BITS Pilani
Pilani Campus

Blockchain Technology
(BITS F452)

Dr. Ashutosh Bhatia, Dr. Kamlesh Tiwari
Department of Computer Science and Information Systems

BITS Pilani
Pilani Campus

Decentalized Cryptocurrency

ScroogeCoin

Crucial Question

Can we de-scoogify the currency and operate without a trusted third party

We need to figure out:

How every one agree upon a single public block chain

How every one agree upon which transactions are valid

How to assign IDs to coins in a decentralized manner.

Decentralization is not all-or-nothing

Email: Decentralized protocol but dominated by centralized webmail services

Aspects of Decentralization in BITCOIN

- Who maintains the ledger?
- Who has authority over which transactions are valid?
- Who creates new Bitcoins?
- Who determines how the rules of the system change?
- How do Bitcoins acquire exchange value?

Beyond the protocol: Exchange, wallet, software and service providers

Aspects of Decentralization in BITCOIN

- **Peer to Peer Network**
  - Open to anyone, low barrier to entry
  - Currently there are several thousands of bitcoin nodes
- **Mining**
  - open to anyone but inevitable concentration of power often seem as undesirable.
- **Updates to Software**
  - Core developers trusted by the community, have great power

BITCOIN’s Key Challenge

Key technical challenge of decentralized ecash : **Distributed Consensus**

or: How to decentralize ScroogeCoin

Why Consensus Protocol ?

Traditional Motivation

Reliability in Distributed Systems

Distributed Key-Value Store enables various applications

DNS, Public-Key Dictionary, Stock Trades

Defining Distributed Consensus

There is a fix number of nodes or processes and each of these has some input value

Protocol terminates and all correct nodes decide on the same value

This value must have been proposed by some correct node

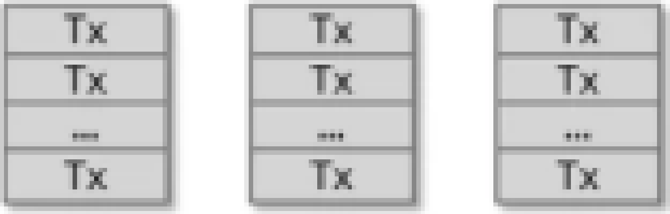
BITCOIN is a P2P system

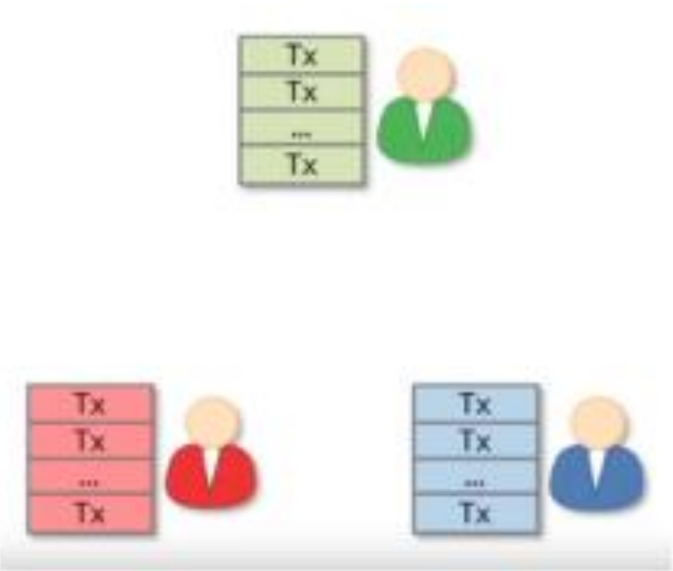
At any given time

- All nodes have sequence of blocks of transactions that they have consensus on

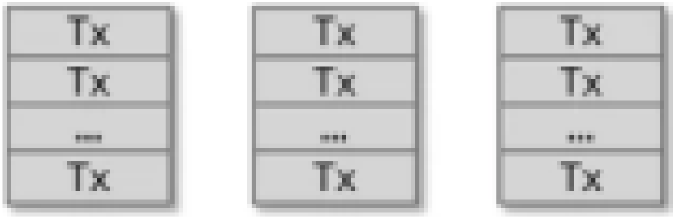
- Each node has a set of outstanding transactions that they have heard about

