BLOCKCHAIN TECHNOLOGY

Introduction

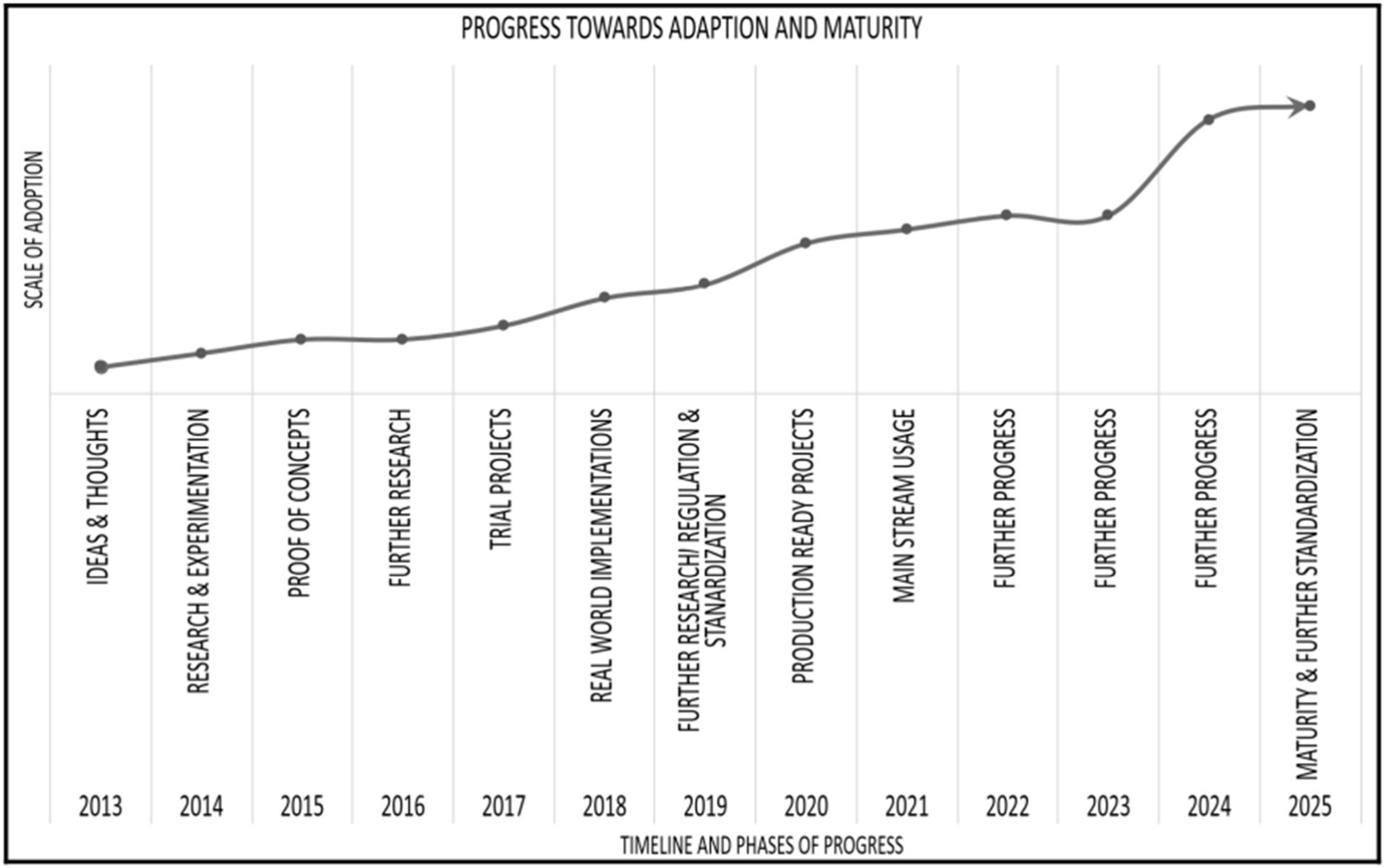
References

- Mastering Blockchain, Imran Bashir, 2nd Edition, Packt Publishing
- The vast ocean of Internet knowledge

The growth of blockchain technology

- With the invention of Bitcoin in 2008
  - the world was introduced to a new concept, which
    - is now likely to revolutionize the whole of society.
    - is something that promises to have an impact on every industry
- Some describe blockchain as a revolution
- Another school of thought believes that it is going to be more evolutionary
  - it will take many years before any practical benefits of blockchain reach fruition.
  - This thinking is correct to some extent,
    - **but, the revolution has already begun**.

