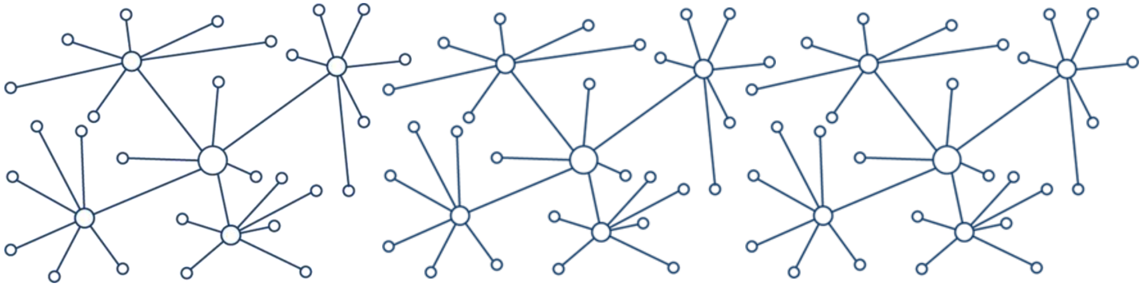


Bitcoin and Crypto Currency Technologies

Elective CSE 662

MTech. I CSE 2nd Sem

(6 and 13 Feb 2023)

Dr. Dhiren Patel

News

- the UK Treasury on Wednesday (1 Feb) outlined a regulatory regime for crypto businesses in Britain. The proposal says that companies wishing to set up shop in the UK will need to obtain authorization from regulators.
- **Bitcoin mining difficulty** hit a new all-time high this week as miners continue to deploy more hardware to mine the largest cryptocurrency by market cap, despite the sector being hit by mounting energy prices.

Technology trends (News)

- Artificial intelligence and acMhine learning will be the most influential technology in shaping the future of trading over the next three years. (Feb 2023)
- Now, AI dwarfs every other major category of technology, its 53% citation rate far and away ahead of API integration (14%) and blockchain (12%). The top 2022 technology, mobile apps, fell to 7%, along with quantum computing and natural language processing.
- Crypto and digital coins, commodities, and credit are predicted to have the biggest increases in electronic trading volumes over the next year!!

Rough weather ahead

- the greatest impact on the markets in 2023
- recession risk (30%), inflation (26%), and geopolitical conflict (19%)

Bitcoin was built on several key innovations

- Firstly, Nakamoto guaranteed that Bitcoin transactions were immutable, by recording all transactions on a distributed ledger known as a blockchain.
- Secondly, he ensured Bitcoin’s scarcity by capping the total number of Bitcoin in existence at 21 million.
- Finally, the community was incentivized to verify transactions by receiving rewards in the form of “mined” Bitcoin for checking the accuracy of the blockchain.

Difficulty adjustment

- Because the Bitcoin network is completely decentralized and not run by any single overarching authority, an algorithm hard-coded into the source code by Bitcoin’s creator(s)
- This algorithm constantly readjusts **the difficulty of the mining process** in line with how many miners are operating in the network to ensure that blocks are discovered at a steady pace.

Difficulty adjustment

- The Bitcoin difficulty algorithm is programmed to keep the entire system stable by maintaining a 10-minute duration for finding new blocks.
- In essence, it takes roughly 10 minutes for one miner out of the entire network to generate a winning code and win the right to propose a new block of bitcoin transactions to be added to the blockchain.
- each 2,016 block interval is called the difficulty epoch (2 weeks = 24 x 60 x 14 = 20160 minutes)

Difficulty adjustment

- To maintain this frequency, the algorithm steps in and increases or decreases the difficulty of mining bitcoin.
- Whenever there’s an influx of miners or mining rigs, it ramps up the difficulty of mining bitcoin.
- If the reverse is the case (that is, if there is a drop in the number of miners competing to find new blocks), the protocol reduces the mining difficulty to make it easier for the remaining miners to discover blocs.
- The mining difficulty of the bitcoin network is altered by adding or reducing the zeros at the front of the target hash.

- Whoever generates a random code that happens to have an equal or higher number of zeros at the front than the target hash first is selected as the winner.

Why?

- The fact that the circulating supply is capped at a maximum of 21 million coins also means it’s a truly finite asset with a relatively scarce maximum supply.
- Both of these factors help support bitcoin’s price over time – assuming demand remains high.

