Blockchain

Cruise Ship
Enrichment Talk

Presented by Sonja Bernhardt OAM

Agenda – Blockchain

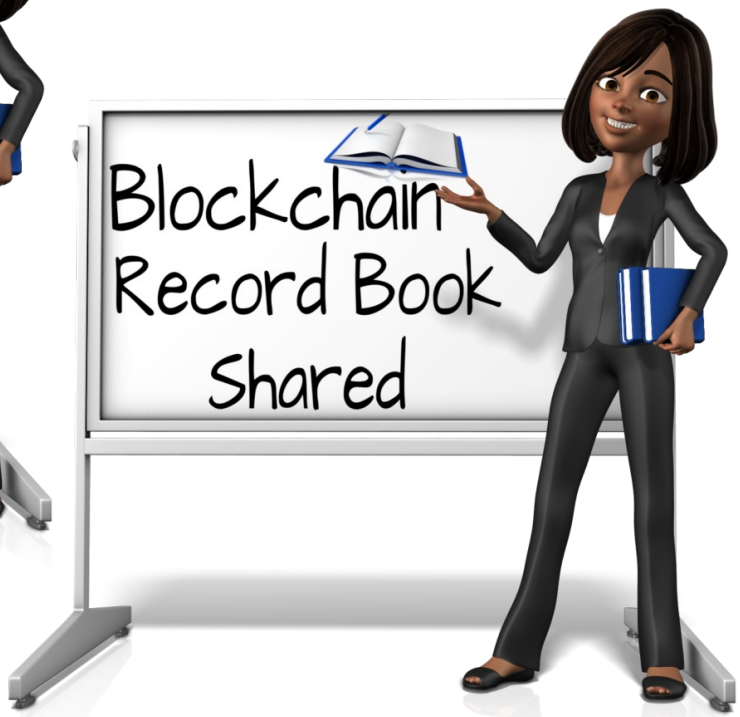
1. Use Cases (Blockchain Why)
2. Blockchain 101 (What and How)
3. The Issues
4. The Future

Cruise Ship
Enrichment Talk

Bitcoin: A Peer-to-Peer Electronic Cash System

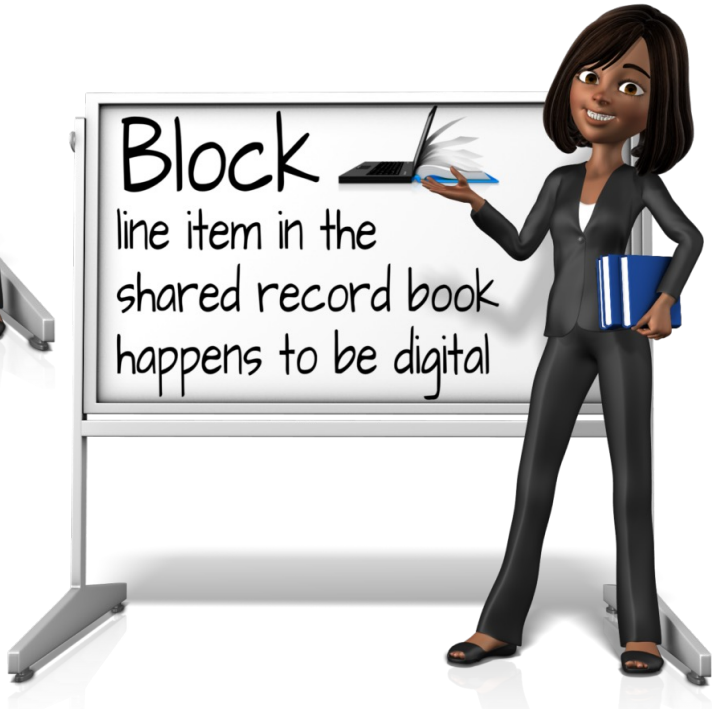
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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 proof-of-work chain as proof of what happened while they were gone.

