Bitcoin: A Peer-to-Peer Electronic Cash System

Paper review

Bea Botyanszki

The original bitcoin paper

- Published on The Cryptography Mailing list, in 2008
- By Satoshi Nakamoto
  - Identity unknown, but probably not a single person, but a group of people

- The open-source bitcoin software was released in 2009

“

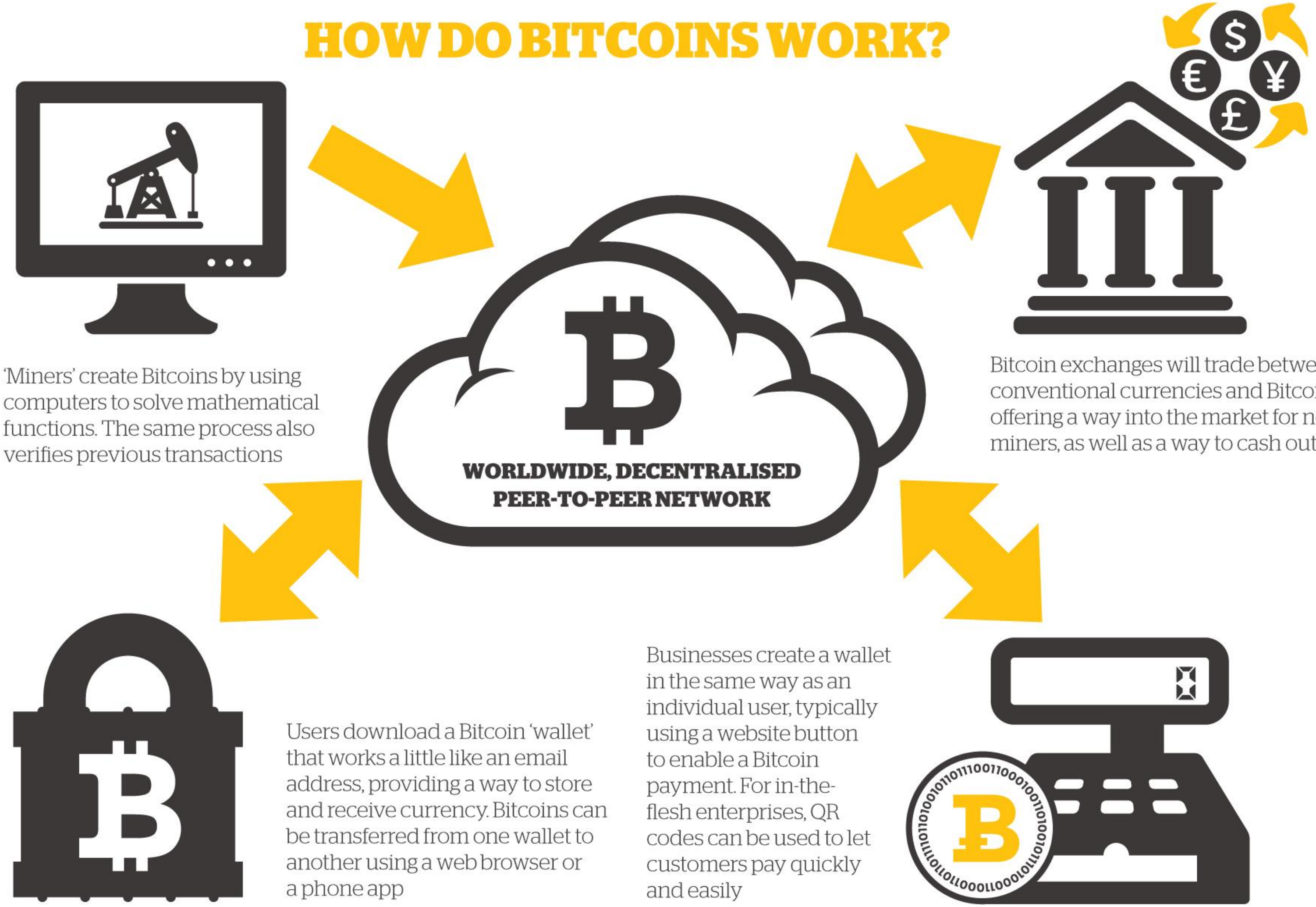
What is needed is an electronic payment system based on cryptographic proof instead of trust…

Motivation & proposed solution

- Commerce on the Internet relies on trusted third parties, to prevent double-spending

- In the paper, the author(s) propose a solution, which uses peer-to-peer network where:
  - Online payments to be sent directly from one party to another
  - Transactions are verified by network nodes in the **block chain**
  - Nodes can join and leave on will

HOW DO BITCOINS WORK?



