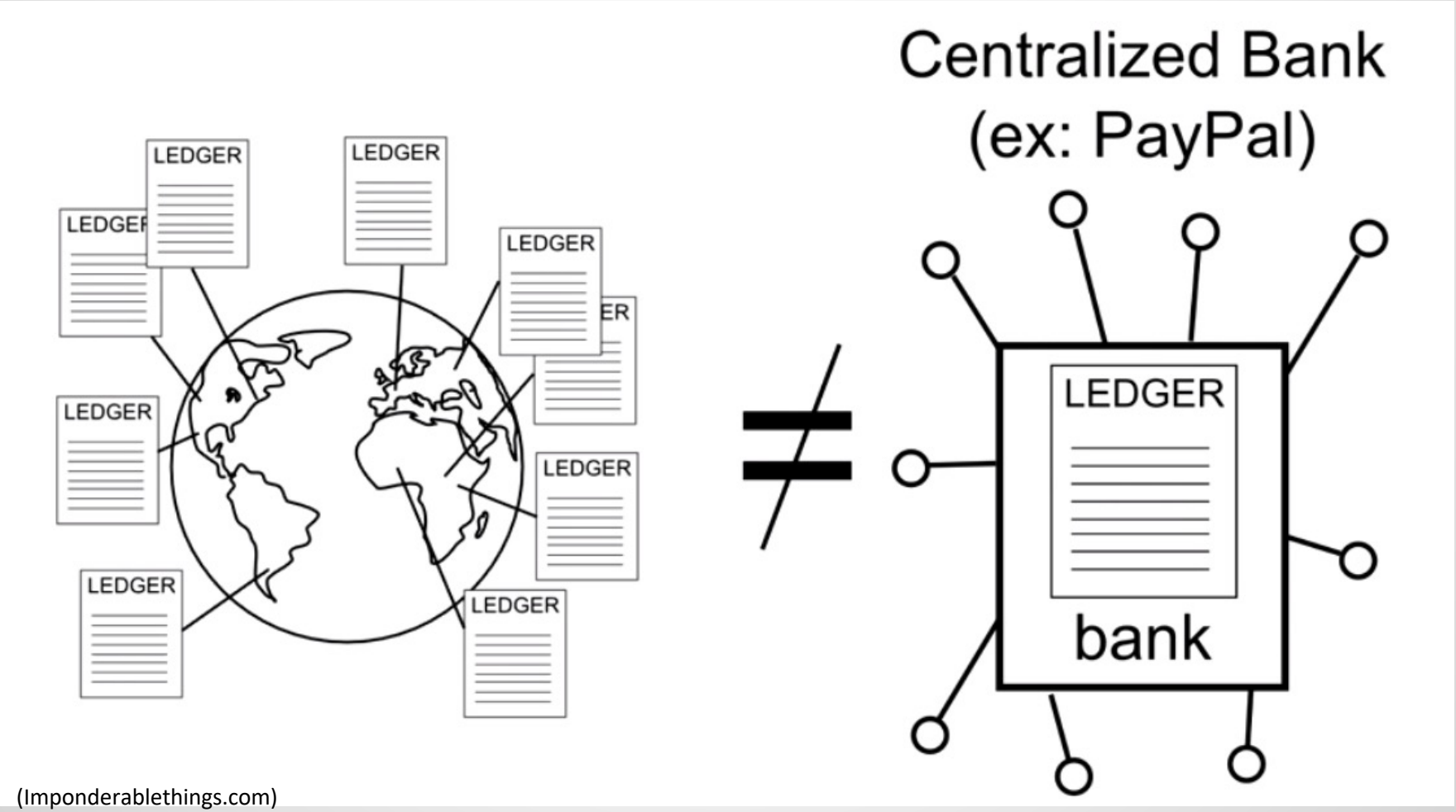
Ledger

Alice
Bob
Frank
Carlos
Jane
Charlie
Scott
Kristin

Transaction
Alice →2B → Bob
Bob →1B → Frank
…

Where are the Transactions Kept?

Copies of transaction records are kept in multiple nodes in the network, in contrast to banks which keep them centralized.