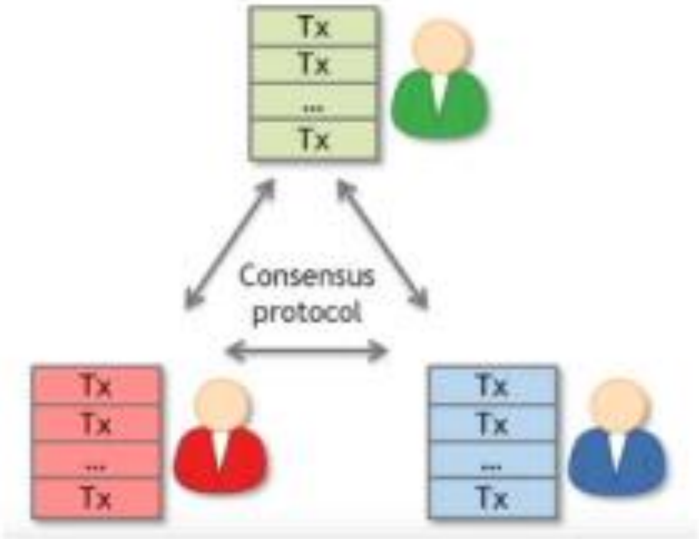
How Consensus could work in BITCOIN



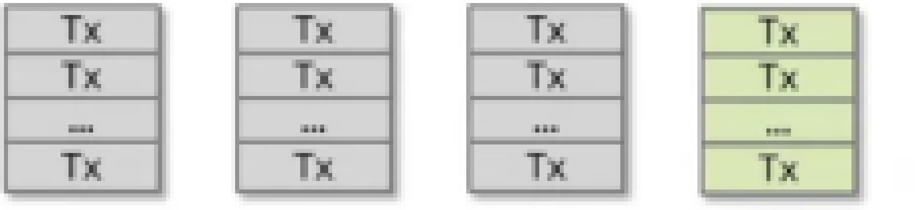


How Consensus could work in BITCOIN





How Consensus could work in BITCOIN



OK to select any valid block, even of proposed by only one node

Why Consensus is hard

Nodes may crash

Nodes may be malicious

Network is imperfect

- Not all pair of nodes connected
- Faults in network
- Latency

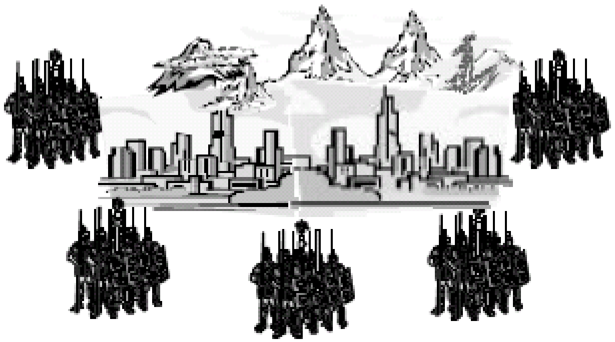
No notion of Global Time

Many impossibility results

- Byzentine generals problem

- Fischer-Lynch-Paterson (FLP) result says that you can't do agreement in an Asynchronous Message Passing system if even one crash failure is allowed, unless you augment the basic model in some way, e.g. by adding randomization or failure detectors.

Byzantine Generals Problem (Optional)



- Generals = Computer Components
- The abstract problem…
  - Each division of Byzantine army is directed by its own general.
  - There are n Generals, some of which are traitors.
  - All armies are camped outside enemy castle, observing enemy.
  - Communicate with each other by messengers.
  - Requirements:
    - G1: All loyal generals decide upon the same plan of action
    - G2: A small number of traitors cannot cause the loyal generals to adopt a bad plan
  - Note: We **do not** have to identify the traitors.

