Cryptocurrencies and Blockchain

Nisha Malik

Email: Nisha.Malik@uts.edu.au

41900 – Fundamentals of Security

Overview

- Limitations of centralized currency
- Overview of Bitcoin
- Wallets and Transactions
- The Blockchain
- The Peer-to-Peer Network
- Attacks on Bitcoin
- Beyond Bitcoin
- Ethereum
- Smart Contracts

Limitations of Centralised Digital Currency

Example: Alice has $100 in her PayPal account, and wants to buy some item off Bob for $25.

1. Bob asks for payment from Alice.
2. Alice speaks to the PayPal server and asks to transfer $25 to Bob.
3. Alice tells Bob that the transaction has been processed.
4. Bob checks with the PayPal server and confirms he is now $25 richer.

Limitations of Centralised Digital Currency contd..

Continuing example: Alice has $100 in her PayPal account, and wants to buy some item off Bob for $25.

Advantages:

- Transactions require minimal work from clients.
- Transactions can be reversed, in the case of fraudulent transactions.
- Transactions are secure, and double spending or cheating cannot occur.

Disadvantages:

- The PayPal servers are a single point of failure.
- PayPal can shift or move money at their discretion.
- Alice and Bob can’t perform a transaction without the PayPal server.

Bitcoin

- The first successful “Crypto Currency” payment system, and the first widespread implementation of a Blockchain technology.
- Bitcoin uses public key encryption to secure transactions.
- The public key is like a bank account number.
- The private key is like a PIN / password.
- A blockchain takes the place of a central server.
- Transactions are announced to the peer-to-peer network.
- All transactions are visible to nodes in the network.
- Bitcoin miners are rewarded to operating the blockchain.
- The creator of the next block is awarded some newly minted Bitcoins.
- The creator of the next block is awarded the transaction fees for transactions processed during the last time period.

What is in a Bitcoin wallet?

- Create a public/private keypair.
- Public: The public key is similar to a bank account number: giving someone this number allows them to transfer Bitcoin to you. This is also called an address.
- Private: The private key allows you to transfer money away from the corresponding address.
- Whilst it is possible to use a single address forever, it's very common to use many addresses, even a unique address per transaction.

Bitcoin Transactions

Bitcoin transactions are like cheques.

- Sender
- Recipient
- Amount
- Signature

We don’t accept cheques because they can’t be trusted.

One must submit it to the bank (***a central authority***) and wait for it to clear before accepting you have the money.

In Bitcoin, the sender submits a ***transaction to the network (a distributed authority).***

If valid, the network will agree that the receiver is the new owner.