(Imponderablethings.com)

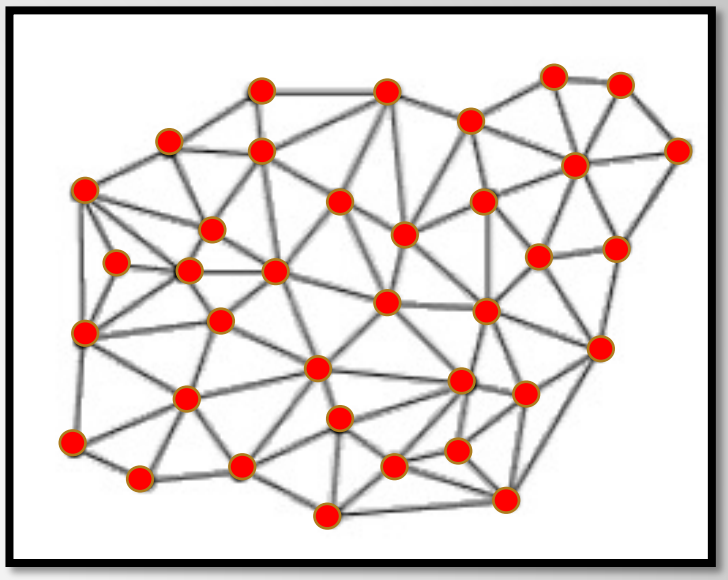
Example: Transferring Money

Alice wants to give Bob 5 Bitcoins:

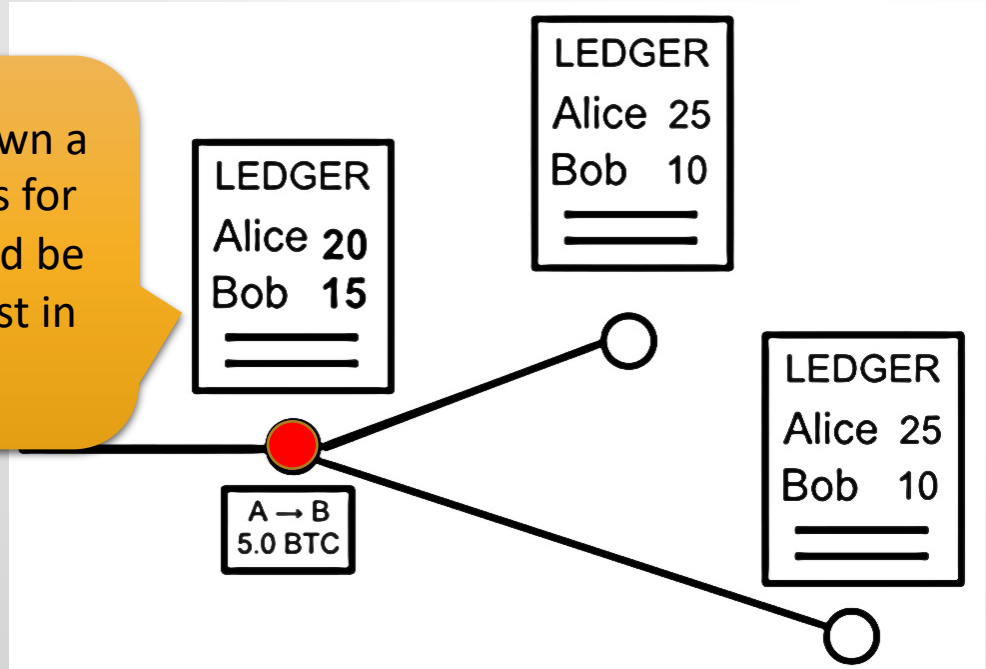
Alice → Bob 5.0 BTC

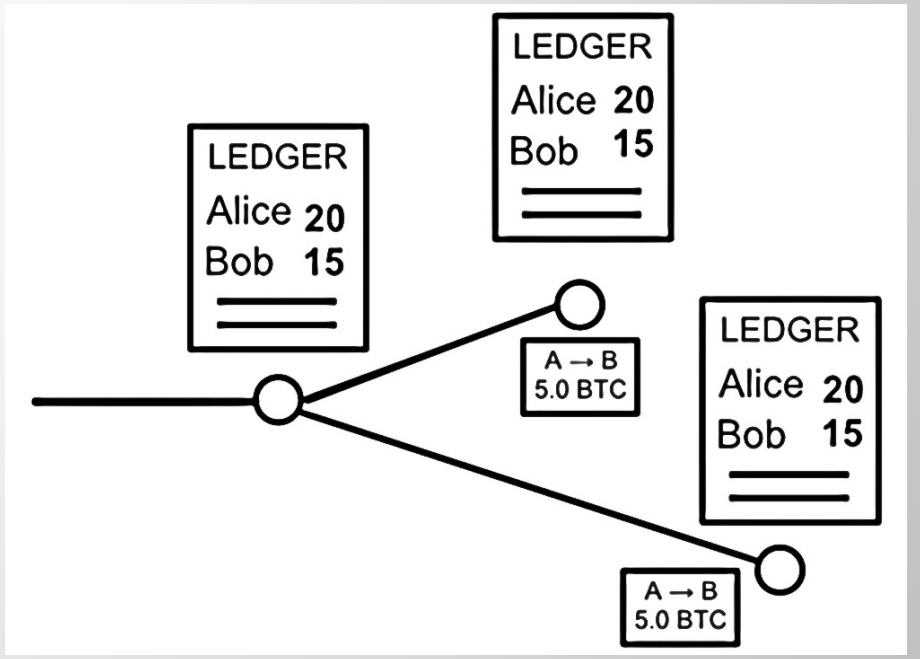
She puts this transaction on a ledger and sends it to everybody she knows, and those will forward the transaction to everybody else so that everyone can update their copy of transactions .

How transactions are flooded



Here, we have shown a ledger by balances for simplicity. It should be the transactions list in practice.





Transaction Record Authentication

- How do the nodes make sure that “A” has really sent the message (and spent the money)?
  - By Digital Signature!
  - Everyone can have multiple pairs of keys in order to use a new signature in every purchase to prevent tracking of his purchases. But still they can be linked!

You don’t send someone the money. You actually send it to a public key!