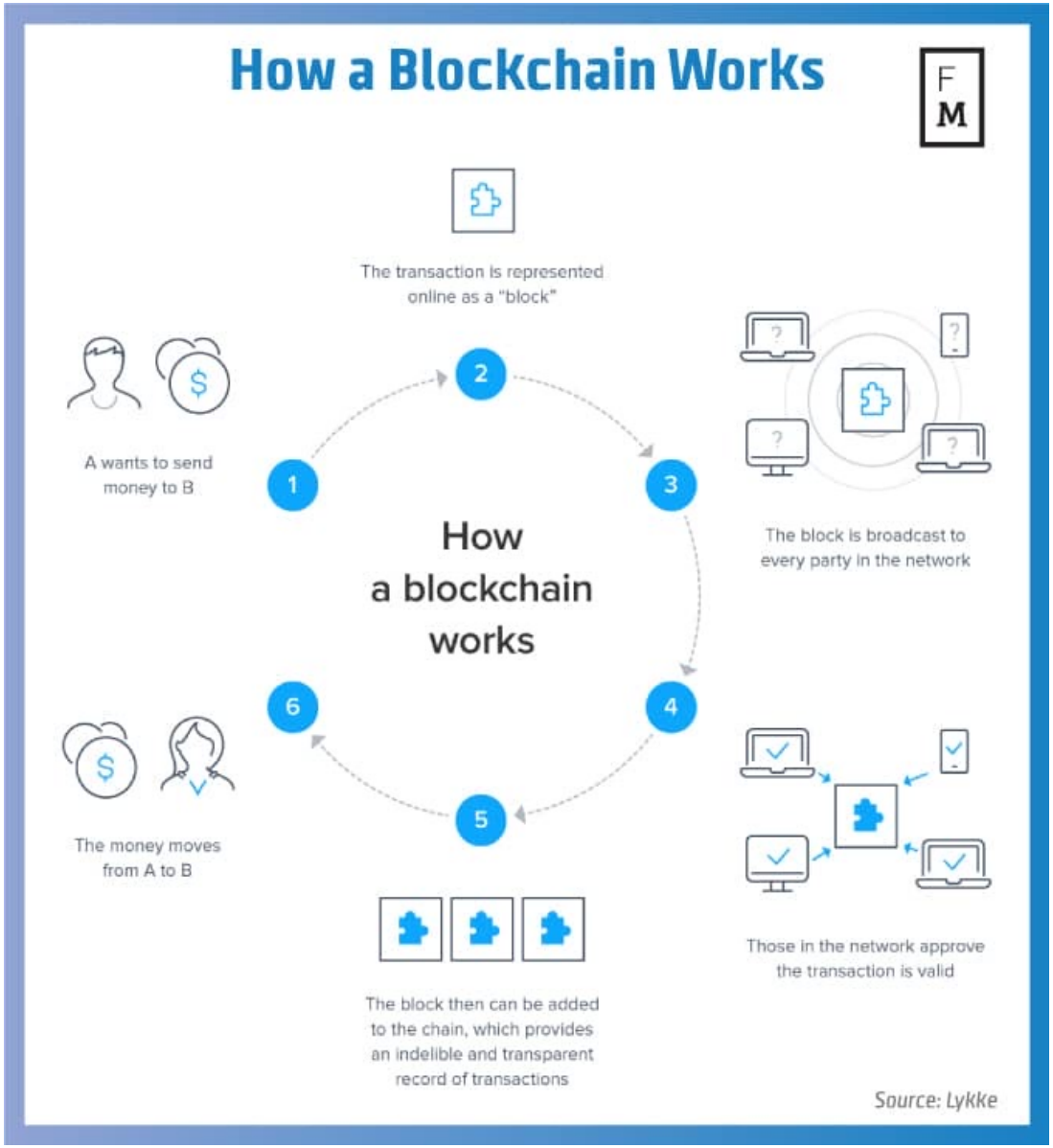


LEDGER

DIGITAL RECORD
Decentralised &
Distributed



Data is stored in BLOCKs and linked together via a CHAIN

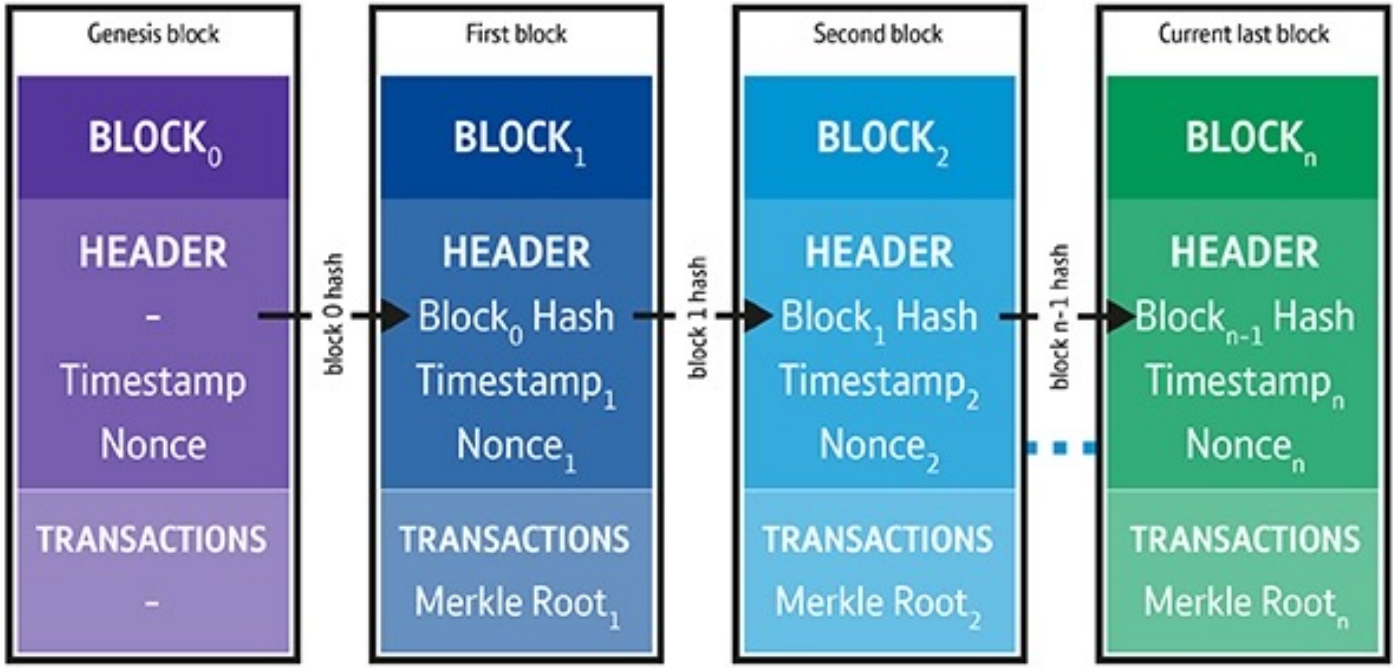


Puzzles and Problem Solving – maths, detective PoW Proof Of Work

Transaction verified, proven and also New Minted for miner(s)

Blockchain101: What and How

Hash – Algorithm:
(input string any length – output fixed length (max 256)
Nonce – random string
Merkle Root – the starting (node) of a tree

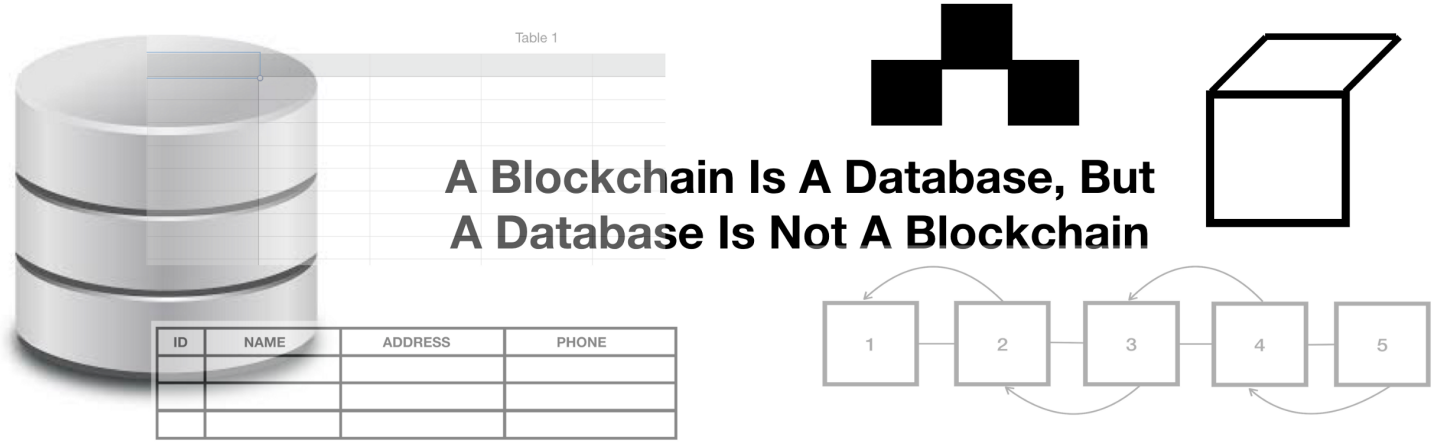


Immutable,
Transparent
and
Tamper Free

Sort of….

The Issues

1. Separate Blockchain from Crypto
   - TECHNOLOGY - Blockchain
2. Blockchain scalability and size not at database level – YET!



Database ideal for data that needs continuous updating updating e.g., monitoring and sensors

Blockchain ideal for verification of trusted data: identity, reputation, credibility, integrity

The Issues

3. Trust

A **trustless** system means that the participants involved **do not need** to know or trust each other or a third party for the system to function.

Move to a Trustless Community

Historically we have moved from trusting individuals to trusting centralised institutes as the intermediary.

Now need to shift away from ‘trusted’ gatekeepers to direct via technology.

The Future

- Eliminate the ‘middle man’ across industries
- Digital Identity: Unique
  - Banking, Healthcare, National Security, Citizenship documentation (birth certificates, passports, wedding certificates), online retail…

- Contracts: smart contracts
  - Mortgages, wills, legal contracts, timestamp notary
- Democracy: eVoting System (Estonia. Trials: Malta, Korea, Russia, India, West Virginia USA)
- Music: Pay artists directly for specific uses
- NFT’s (Non-Fungible Tokens)

The Future

fungible

[**fuhn**-*juh*-b*uh*l]

adjective

being of such nature or kind as to be freely exchangeable or replaceable, in whole or in part, for another of like nature or kind.

Fungible

My $10 is the exact same as your $10

Semi-fungible

All general admission tickets get each person in to the same specific concert, but may not work for a different concert or date.

Non-fungible

Represents something unique and 1-of-1!