The growth of blockchain technology



Distributed systems

- Understanding distributed systems is essential
  - Blockchain
    - is a distributed ledger which can be centralized or decentralized.
    - usually used as a decentralized platform.
    - has properties of both decentralized and distributed paradigms.
    - is a decentralized-distributed system

Distributed systems

- Distributed systems are a computing paradigm
  - two or more nodes work with each other
    - in a coordinated fashion to achieve a common outcome.
  - users see it as a single logical platform

Distributed systems

- A node in a distributed system
  - can be defined as an individual player
  - can send and receiving messages to and from any other node.
  - can be honest, faulty, or malicious
  - has memory and a processor.
- A node that exhibits irrational behavior is also known as a Byzantine node

Distributed systems

- The Byzantine Generals problem
  - a group of army generals who lead different parts of the Byzantine army are planning to attack or retreat from a city.
  - The only way of communicating among them is via a messenger.
  - They need to agree to strike at the same time in order to win.
  - The issue is that one or more generals might be traitors who could send a misleading message.
  - Therefore, there is a need for a viable mechanism that allows for agreement among the generals,
    - even in the presence of the treacherous ones
- As an analogy to distributed systems
  - the generals can be considered nodes
  - the traitors as Byzantine (malicious) nodes
  - and the messenger can be thought of as a channel of communication among the generals.

Distributed systems

- The primary challenges in distributed system
  - coordination between nodes
  - fault tolerance.
- They should tolerate
  - faulty nodes
  - network links break

The history of blockchain and Bitcoin

- Electronic cash
  - The concept is not new
    - Since the 1980s, e-cash protocols have existed
  - Two fundamental issues need to be addressed
    - Accountability
      - ensure that cash
        - is spendable only once (double-spend problem)
        - can only be spent by its rightful owner
    - Anonymity
      - protect users' privacy (As with physical cash)

The history of blockchain and Bitcoin

- Electronic cash
  - Bitcoin: the first practical implementation in 2009
    - solved the problem of distributed consensus in a trustless network
    - It used
      - public key cryptography
      - Proof of Work (PoW) mechanism
    - The key innovation was
      - the idea of an ordered list of blocks composed of transactions
      - cryptographically secured by the PoW mechanism

The history of blockchain and Bitcoin

- Blockchain
  - A groundbreaking paper in 2008
    - Entitled “Bitcoin: A Peer-to-Peer Electronic Cash System”
    - Under the pseudonym Satoshi Nakamoto
      - No one knows the actual identity
      - remained active in the Bitcoin developer community until 2011
      - He then handed over Bitcoin development to its core developers and simply disappeared.
    - It introduced the term chain of blocks.
      - Evolved over the years into the word **blockchain**

The history of blockchain and Bitcoin

- Blockchain
  - Technical definition:
    - A peer-to-peer, distributed ledger that is
      - cryptographically-secure
      - append-only
      - immutable (extremely hard to change)
      - updateable only via consensus or agreement among peers

The history of blockchain and Bitcoin

- Blockchain
  - Peer-to-peer
    - Means that
      - there is no central controller in the network
      - all participants talk to each other directly
    - Allows for
      - cash transactions to be exchanged
        - directly among the peers
        - without a third-party involvement (such as a bank)

The history of blockchain and Bitcoin

- Blockchain
  - Distributed ledger
    - a ledger is spread across the network among all peers in the network
    - each peer holds a copy of the complete ledger
  - Cryptographically-secure
    - cryptography has been used to provide security services
    - make the ledger secure against tampering and misuse