Bitcoin Technology

- Bitcoin components (max. supply 21 M BTC)
- Hash function SHA256
- Puzzle to solve (making x leading bits of block hash to 0)
- Difficulty adjustment (auto – approx. every 2 weeks (time it took to find the last 2,016 blocks) to keep av. time between blocks to 10 min)
- Elliptic curve crypto - Secp256k1 is the name of the elliptic curve used by Bitcoin to implement its public key cryptography (wallets)

Blockchain - visualization

- https://andersbrownworth.com/blockchain/distributed

Blockchain Immutability Demo

- https://andersbrownworth.com/blockchain/hash
- https://blockchaindemo.io/

Cryptocurrency (Wikipedia)

- It is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure transactions, control the creation of units, and verify the transfer of assets
- encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds
- It uses decentralized control as opposed to centralized currency and central banking systems
- (normal (fiat) currency example – exchange, storage, ownership, value, purchase power, trust, production, interoperability..)
- The decentralized control of each cryptocurrency works through DLT, typically a blockchain, that serves as a public financial transaction database (coinbase??)

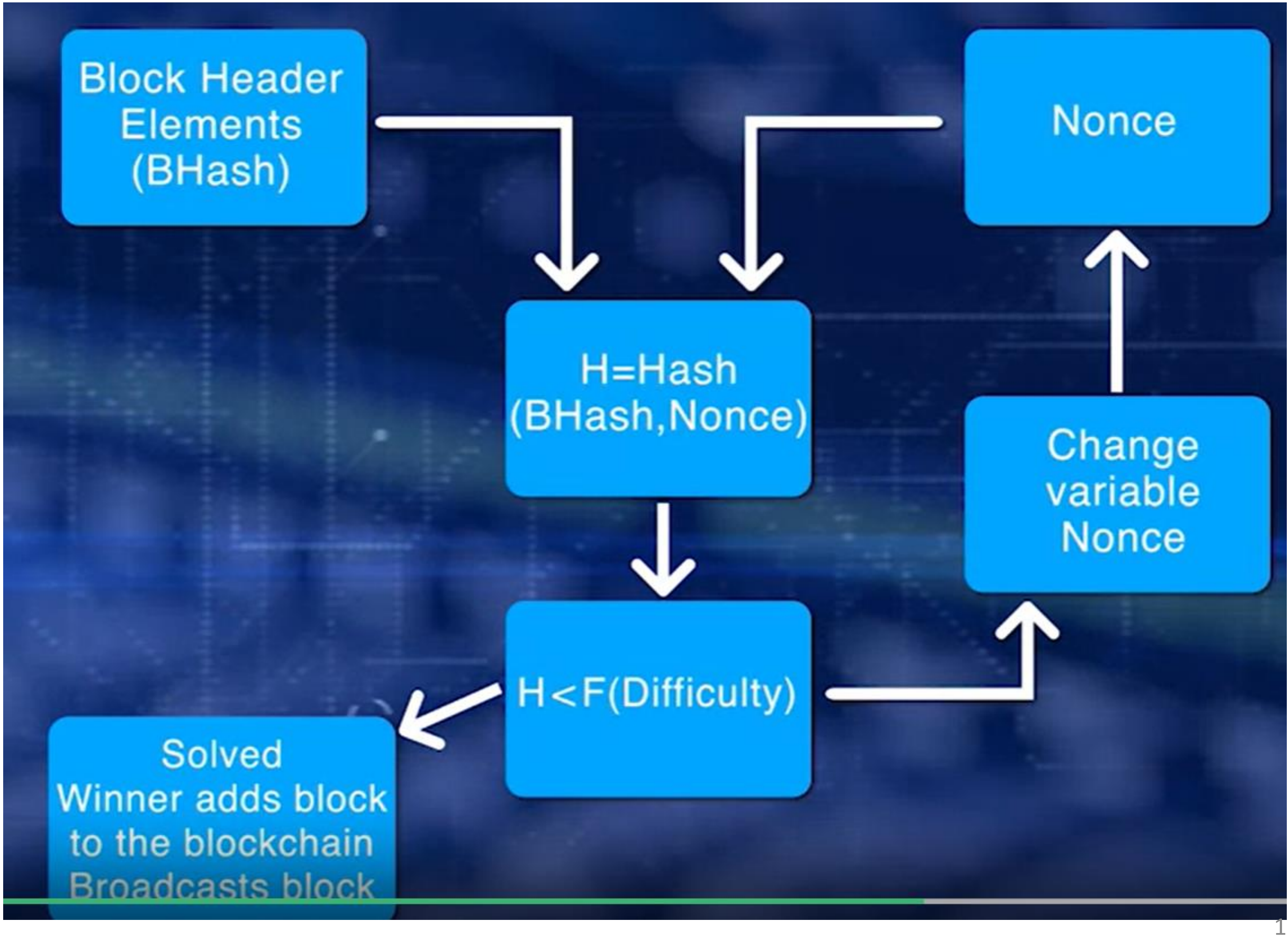
Mining

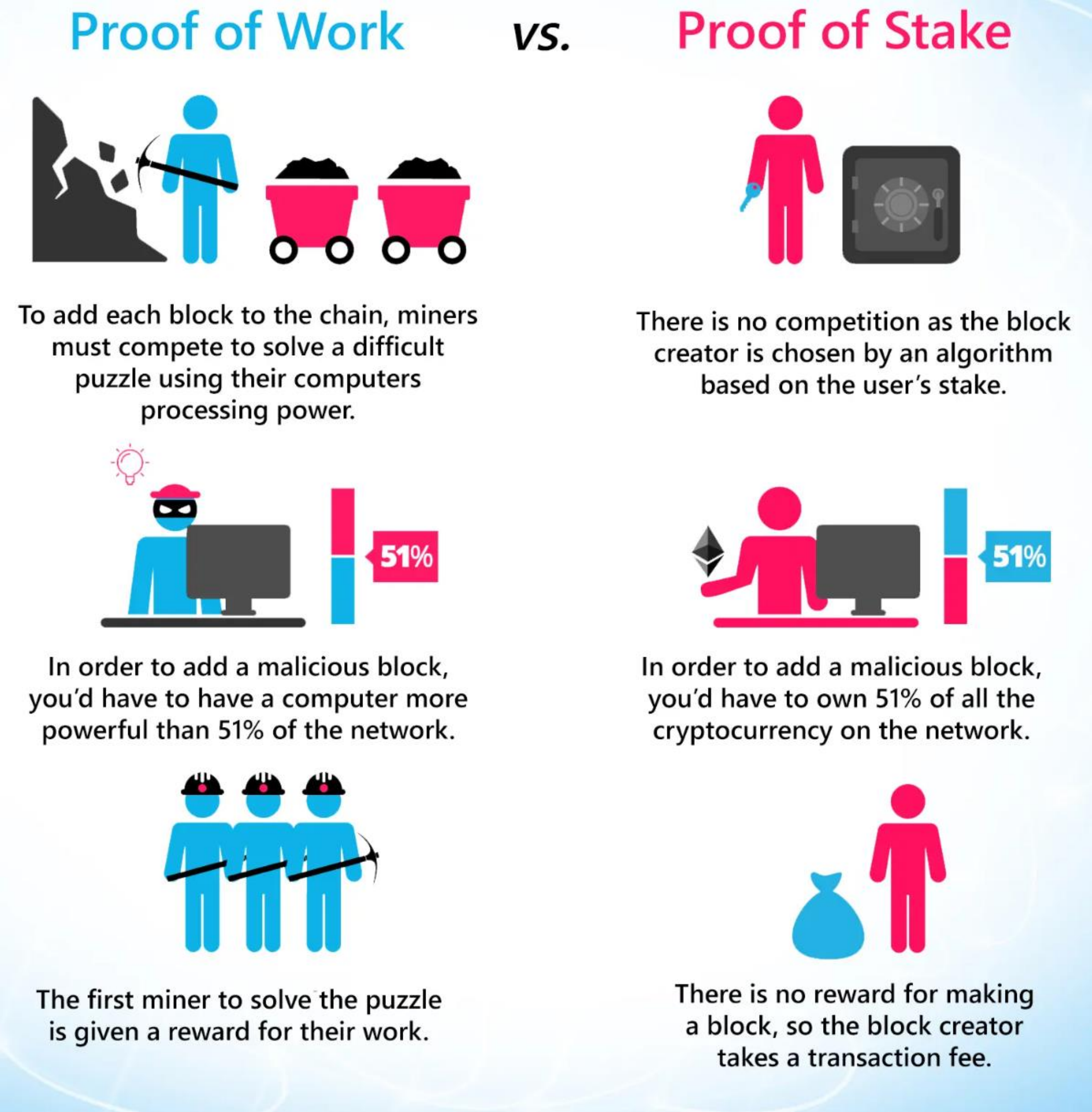
- A trustless and distributed consensus system means that if you want to send and/or receive money from someone you don’t need to trust in third-party services.
- Mining serves as two purposes:
- To verify the legitimacy of a transaction by avoiding the so-called double-spending;
- To create new digital currencies by rewarding miners for performing the previous task.

