BLOCKCHAIN APPPLICATIONS & SMART CONTRACTS

Course Overview

Relevance

Foundations: Bitcoin

Disruptive potential of Blockchains Internet of Value

Arthur Adamopoulos, Huy Doan, Son Ha

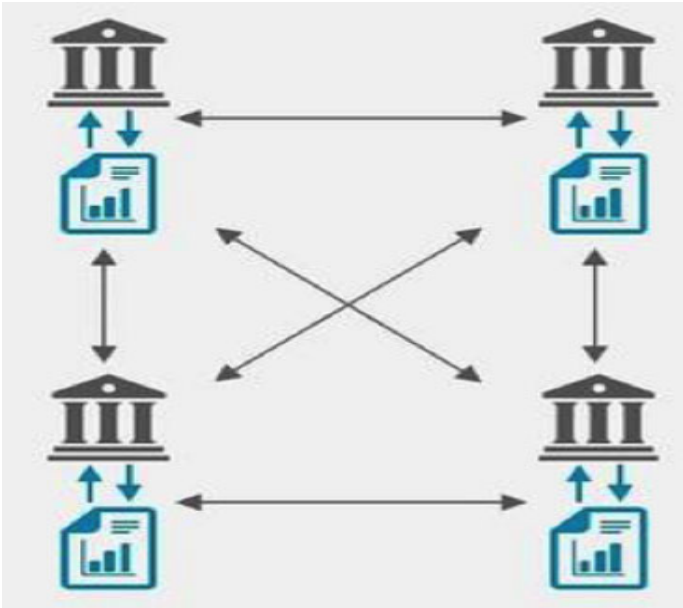
Course Organisation

(discussed in tutorial 1)

- 1-hour online lecture
- Watch video and watch/read references.
- Technical, hands-on course.
- All tasks can be completed on your own device and on cloud services.
- Help available during tutorials or email your respective lecturer
- Go through Canvas Shell

What is a BLOCKCHAIN ?

- The term “Blockchain” is widely used and abused to mean anything related to technologies based on Bitcoin
- Distributed Ledger Technologies (DLT) is probably a better term but ‘Blockchain’ sounds better for marketing
- A Blockchain platform usually consists of:
  - Peer-to-peer network of nodes
  - Replicated, read-only database (the ledger)
  - Consensus algorithm
  - Cryptography
  - Virtual Machine (smart contracts)



Forms of Blockchains

- Cryptocurrencies
  - Bitcoin and thousands of variations
  - Litecoin, Ripple, Dogecoin etc etc
  - Blockchain records transfers of balances
- Smart contract platforms
  - Ethereum, Hyperledger, EOS
  - Blockchain includes balances and also executable code logic (smart contracts).
- All are Open Source

What is Bitcoin ?

- The first currency BORN from the Internet

- How Bitcoin Works:

http://www.youtube.com/watch?v=t5JGQXCTe3c

Watch the above video, it is only 5 minutes long but gives an excellent overview of how Bitcoin works

- New block created approx. every 10 minutes
- Only 21,000,000 bitcoins will ever be created

Who Invented Bitcoin ?

- Bitcoin was created by an anonymous person or people going by the name ‘Satoshi Nakamoto’, who has since disappeared from the scene.
- Original White Paper:
  - https://bitcoin.org/bitcoin.pdf
- The code is currently managed by a group of volunteer programmers.

Not this Guy!

Bitcoin is Open Source

- Code can be downloaded by anyone.
- https://github.com/bitcoin/bitcoin

- This means that anybody can clone bitcoin and replicate the bitcoin network.
- This has led to thousands of other coins being launched:
  - Litecoin
  - Dogecoin
  - Darkcoin
  - BBQ Coin

  - http://Coinmarketcap.com
  - http://www.coinwarz.com/cryptocurrency

There are actually no Coins

- Despite the name, there are no actual coins.
- The blockchain stores balances associated with each address, and transactions transfer balances from one address to another.
- Wallets do not contain any balances or coins either.
- All balances exist in the blockchain that is the core of the bitcoin network.
- A wallet only contains public and private keys.