Some well known protocols

Example: Paxos

Nerver produces inconsistent result but can get stuck.

BITCOIN consensus theory and practice

BITCOIN consensus works better in practice than in theory

Theory is still catching up

BUT theory is important, can help predict unforeseen attacks.

Some things BITCOIN does differently

- Introduces incentives
    - Possible only because it’s a currency

- Embraces randomness
    - Does away with the notion of specific end point
    - Consensus happen over a long time scale

BITCOIN consensus algorithm

Keep in mind that BITCOIN does this without having any long term identities which is different from classical distributed system.

Why don't BITCOIN node have identities

Identity is hard in P2P system – **Sybil Attack**

Psedoanonymity is a goal of BITCOIN

Key Idea: Implicit Consensus

In each round a random node is picked

This node proposes a next block in the chain

Other nodes implicitly accept/reject this block

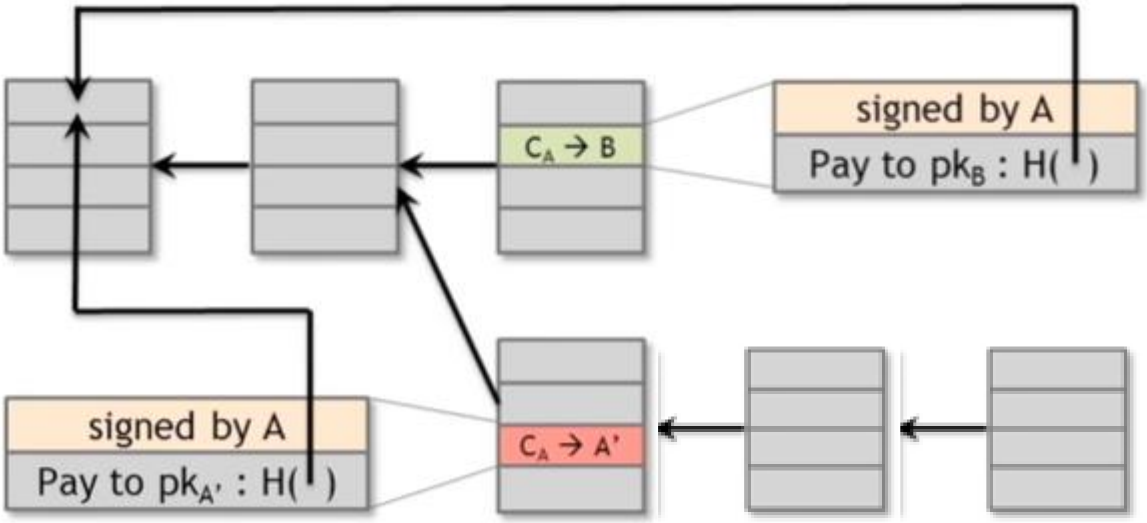
- By either extending it
- Or ignoring it and extending the chain from the earlier block

Every block contains the hash of the block it extends

Consensus algorithm simplified

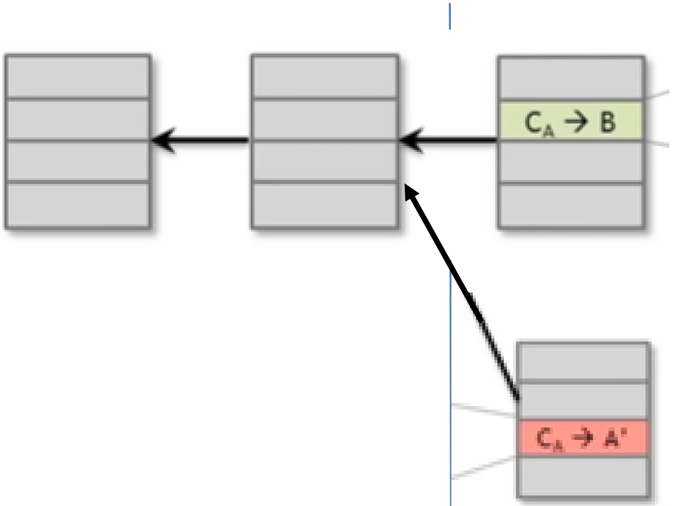
1. New transactions are broadcast to all nodes
2. Each node collects new transactions into a block
3. In each round a random node gets to broadcast its block
4. Other nodes accept the block only if all the transaction in the block are valid (unspent, valid signatures)
5. Nodes express their acceptance of the block by including its hash in the next block they create.