Mining (Difficulty)

- From a technical point of view, the mining process is an operation of inverse hashing: it determines a number (nonce), so the cryptographic hash algorithm of block data results in less than a given threshold.
- This threshold, called difficulty, is what determines the competitive nature of mining

Proof of Work Puzzle and Difficulty


Block Header Elements (BHash)
Nonce
H=Hash (BHash,Nonce)
Change variable Nonce
H<F(Difficulty)
Solved Winner adds block to the blockchain Broadcasts block



Proof of Work vs. Proof of Stake

Proof of Work	Proof of Stake
To add each block to the chain, miners must compete to solve a difficult puzzle using their computers processing power.	There is no competition as the block creator is chosen by an algorithm based on the user's stake.
In order to add a malicious block, you'd have to have a computer more powerful than 51% of the network.	In order to add a malicious block, you'd have to own 51% of all the cryptocurrency on the network.
The first miner to solve the puzzle is given a reward for their work.	There is no reward for making a block, so the block creator takes a transaction fee.

PoW v/s PoS

- Using a Proof-of-Work system, bad actors are cut out thanks to technological and economic disincentives.
- programming an attack to a PoW network is very expensive, and you would need more money than you can be able to steal
- the Casper protocol (Ethereum PoS), a bad validator might lose their deposit. (use the set some circumstances)

What? Why?

- Blockchain’s decentralized network participants, are not necessarily known to each other.
- Credentials cannot be checked by the conventional means such as verifying who you are with your driver's license.
- Participants can join and leave the chain as they wish.
- They operate beyond the boundaries of trust.

What? Why?

- Given this context: how do you identify the peer participants?
- How do you authorize and authenticate the transactions?
- How do you detect forged or faulty transactions?
- Private public key pair and hashing are important foundational concepts in decentralized networks that operate beyond trust boundaries.

Double spending

- what if more than one miner solves the consensus puzzle where it close in time to each other?
- What if more than one transaction references as input the same digital asset?
- There's a possibility that digital currency and other consumables are single used digital assets, can be intentionally or inadvertently reused in transactions.
- This situation is called double spending.

Handling exceptions

- In a decentralized network, like a blockchain, there is no intermediary.
- We need a policy and an automatic deterministic way to handle this situation.
- A policy for handling transaction and double spending in Bitcoin is to allow the first transaction that reference the digital asset and reject the rest of the transaction that reference the same digital asset.
- There should be a well-defined processes for handling exception improve trust in the blockchain

Fork

- Background - a minor perturbation in the chain - is handled as a naturally expected occurrence within the block chain.
- On the other hand, occasionally, a minor process adjustment has to be carried out typically by bootstrapping a new software to the already running processes.
- This is soft fork. (sort of - the release of software patches)

Hard fork

- Hard fork implies a major change in the protocol.
- (sort of – a new version of operating system)
- Forks are mechanisms that add to the robustness of the blockchain framework.
- Well-managed forks help build credibility in the blockchain by providing approaches to manage unexpected faults and planned improvements.

Forks

- A **Soft Fork** is a fork where updated versions of the protocol are backwards compatible with previous versions.
- A **Hard Fork** is a change of the protocol that is not backwards compatible with older versions of the client. Participants would absolutely need to upgrade their software in order to recognize new blocks.

What is the threat to Bitcoin?

- Bitcoin has never been successfully hacked, but many see brute force attacks using quantum computers as the likely tool someone would use to take down Bitcoin.
- Could Quantum Computers Defeat Bitcoin? Not So Fast

Quantum computing

- Quantum computing uses quantum mechanics to perform operations on data at much greater speeds than modern computers.
- Many times more powerful than an average desktop PC, quantum computers are attractive in calculation-heavy cryptography, but are much more challenging to build, program, and use.
- Their speed and processing power, crypto enthusiast fear, may one day be able to break the encryption used to secure Bitcoin.

Estimate by University of Sussex

- a quantum computer with 1.9 billion qubits could essentially crack the encryption safeguarding Bitcoin within a mere 10 minutes.
- Just 13 million qubits could do the job in about a day.
- IBM unveiled its 127-qubit processor in 2021, while a unit sporting 1,000 qubits is set to be completed by the end of 2023.

Future

- The process of upgrading existing private keys, however, could create new vulnerabilities.
- That’s because, new keys will be generated by the system after successfully implementing post-quantum encryption.
- To activate a switch to the new key, users will have to sign for approval with their old one.

Problem

- Sizable dormant wallets, like the ones containing around 1 million Bitcoins that supposedly belong to Satoshi Nakamoto, likely will never see an encryption enhancement.
- This could leave certain legacy portions of the crypto ecosystem open to quantum-based attacks even if the blockchain they rely on has been safely upgraded.