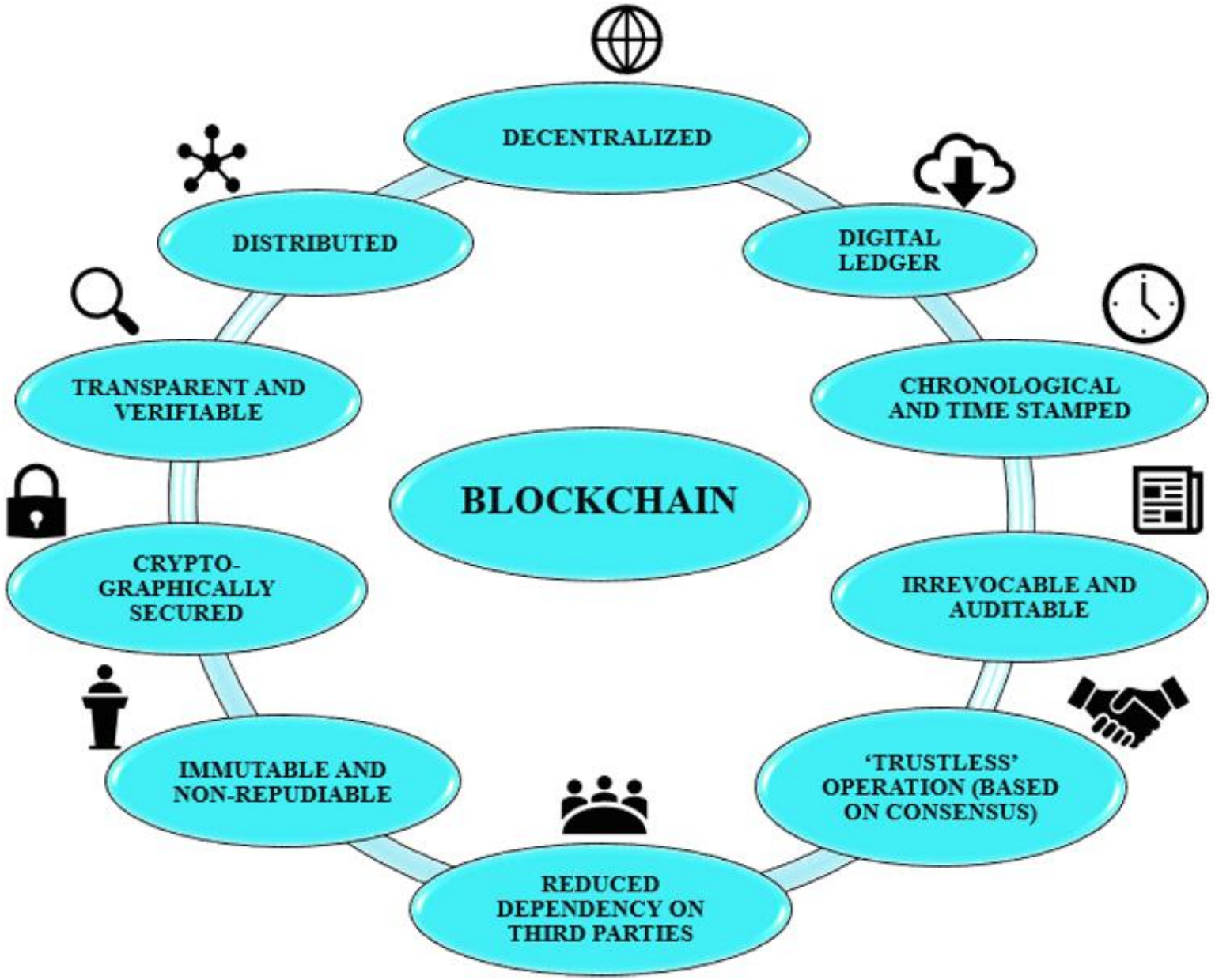
The Blockchain

The payee of a transaction must be able to “prove” that the previous owners of the bitcoin did not double spend it at any point.

In bitcoin, this is achieved by making everyone in the network aware of all *previous transactions*.

In order to accomplish this without a trusted third party,

- *Transactions must be publicly announced.*
- *All participants must agree on a single history for the order of transactions.*


BLOCKCHAIN
DECENTRALIZED
DISTRIBUTED
DIGITAL LEDGER
TRANSPARENT AND VERIFIABLE
CHRONOLOGICAL AND TIME STAMPED
CRYPTO-GRAPHICALLY SECURED
IRREVOCABLE AND AUDITABLE
IMMUTABLE AND NON-REPUDIABLE
'TRUSTLESS' OPERATION (BASED ON CONSENSUS)
REDUCED DEPENDENCY ON THIRD PARTIES