What can a malicious node do



Double-spending attack

From Bob the merchants point of View

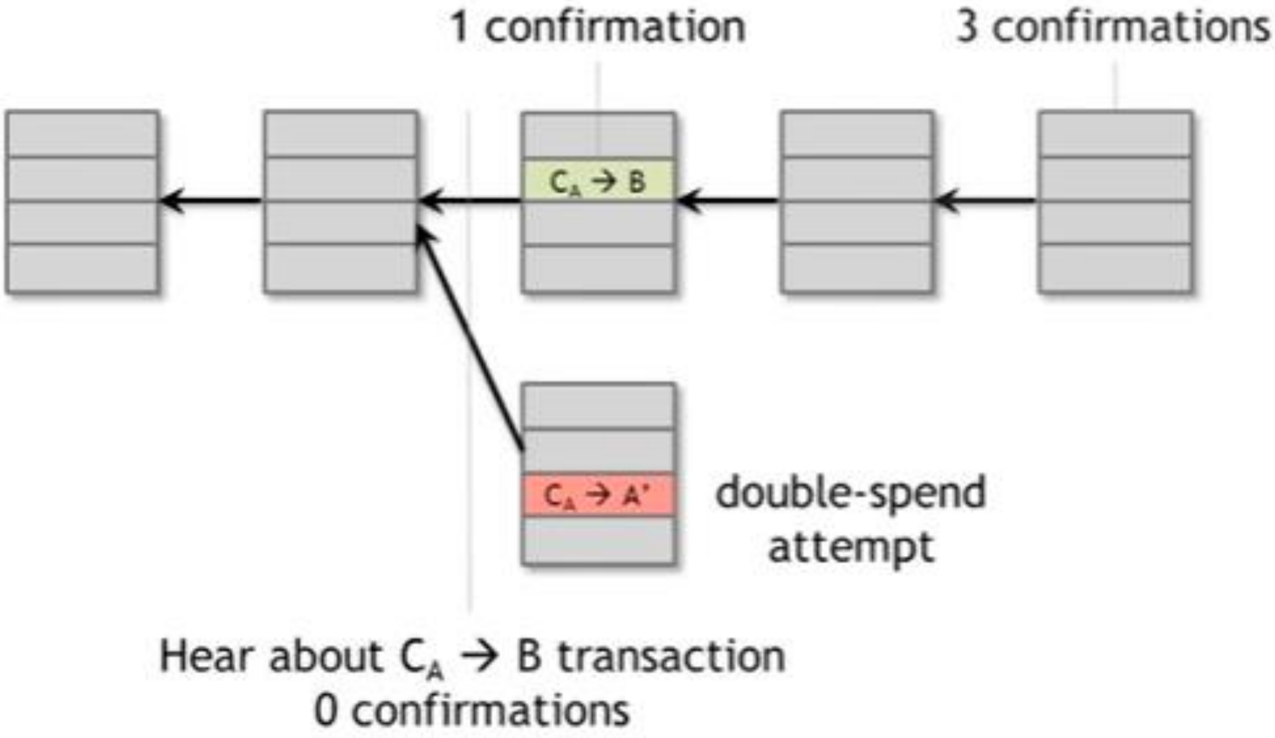


Hear About C_A -> B transaction in the blockchain first time (**1 confirmation**)