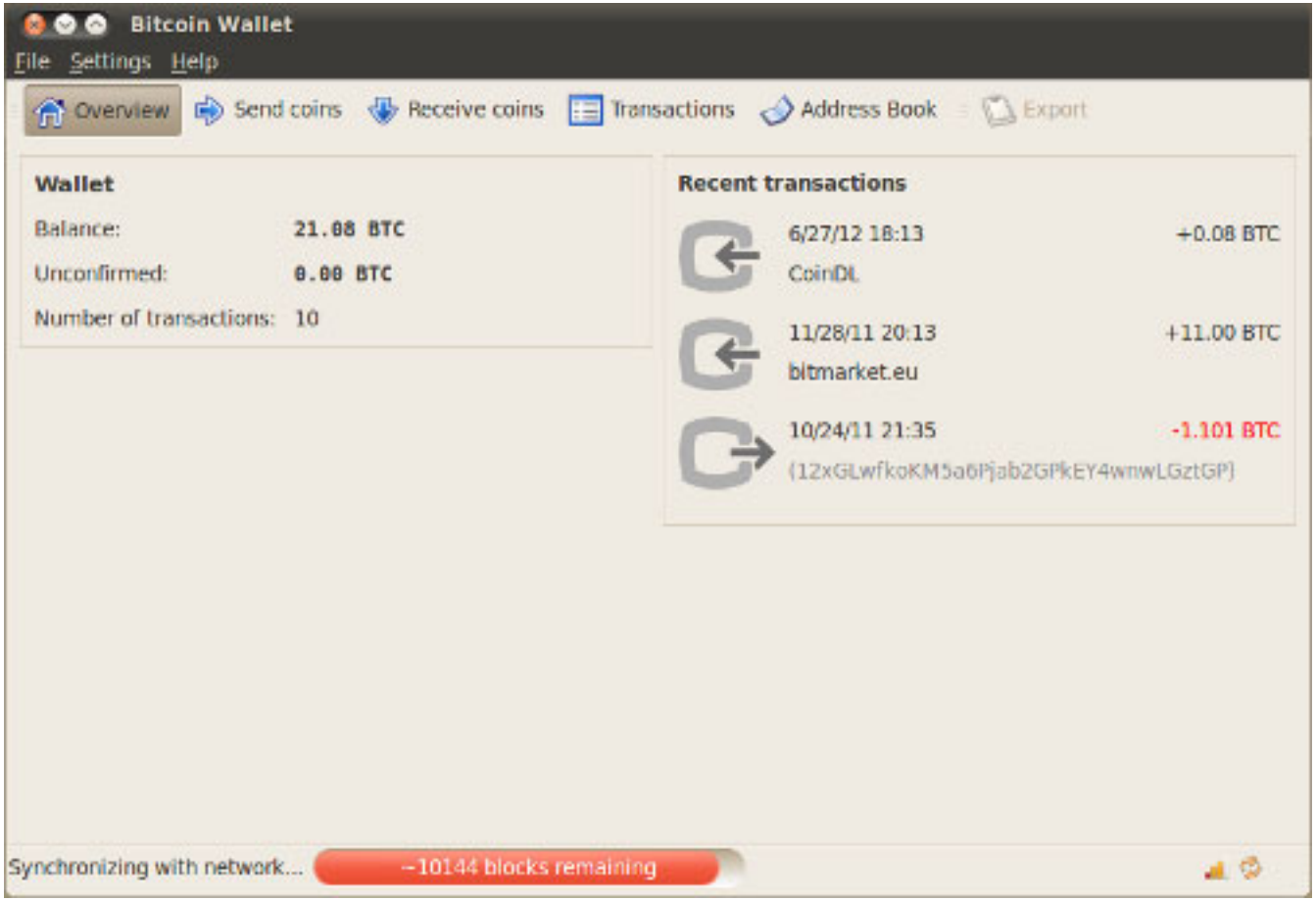
ACTIVITY 1

What is the Bitcoin Blockchain ?