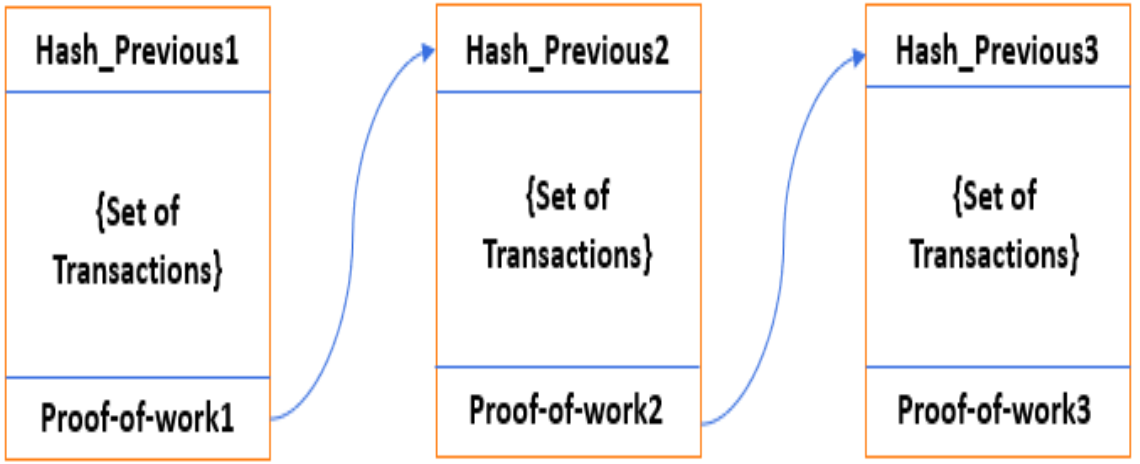
What exactly is a blockchain?

The concept of a blockchain incorporates a series of interdependent blocks, which store a consistent history of information.

Each block contains:

- Tx.: A set of transactions.
- block hash: block identifiers, linking them together.
- time the block was “completed”.
- Proof of Work – what miners do.

- Data is appended only – with a new block.



Hash_Previous2 = Proof-of-work1

Hash_previous3 = Proof-of-work2

Proof-of-work = H ({value_found, set of transactions, Hash_previous})

H()= Cryptographic Hash function say SHA-256

- ***The blockchain must definitively record all transactions***

It must show the order in which these transactions occurred, hence it must implement some form of timestamping that is agreed upon by all observers.

- ***The blockchain must be difficult to modify***

Specifically, it should be difficult to modify an existing blockchain such that past transactions may be modified, added, or removed.

The blockchain achieves both these goals by segregating work into chunks, called ***blocks***, which are processed on average once every 10 minutes. This time limit, and the difficulty of modifying previous blocks, is accomplished via a ***proof-of-work*** function.

Blockhain: Timestamp Server

- The blockchain can be thought of as implementing a *timestamp server*, which takes a group of items from timestep *n*, and combines them into a block B_u.
- The hash of current block, H_n, is a function of both the block's contents and the previous hash H_{n-1}.

$$H_n = \text{Hash}(H_{n-1} \| B_n)$$

- Thus, to modify a previous item, all hashes following the modification must be recalculated.