Double Spending Attempt

Hear About C_A -> B transaction over P2P network
(**0 confirmation**)

From Bob the merchants point of View



- **Double spending probability decreases exponentially with number of confirmation**
- **Most common heuristic is wait for 6 confirmations**

Recap

Protection against invalid transactions is cryptographic but enforced by consensus

Protection against double spending is purely by consensus

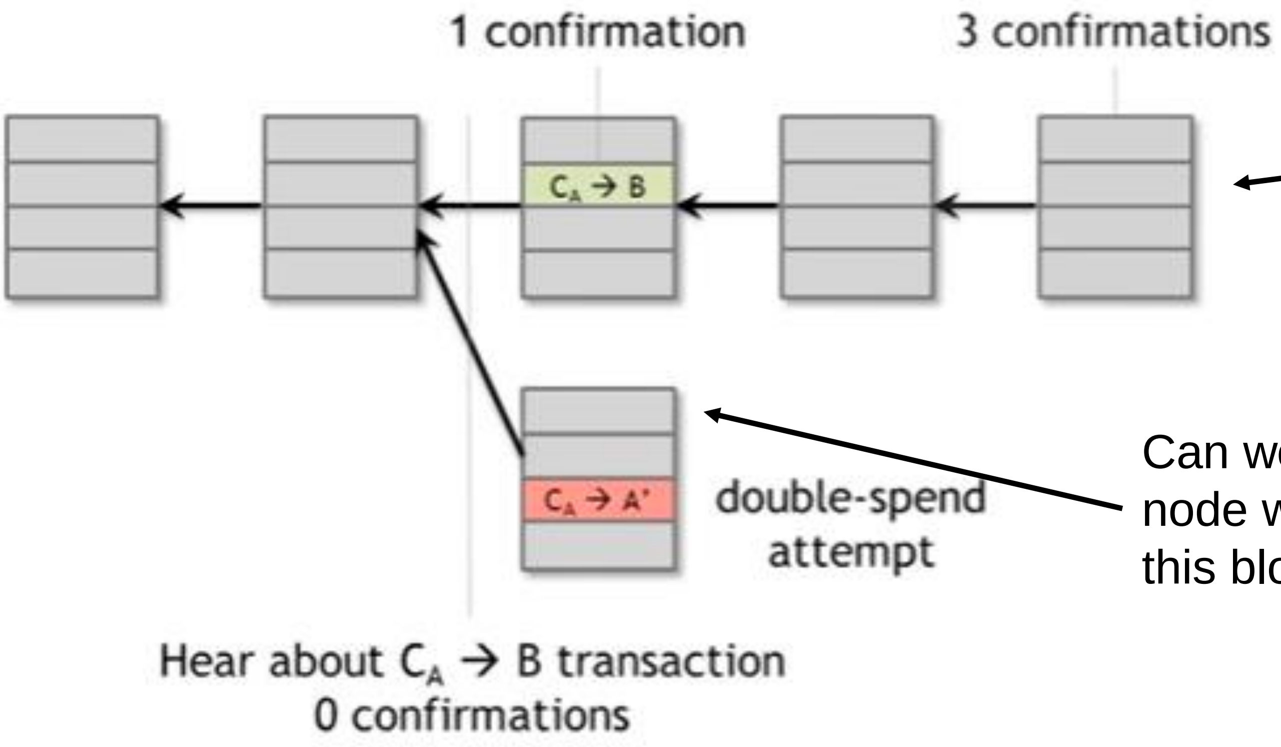
You are never 100% sure that a transaction is in consensus branch

Guarantee is probabilistic

Incentives and Proof of Work

Assumption of honesty is problematic

Can we give nodes incentives for behaving honestly.