a. A master ledger of all Bitcoin transactions and balances
b. The part of the Bitcoin protocol that implements security
c. A list of all blocked addresses
d. A Bitcoin payment gateway

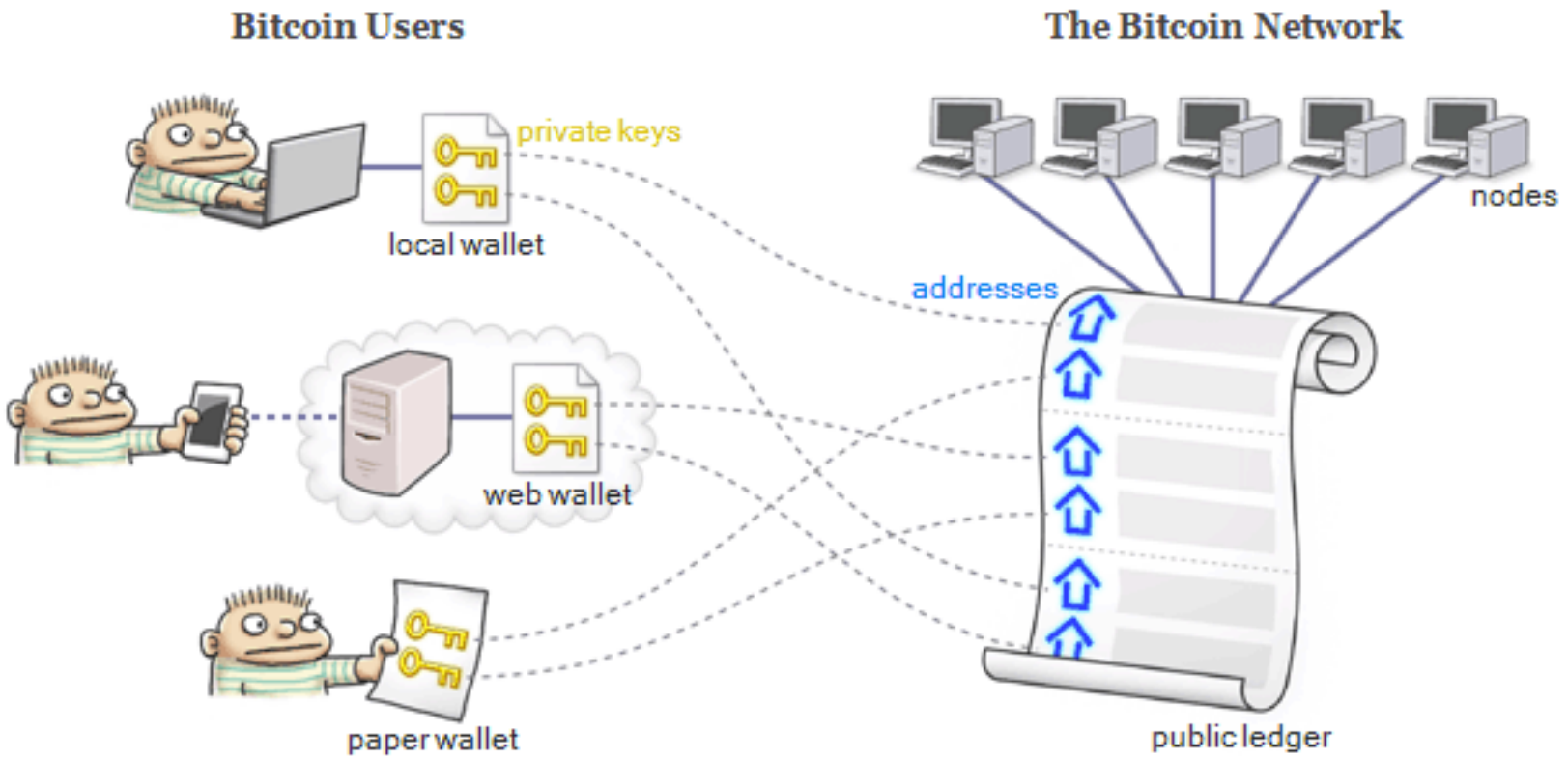
Clients and Wallets

- The bitcoin core client looks like this:



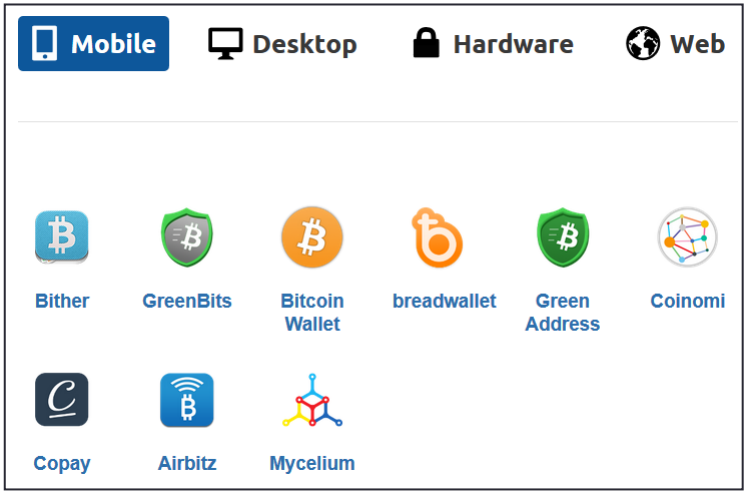
Other Bitcoin wallet: https://sparrowwallet.com/

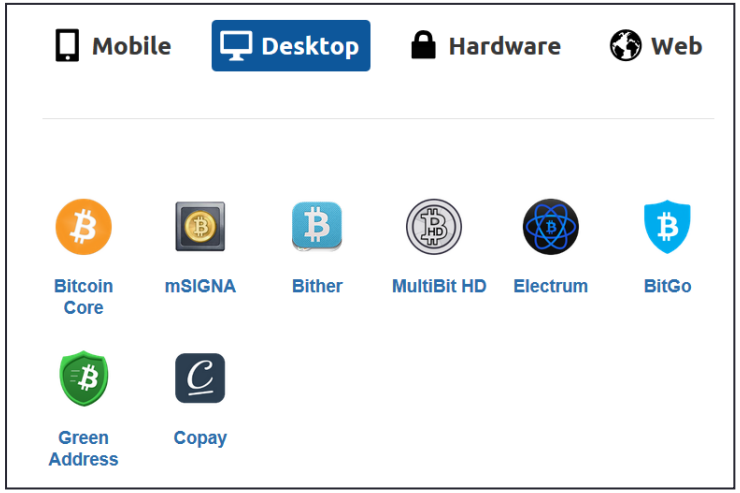
Bitcoin Clients and Wallets



Bitcoin Clients and Wallets (Aside)

- Clients and wallets are available for desktops and mobiles
- The original Bitcoin Core is the full client
  - Downloads and maintains the entire blockchain (200Gb+)
- Many other clients are light clients
  - They scan the online blockchain but don't download it
  - These are fine for personal use but not for mining





ACTIVITY 2

What does a Bitcoin wallet contain ?