Progress

- if researchers were successful in developing quantum computing, the first target would not be cryptocurrency but massive stores of leaked and stolen encrypted data that nation-states have accumulated over the years
- While quantum computers may still be years away from posing a threat to encryption and cryptocurrency, several companies—including Google, Microsoft, Amazon, Raytheon, and Lockheed Martin—have entered the race to bring quantum computing to the market.

Token Economics: Crypto currency foundations

- Back in time before there were governments, before there was currency, one system that worked for acquiring goods was barter.

The History of Purchasing Assets

- Before the introduction of currency, assets were obtained through a barter system, which meant goods were directly exchanged
- led to problems where one or both actors did not want what the other had to offer, which necessitated the involvement of other secondary actors to complete relatively simple transactions
- with a tangible measure of value - metal coins were invented in Lydia (Turkey) – 2600 years ago
- in order to decrease the weight of carrying coins and further ease the use of currency, the Chinese invented paper money in the 7th century
- State or Central Banks were created to monitor and regulate the system – 19th century
- the Internet allowed for remote transactions with electronic money – 20th century (facilitated the transfer of assets, increasing liquidity)

What do these things have in common?

Types of Currencies

Commodity Currencies

- transfer of value
- transfer of assets

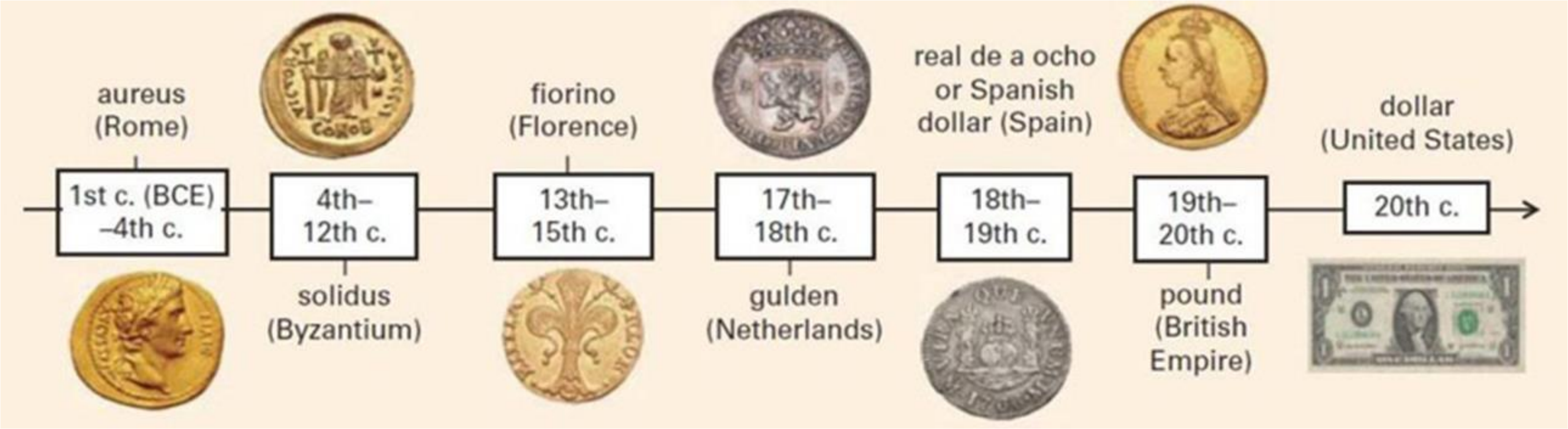
Barter system

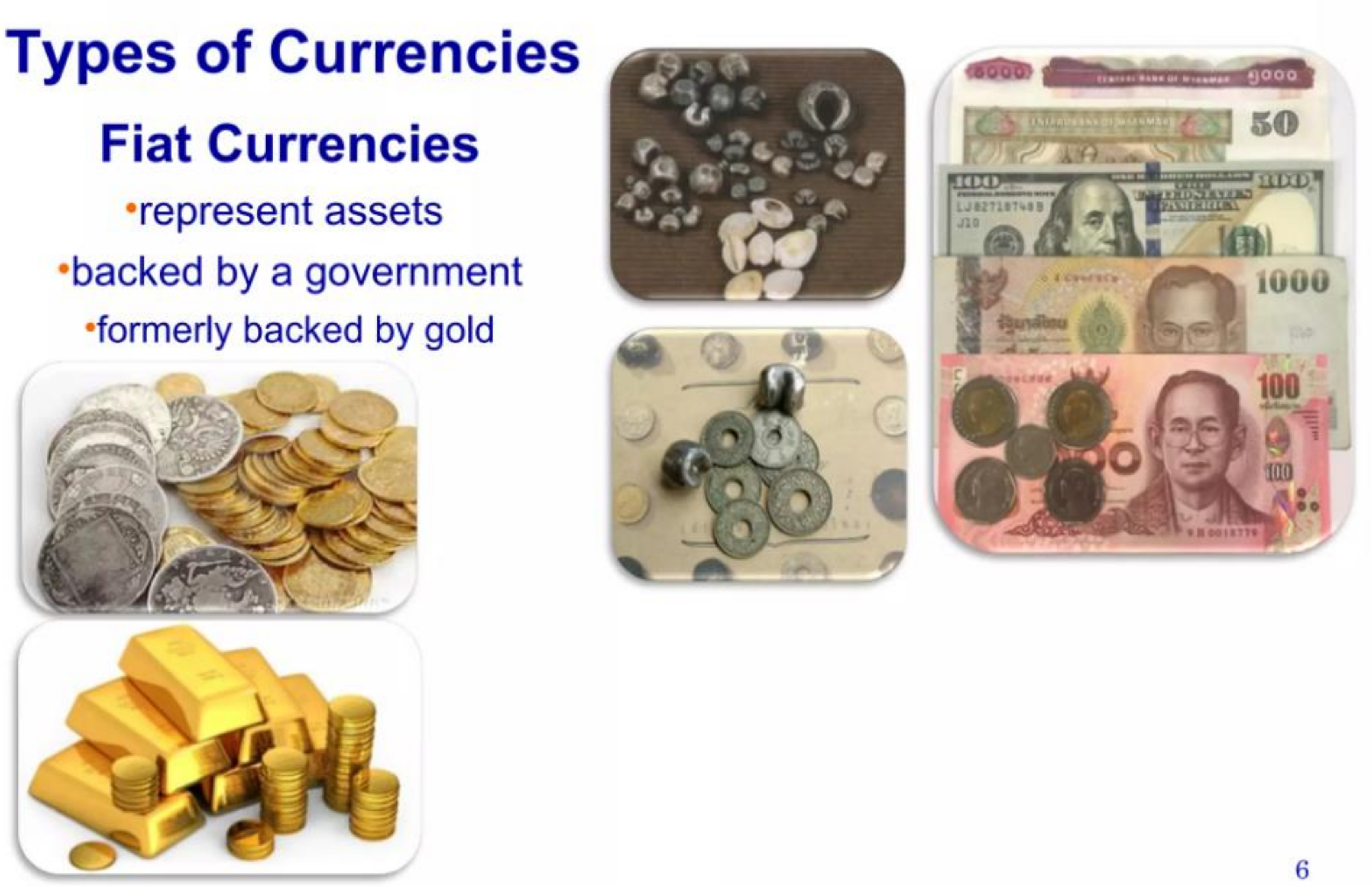
- Let’s say Alice wants a tool and Bob wants medicine. If each of them happen to have what the other person needs, then they can swap and both satisfy their needs.
- On the other hand, let’s say Alice has food that she’s willing to trade for a tool, while Bob, who has a tool, doesn’t have any need for food. He wants medicine instead.
- Alice and Bob can’t trade with each other, but if there’s a third person, Carol, who has medicine that she’s willing to trade for food, then it becomes possible to arrange a three-way swap where everyone gets what they need.

Coordination problem in Barter system

- The drawback, of course, is coordination — arranging a group of people, whose needs and wants align, in the same place at the same time.
- Two systems emerged to solve coordination: credit and cash