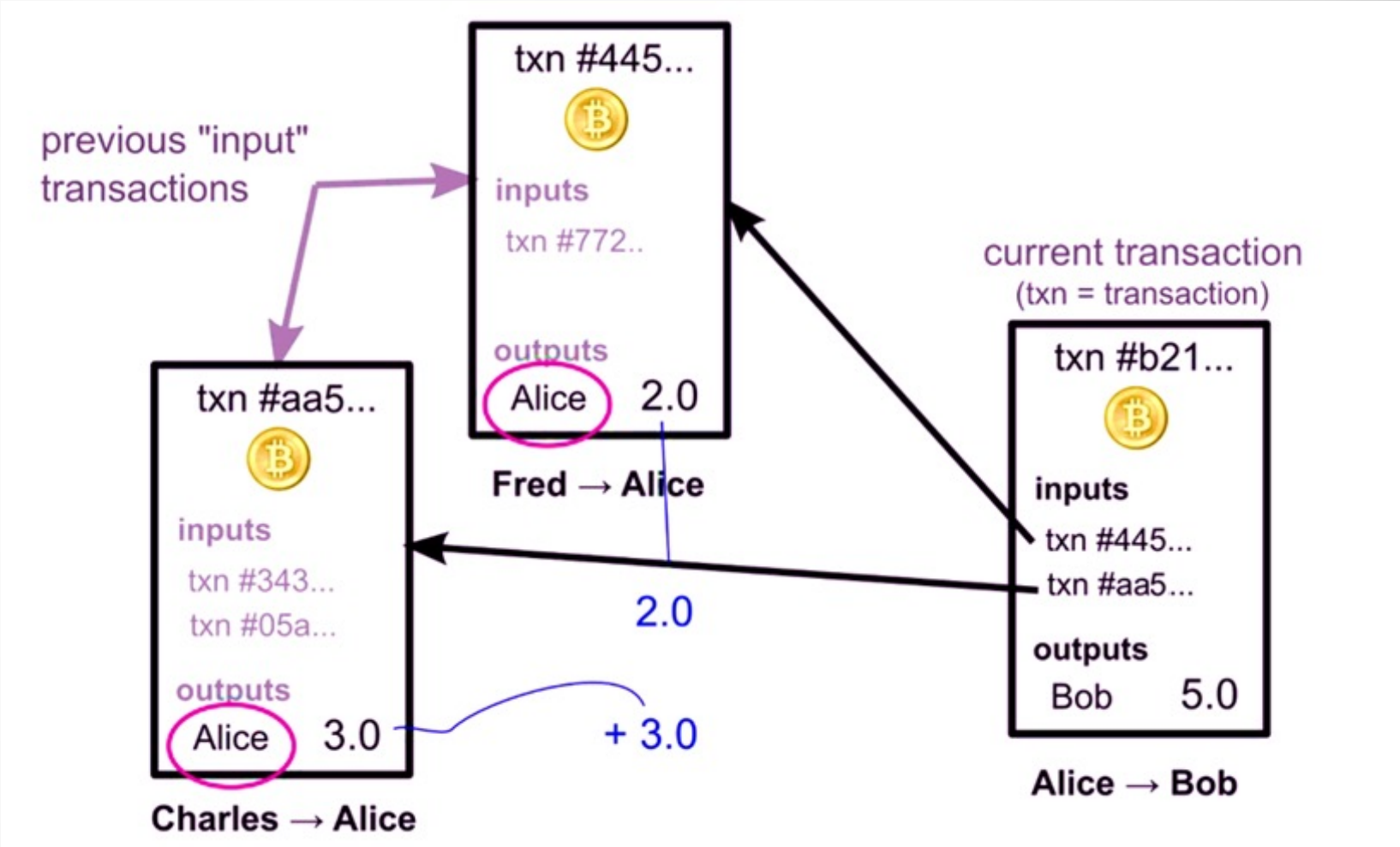
Transaction Record Authentication

- So for message authentication, Digital Signature is used.
  - For Bitcoin:
    - Elliptic Curve Digital Signature Algorithm (ECDSA)
    - The hash function is usually SHA-256

- To prove you have the money, you have to sign a message with the private key corresponding to the public key which the money has been given to (according to the previous records).

How does Alice prove she has the money to spend?

- There is no balance!
- Instead, Alice mentions the previous (input) transactions.
  - Everybody can verify (by signatures) that she has received 5 bitcoins (from Charles and Fred).



What happens if I lose my private key?

If you lose your private key, e.g. in a hard drive crash, the bitcoin money is lost forever!

A Real (Bitcoin) Transaction

Previous transactions that prove A has 12.074 BTC

Every transaction has a signature to prove the ownership of money.

Inputs

Previous output (index)	Amount	From address	Type	ScriptSig
e631567f352f...:1	3.02887912	1CGVyAgAx9gg1va5pGNVJtF6gdKpPUVTSf	Address	304402201700305a3d79a[....]2b985b15daa0ab9c50cd61449ca037dc9f0
c284ec14325f...:0	3.04042789	1GY84QPLfM9d4KqTjTbbHsb9BX9FF1kYQx	Address	3045022100e724004f2d3[....]91d95b56ad29f817f3e3259daffbd72f2a98
0fbec1d29b8e...:0	2.99934316	1CGVyAgAx9gg1va5pGNVJtF6gdKpPUVTSf	Address	304402200f6e9b4281cb0[....]2b985b15daa0ab9c50cd61449ca037dc9f0
232715b3c51a...:1	3.00515088	17ALqzZFPbSqXz9aQhzgK6ts9htZfV8Mwu	Address	304402207311495478c1d[....]8d4656bf7613d47dd4e6a5b062d9fb6a34

Outputs

Output goes to two addresses, one can be for the change that goes back to the sender (via a shadow address).

Index	Amount	To address	Type	ScriptPubKey
0	0.51682435	1LUHXNTsHPUGVJJeefPdb2rpdxtWoHrcKv	Address	OP_DUP OP_HASH160 d5936a017660c48be2adaa9a77153ec[illegible] OP_EQUALVERIFY OP_CHECKSIG
1	11.5569767	1HzAb4E1kZH4pDKoxML4KXBLPPyUootw4s	Address	OP_DUP OP_HASH160 ba51b9aee7595c72a2cbc1d4e3e90e356f77804 OP_EQUALVERIFY OP_CHECKSIG

What Comes Next …

- We learned about distributed ledgers and transactions.
- We also learned how transactions are authenticated by asymmetric cryptography.
- In the next video, we explain Bitcoin details by starting from the problem of consensus and the problems not having it creates.

See you in the next video …