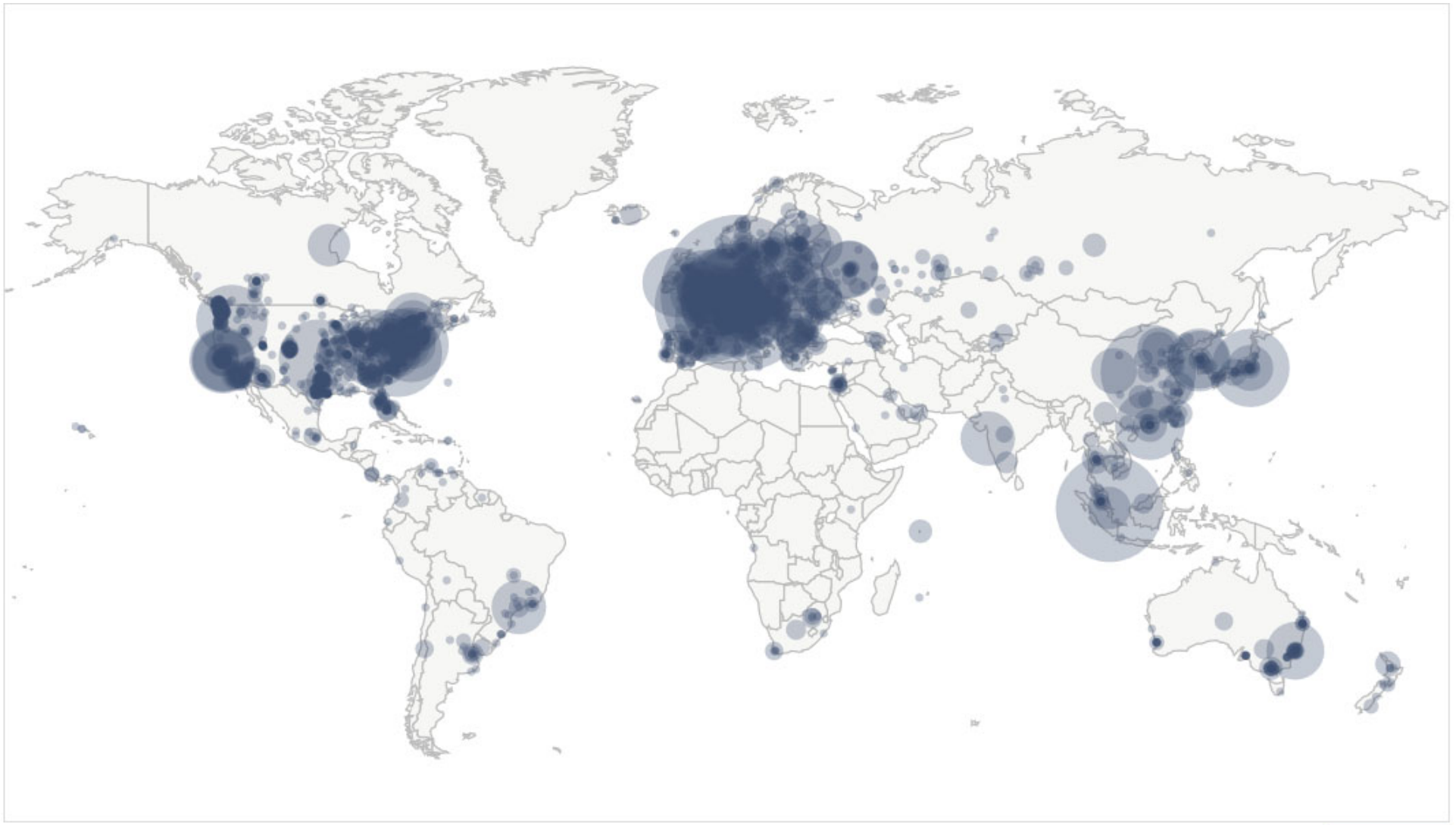
a. Only private and public addresses/keys
b. An address and bitcoin balance
c. All your Bitcoin transactions
d. Bitcoins and US dollars

The Bitcoin Network

- Bitcoin is a Peer-to-Peer network.
- Nodes communicate with up to 8 nodes on the network
- Nodes pass each other copies of the blockchain, transactions and mining information
- Changes propagate within seconds throughout the network.