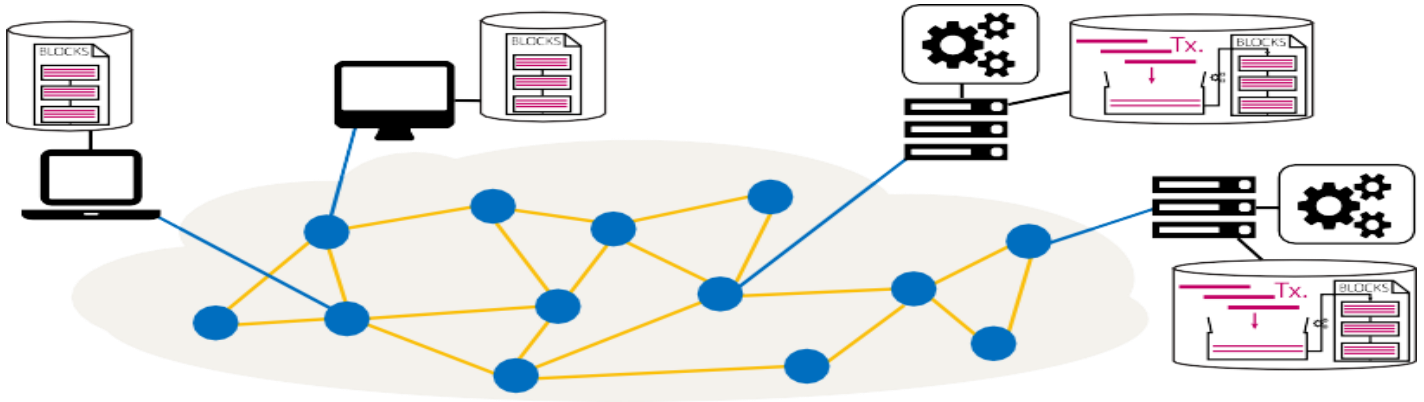
Blockchain: Proof-of-Work

Pure hashing is fast (in fact, most hash algorithms are designed to be fast).

The proof-of-work involves making the hashing more time consuming, by including a nonce in the block Bn.

The nonce has to be changed until the hash Hash($H_{n-1} \| Bn$) starts with a set number of zero bits.

The Peer-to-Peer Network



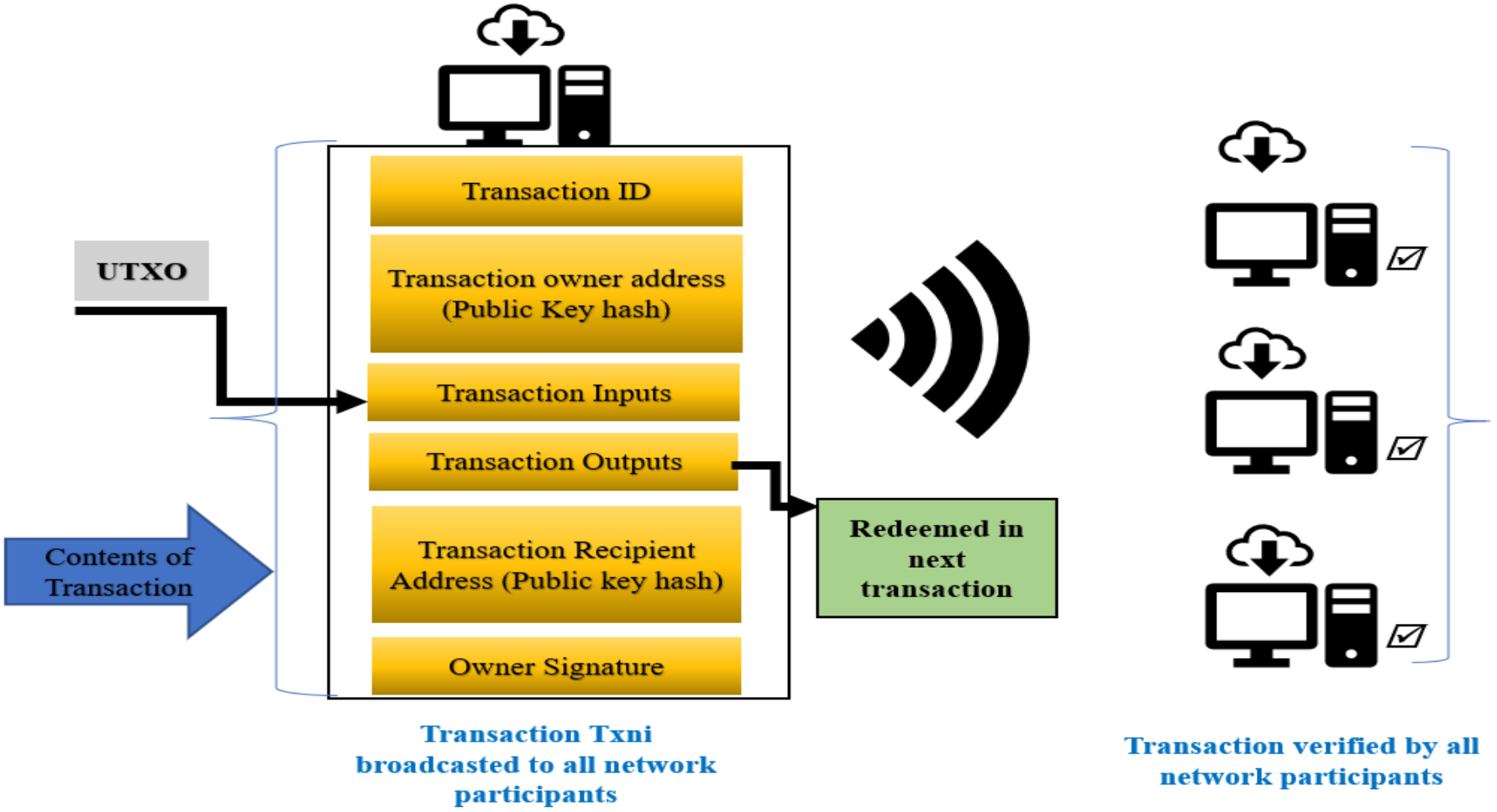
Each element $a \in Z_n^{\times}$ All Bitcoin clients are sharing the latest block information via a P2P network.