The history of blockchain and Bitcoin

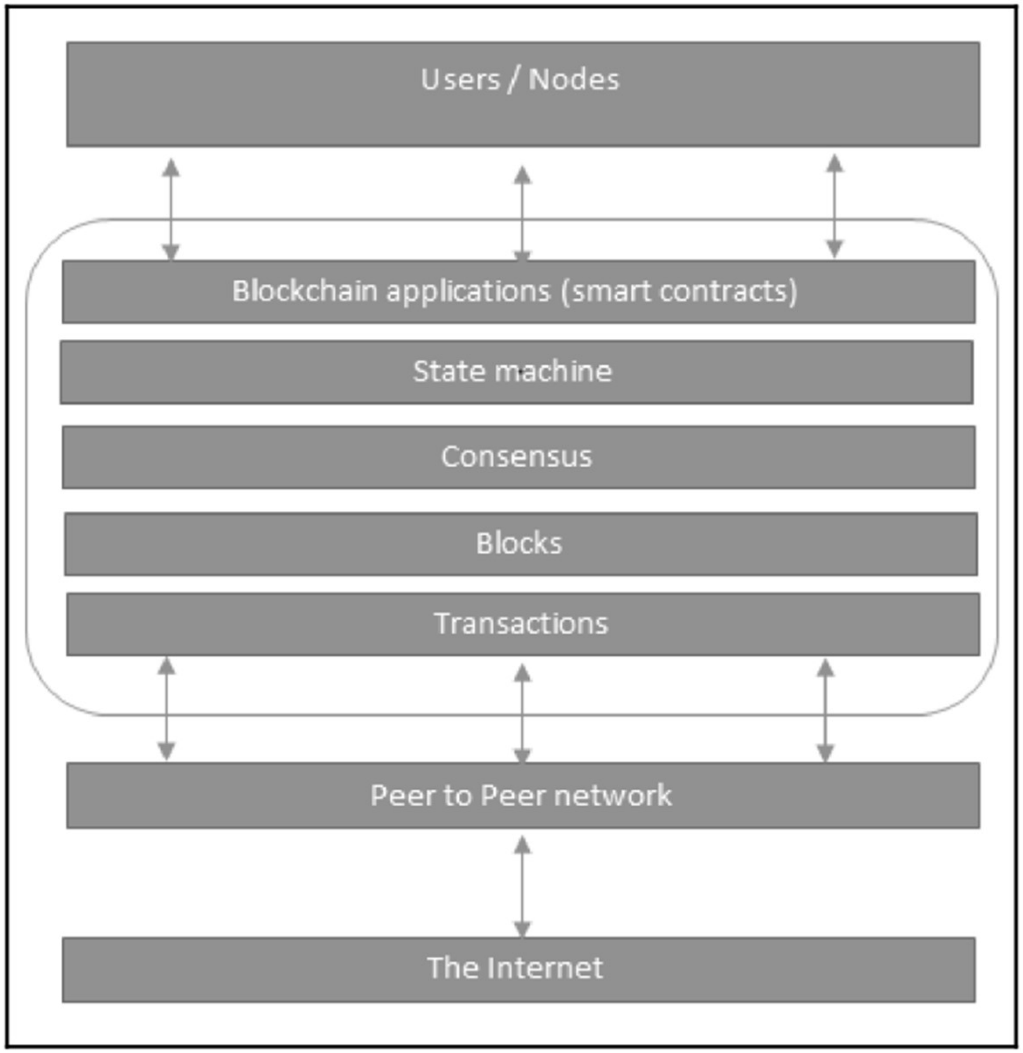
- Blockchain
  - Append-only
    - data can only be added to the blockchain in time-ordered sequential order
    - once data is added to the blockchain
      - it is almost impossible to change that data
      - can be considered practically immutable

The history of blockchain and Bitcoin

- Blockchain
  - Updateable only via consensus
    - most critical attribute
    - gives the power of decentralization
    - no central authority is in control of updating the ledger.
      - any update
        - is validated against strict criteria
          - defined by the blockchain protocol
        - added to the blockchain only after a consensus among all nodes