- The blockchain is the master ledger of all bitcoin transactions and balances.
- Can inspect the blockchain online:
- https://blockchain.info

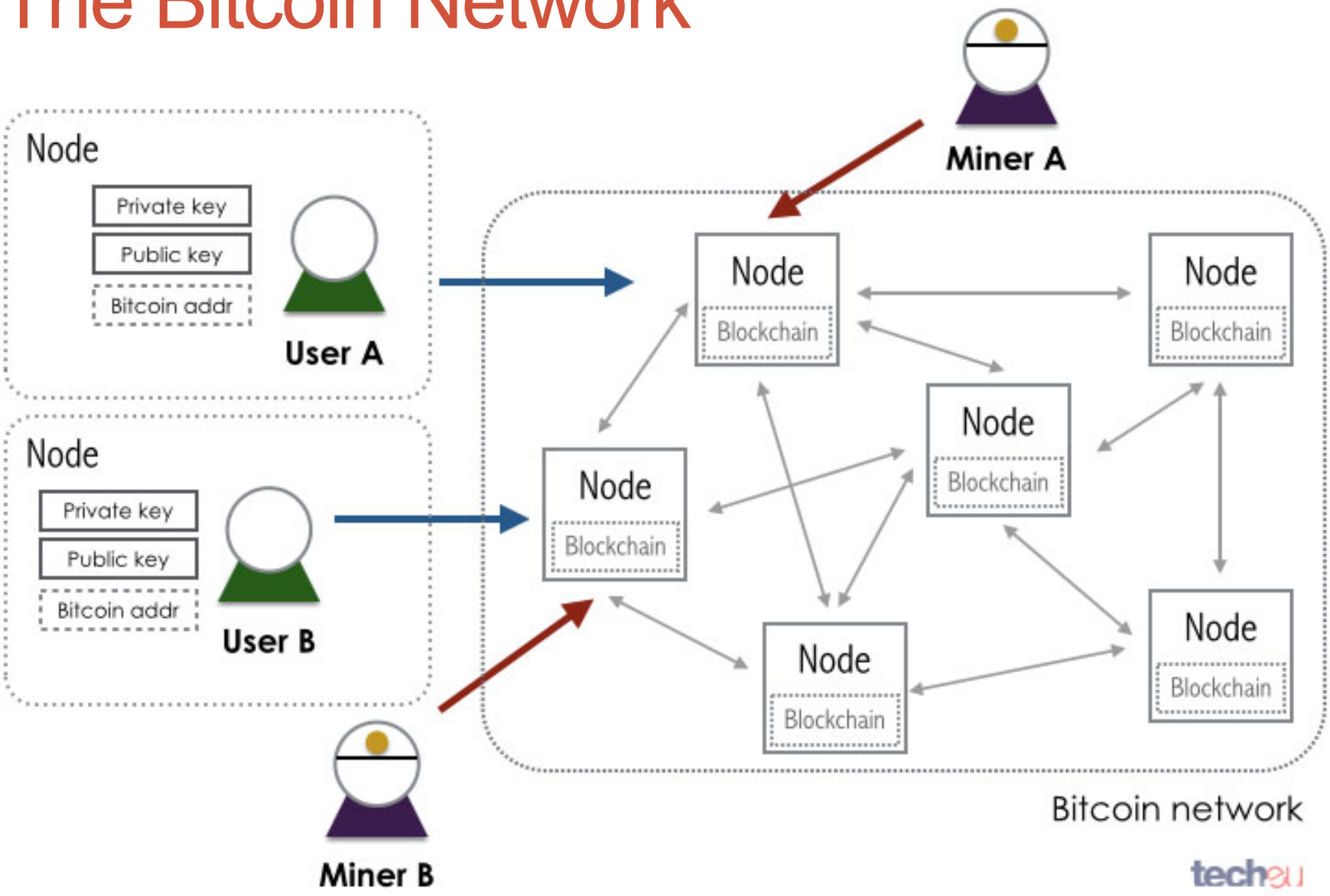
The Bitcoin Network



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

The Bitcoin Network



Bitcoin Mining

The Bitcoin mining map: https://ccaf.io/cbeci/mining_map

Bitcoin mining in China: https://www.youtube.com/watch?v=K8kua5B5K3I

Disruptive Potential of the BlockChain - Finance

- Finance
  - Banks may use a blockchain for interbank transactions
    - Currently being investigated by SWIFT
    - Commonwealth bank issued bonds on a blockchain in 2018
  - Transfer money anywhere in the world – low fees
  - Cryptocurrencies touted as replacements for money
    - Public cryptocurrencies possibly might take this role but,
  - CBDC – Central Bank Digital Currency
    - Governments create their own cryptocurrency to replace cash
    - China is currently implementing this
  - Vietnam: bond issuance and management