Evolution of Cash





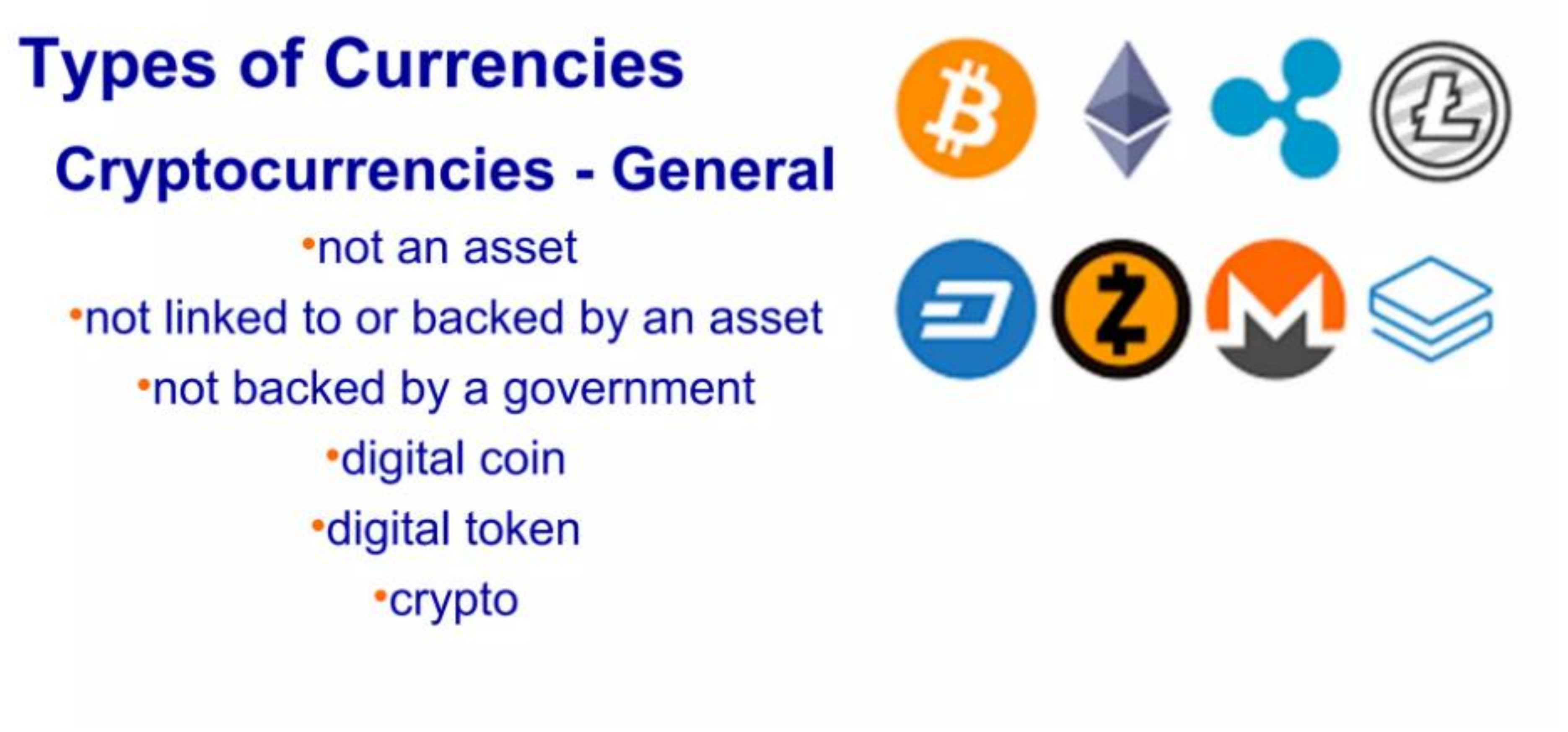
Types of Currencies

Fiat Currencies

- represent assets
- backed by a government
- formerly backed by gold

Blockchain Technology

- Blockchain at the core is a social innovation that gives individuals more freedom because they are less dependent on middle men, government and companies



Types of Currencies

Cryptocurrencies - General

- not an asset
- not linked to or backed by an asset
- not backed by a government
- digital coin
- digital token
- crypto

agenda

- set of clear rules and guidelines on how to deal with tokenization
- to achieve widely supported token regulation
- to reduce the barriers to the adoption of tokenization and help realise the wider societal benefits

Tokens

- Although the use of tokens dates back to ancient times, new technology, such as blockchain, increases the potential of tokens.
- Token technology offers more efficient digital solutions for, among other things, existing financing methods (e.g. crowdfunding, fractional ownership) and the emergence of completely new models for financing and partnerships.
- Because tokens are also programmable, it provides new opportunities for companies to be more flexible with regard to ownership, voting rights, dividends, and financing.

Tokens

- Tokens offer us the chance to rethink collaboration across society as a whole, from businesses to governments and citizens. With tokens, value transactions become immutable, verifiable and traceable without the need for an intermediary, while significantly increasing efficiency and effectiveness.
- Until today, real estate, collectables and art have been perceived as illiquid, but with the advent of tokens, this will drastically change.
- When such assets are tokenised and sold across the globe, they have the potential to become highly liquid.
- That would result in an influx of liquid assets (trillions of USD) that could significantly change global markets.