WORLDWIDE, DECENTRALISED PEER-TO-PEER NETWORK

'Miners' create Bitcoins by using computers to solve mathematical functions. The same process also verifies previous transactions

Bitcoin exchanges will trade between conventional currencies and Bitcoin, offering a way into the market for non-miners, as well as a way to cash out

Users download a Bitcoin 'wallet' that works a little like an email address, providing a way to store and receive currency. Bitcoins can be transferred from one wallet to another using a web browser or a phone app

Businesses create a wallet in the same way as an individual user, typically using a website button to enable a Bitcoin payment. For in-the-flesh enterprises, QR codes can be used to let customers pay quickly and easily

Rules of the network

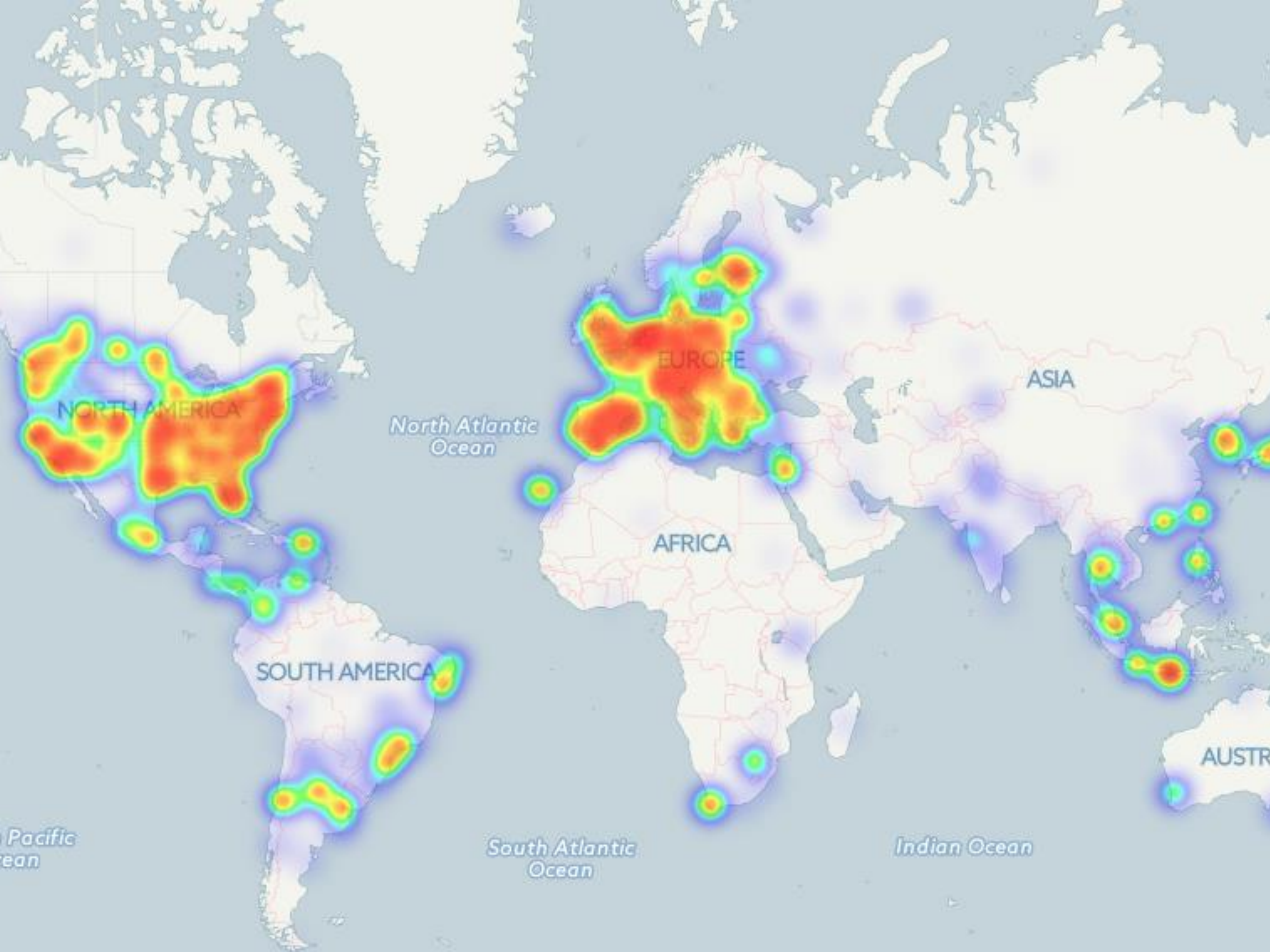
1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block. ➡ 25 BTC reward if successfull
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Incentive & attack

- The successful miner finding the new block is rewarded with newly created BTC and transaction fees.
- The reward for adding a block will be halved approximately every four years. Eventually, the reward will decrease to zero, and the limit of BTC (21 million)will be reached
- A posible weakness of the system: the **51% attack**
  - An attaker gains hashpower up to 51% of the system
  - This would collapse the currency

Summary

- The author(s) have proposed a system for electronic transactions without relying on trust.
- In the system nodes work all at once with little coordination. They can join or leave on will
- Bitcoin is peer-to-peer network, it uses proof-of-work to record a public history of transactions .


NORTH AMERICA
North Atlantic Ocean
EUROPE
ASIA
AFRICA
SOUTH AMERICA
AUSTR
Pacific
ean
South Atlantic Ocean
Indian Ocean