DeFi – Decentralized Finance

- Interest in DeFi (Decentralized Finance) boomed in 2020 and beyond
- Smart contracts and tokens on blockchains (mainly Ethereum) are being used to:
  - Swap between cryptocurrencies
  - Stake cryptos and earn interest
  - Borrow and lend cryptocurrencies
- Billions of dollars worth of cryptos involved
- Currently only involves cryptocurrencies – no crossover into real finance (as yet?)
- Some elements of DeFi are boomy/scammy

Potential Blockchain Benefits in Finance (Aside)

- Lower costs
  - Financial systems spend a large amount of money and generate large profits – potential for lowering costs
- Faster transactions
  - Time to transfer money between banks or around the world could be cut from days to minutes
- Faster settlements
  - Settling stock trades takes 3 days – could be instant.
- Banking the unbanked
  - 40% of the world population don't have a bank account

Blockchain Barriers in Finance

- Scalability
  - Ethereum currently processes 15 transactions per second (TPS) but VISA alone handles 1700 TPS
- Legal
  - Financial systems are highly regulated and controlled by governments.
- Identity
  - Cryptocurrency allow anonymous transactions. Anti-money laundering laws want people to be identified.
- Incumbents
  - The existing financial system participants will not go quietly into the night.

Art on the Blockchain - NFTs

- Ownership of digital Artistic objects (art, music) is being recorded on blockchains using NFTs (Non Fungible Tokens)
- In March 2021 the NFT for a digital artwork was sold for $69 million USD.
  - The buyer runs a fund that collects NFTs and paid with Ether
- Jack Dorsey (Twitter founder) sold the ownership of the first ever tweet for $2.9 million USD.
- The tweet is still visible to everyone – only a token for ownership of it was sold.

Blockchains in Supply Chains

- Supply chains have been one of the industries most actively investigating and trialling blockchains
- Supply chains are naturally suited to the application of blockchains to solve existing problems:
  - Multiple parties involved
  - Current supply chains often involve paper based documents
  - There is a need to share data along the chain
  - Currently hard to trace products back through the chain
  - Supply chains cross multiple countries and legal systems
  - No single trusted authority

Application of Blockchains in Healthcare

Data Management Applications

- **Global Scientific Data Sharing for R&D**
- **Data Management**
- **Data Storage (Cloud-based applications)**
- **Electronic Health Record**

Example of single point of failure in central database

Supply Chain Management

- **Clinical Trials**
- **Pharmaceutical**

Internet of Medical Things

- **Healthcare IoT and Medical Devices**
- **Healthcare IoT Infrastructure and Data Security**
- **Artificial Intelligence**

- Khezr Et Al. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. Appl. Sci. 2019, 9, 1736.

ACTIVITY 3

What are the problems with relying in big intermediaries to establish trust ? Select all answers that apply.

a. They can be hacked

b. They exclude billions of people from the economy

c. They slow things down

d. They take large fees

e. They capture personal data and undermine privacy

ACTIVITY 4

How could Blockchain be used by governments ? Select all answers that apply.

a. To run elections

b. To operate essential services such as police

c. For registration of births, deaths and marriages

d. To register and track land titles

e. To run their public websites

Disruptive Potential of the BlockChain (Aside)

- Legal
  - Contracts could be recorded on a blockchain instead of pieces of paper
  - Enforcement of contracts could be performed by the contract code itself
  - Copyright – ownership rights publicly recorded on a blockchain – currently a mess
- Qualifications
  - Educational qualifications, courses completed etc. are being recorded on public blockchain
  - RMIT is doing this now

Disruptive Potential of the BlockChain (Aside)

- Government
  - Elections – investigations of voting using a blockchain
  - Registrations
    - Births, deaths, marriages ?
    - Property transactions
      - Swedish government transferring property registration to a blockchain
    - Ownership transfers (vehicles)