The history of blockchain and Bitcoin

- Blockchain



The history of blockchain and Bitcoin

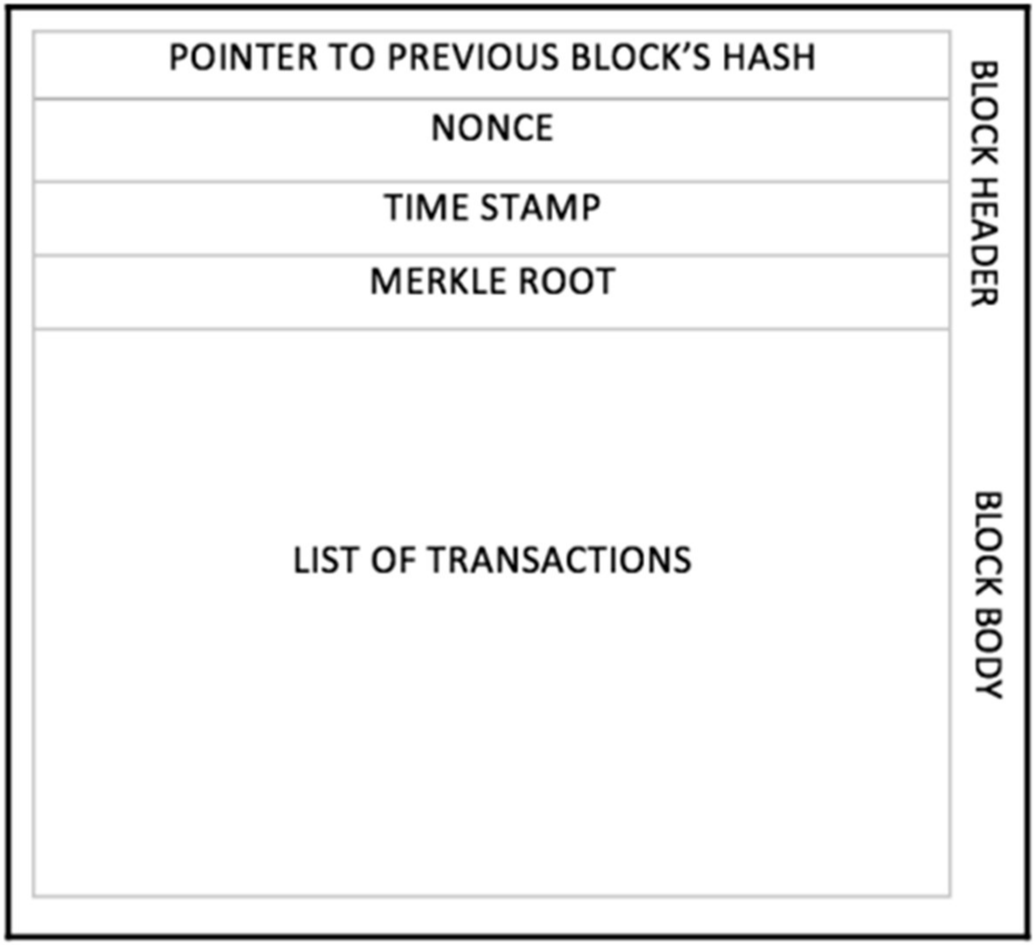
- Blockchain
  - A block
    - is merely a selection of transactions bundled together
      - A transaction is a record of an event
      - E.g., the event of transferring cash from a sender's account to a beneficiary's account
    - Has a reference to a previous block
      - unless it is a genesis block (the first block in the blockchain)
    - Has a nonce
      - a number that is generated and used only once
      - used
        - in PoW consensus algorithms
        - for transaction replay protection

The history of blockchain and Bitcoin

- Blockchain
  - A block
    - Has a Merkle root
      - a hash of all the nodes of a Merkle tree.
      - Merkle trees are widely used to validate the large data structures securely and efficiently.
      - Merkle tree in the blockchain world
        - is used to allow efficient verification of transactions.
        - presents in the block header section of a block
          - which is the hash of all transactions in a block.
      - Its verification is only required to verify all transactions present in the Merkle tree

The history of blockchain and Bitcoin

- Blockchain
  - A block



The history of blockchain and Bitcoin

- Types of Blockchain
  - Permissionless
    - Participants of the network are not known
    - Anyone can participate in the network
  - Permissioned
    - Participants of the network are already known and trusted
    - do not need to use a distributed consensus mechanism
      - instead, an agreement protocol is used to maintain a shared version of the blockchain.
    - There is no need for a mining mechanism
      - All transaction verifiers are already preselected by a central authority

Blockchain Demo

Consensus protocols

- What is Consensus & Why do we need it?
  - is a method for coming to agreement over a shared state
    - Solving Byzantine general problem
  - Contain two parts:
    - Sybil resistance mechanism: defends against users creating a large amount fake nodes
      - PoW
      - PoS
    - Chain selection algorithm
      - E.g. Nakamoto longest chain rule

Consensus protocols

- Classical consensus protocols
  - has been used since the 1980
  - are based on all-to-all voting
  - They typically have
    - a designated leader who initiates the decision process
    - a series of rounds of all-to-all communication to ensure that all correct nodes reach the same decisions with absolute certainty.

Consensus protocols

- Classical consensus protocols
  - They typically require quadratic communication overhead with all-to-all communication of $O(n^2)$
    - with 100 nodes each round requires 10,000 messages.
    - In the event that the leader fails the communication overhead increases further to $O(n^3)$
    - they need accurate knowledge of membership of all participating nodes
    - If an attacker gains control of 1/3 +1 of the network, they can launch a double-spend attack which is guaranteed to succeed.

Consensus protocols

- Classical consensus protocols
  - HotStuff : The most scalable Classical protocol used by Facebooks
    - only supports approximately 100 validators before the performance begins to suffer.
  - They are not suitable for large, open and permissionless networks due to
    - limitations in the scalability of number of participants
    - being more fragile where accurate membership needs to be maintained

Consensus protocols

- Nakamoto consensus protocols
  - The first breakthrough in consensus protocols
  - have become popular with the rise of Bitcoin.
  - does away with the requirement for all-to-all communication
  - Is based on the longest chain rule
  - provide a probabilistic rather than deterministic safety guarantee.
    - Unlike classical consensus protocols
  - Probability of a double spend is arbitrarily small
    - enabling high value financial systems to be constructed on this foundation