Some of those clients also mine blocks.

These miners are resposible for including transactions (Tx.)

New Tx. are announced on the network by clients and included in new blocks.

Transaction Broadcast



Transaction Confirmation

Ties are resolved when one of the competing heads solves the next block.

The longest chain at any time is the most authoritative.

To fork the blockchain, you need to command more than 50% of the computing power in the network.

If you're really unlucky, your transaction will end up in a dead branch, which opens you up to double spending attacks.

Transaction Confirmation

Wait a certain number of blocks before being 'sure' that your transaction will be permanent and irrefutable.

Six confirmed blocks (≈ one hour) is generally considered very safe for

Bitcoin.

Incentives for Mining

If you solve the proof-of-work and mine the next block, you receive two significant rewards:

The mining reward is essentially “free money in a block” rewarded to the successful miner.

- The only way to create new bitcoin.
- Started at 50 BTC per block, halves approximately every two years.
- Eventually will hit zero.

Transaction fees incentivise miners to include your transaction.

- A successful miner takes the transaction fees associated to each transaction in the block.
- These fees will drive mining in the long run, once the “mining reward” runs dry.

Attacks on Bitcoin

- Improper verification. Verification wasn't properly done on transactions before they entered the block chain and less than a week after discovery a fraudulent transaction resulted in 184 billion fake Bitcoins being created (reverted by the community).

- Blockchain Forks. The blockchain temporarily forked into two independent chains due to a major software bug. The new Bitcoin client produced a transaction that wasn't accepted by the older client, splitting the blockchain and producing the first real world examples of "double spending".

- Control of the Network. If an attacker had more than 50% of the computing power of the network, the attacker could perform double spending and also reject other people's transactions from receiving confirmations.

Ethereum

- Ethereum fully extends the concept of transactions, by creating “smart contracts”.
- A contract is like an independent entity that is governed by it’s (full-turing) code. It has data storage, it’s own currency balance, and can be interacted with via transactions.
- Now we can easily run arbitrary software on a blockchain without creating a whole new chain.
- Ethereum has an internal currency, “ether”, which is burned as “gas” when executing contracts.

Smart Contracts

A smart contract is a program on the blockchain. Like a regular program, a smart contract has:

- Code
- Inputs
- Outputs
- Data storage

Unlike a regular program, a smart contract is executed by all nodes in the network.

Anyone can send a message (input) to a smart contract, causing all nodes in the network to agree on the state change caused as a result of the message and code.

Smart Contracts

➢A smart contract:

- is fully defined by it's initial code (code is public)
- cannot be modified (unless it's code explicitly permits)
- can receive input from anyone on the network.
- Since a smart contract could fully encapsulate business logic, they can be used to create:

➢decentralized autonomous organisations (DAOs).