Can we reward the nodes who created these blocks

Can we penalize the node who created this block

Incentive 1 : Block Reward

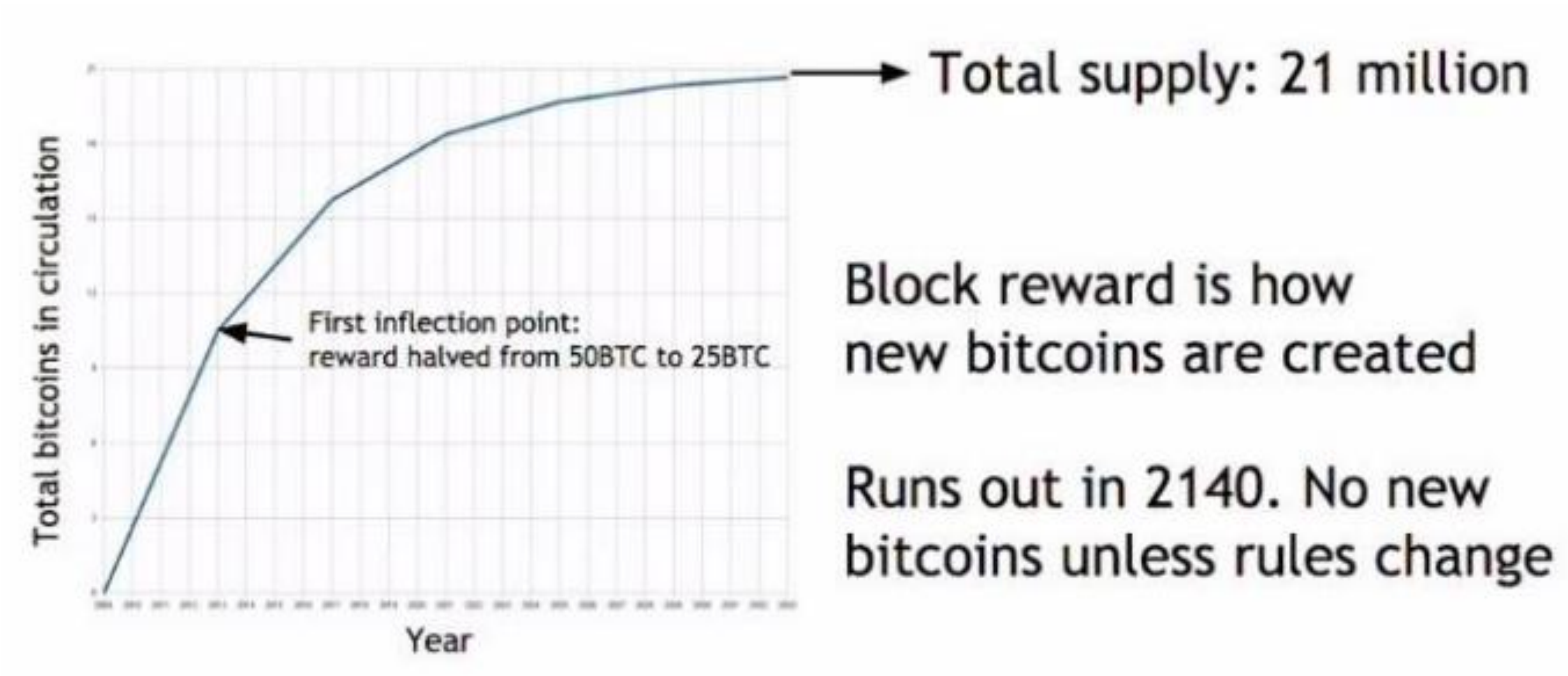
Creator of block get to

- Special coin-creation transaction in the block
- Choose receipt address of this transaction

Value is fixed currently : 6.25 BTC halves every 4 year

If the block end up on the long term consensus branch

Finite Supply of BITCOINs



Block reward is how new bitcoins are created

Runs out in 2140. No new bitcoins unless rules change

Incentive 2: Transaction Fee

Creator of a transaction can make its output value less than to its input value

Remainder is the transaction fee and it goes to the block creator

Purely voluntary like a tip

Remaining Problems

How to pick a random node?

How to avoid a free-for-all due to rewards?

How to prevent the Sybil attack?