Tokens

- A token is a *representation of something in the blockchain*.
- This something can be money, time, services, shares in a company, a virtual pet, anything.
- By representing things as tokens, we can allow smart contracts to interact with them, exchange them, create or destroy them.

Why Tokenization?

- Tokenization is the process of transferring the information and associated values of real world assets onto the blockchain
- tokenization is somewhat similar to corporatization: stocks are akin to tokens, rights and conditions are set out by smart-contracts, and the classic stock exchange has its digital reflection
- Its much more than Corporatization.... with
- automated smart contracts for increased conversion rates, commands for automatic transactions, and formulas for calculation of the asset price

Tokenization

- With the help of tokenization, you don’t need to be at the point of purchase: all terms of the deal will be set out by the smart contract
- smart contract is a set of tasks that the program automatically carries out when the asset owner fulfills certain conditions
- It then creates a valuation, or deal, which can be independently verified on the platform
- So, tokenization is more about the digitization of assets in an accessible and transparent manner, in order to share their value among multiple actors

terminology

- **Tokens**: the digital representation of value (e.g. asset) on a blockchain.
- **Tokenisation**: the process of changing value (e.g. asset) into its digital representative
- **Tokenomics**: the study of the emerging field of the design of crypto tokens and related digital assets using economic incentives, game theory, cryptography and computer science.
- **Token engineering**: the practice of using tokens as the foundation for designing value flows and ultimately economic systems
- **Purpose-driven tokenisation**: leveraging the exchange of value to drive behaviours of an ecosystem towards a particular goal

Crypto currency basics

- online capital distribution protocols - that transfer the cash flow of the assets. These protocols have the responsibility of allowing access to the various sources of cryptocurrencies and fiat money, as well as hedging against misuse and bad actors

Proof of Asset Protocol

- connects asset-buyers with asset-sellers
- Proof-of-Asset means the token released as part of the protocol is insured with an asset
- It also allows for independent experts to create different add-ons like oracles, databases, and nodes
- As a result, the Proof-of-Asset protocol will bring increased cash flow to the token that is issued by an originator, or asset owner
- The Proof-of-Asset protocol involves participants who control, validate and verify the transactions, which makes ecosystem more trustworthy

Initial Smart-Asset Offering (ISAO)

- Tokenization can be performed using an ISAO.
- ISAO is a new method for businesses (farms, stores, manufacturing plants) to raise capital using tokenization of their assets
- an ISAO may be held only when the company controls a physical asset. As a result, technology startups or research and development activities cannot be tokenized
- Tokenization further facilitates the trading of assets and makes it more secure.
- Tokenization transfers real-world assets to the world of the blockchain

Tokenization 2.0

- For example, in the case of real estate, there will be tokenization of assets of different qualities, which will allow for a new method of their evaluation
- possible through the globalization of capital
- these assets will acquire new features, such as voting, analysis, dividends, and the possibility of quick unrestricted transactions among many others.
- As a result, the market built around tokenization will become more sustainable
- Increased demand will catalyze the growth of price, demand, and associated expectations
- Tokenized assets’ price growth is essentially an added value to the new opportunities that will open with the transition to blockchain
- So, tokenization is a perfect way to increase capitalization and raise an asset’s value

Tokenization 2.0

- In the blockchain, transactions will be held without bank accounts and currency conversion, and the number of documents needed for the identity verification significantly decrease
- Will tokens with smart-contracts be able to replace traditional equity?
- technically it’s possible - the costs of such an upgrade is a challenge today
- In the near future, the majority of companies will tokenize their assets, and government regulators will have to adapt to the changing reality…

Tokenization 3.0

- strengthen the linkages between the world of blockchain and traditional economy
- tokenization development will increase the variety and flow of cryptocurrencies and fiat money, and cryptocurrency holders will therefore be incentivised to buy traditional assets
- the correct interaction of a large number of components, such as depositaries, cadastre chambers, archives, dealers and distributors, KYC, escrow agents – expensive affair

Tokenization 3.0

- Tokenization of intangible assets (such as audio and video content) may decrease their cost and improve their availability, which will be convenient, but not profitable
- With the help of the smart-contracts code, it is possible to prevent market manipulation, financial mismanagement, corruption, and money-laundering
- Smart-contracts also solves problems such as misdirected transactions, transaction repayment, and public keys loss
- Cryptocurrency Popularization – no more exclusive territory of advanced internet users and programmers

Tokenization 3.0

- Soon enough car dealers, real estate agents, traders, bankers, directors and senior executives will have to know about the blockchain ecosystem, just like they are currently adapting to internet-marketing
- positive effect on transparency and the integrity of a business linked with blockchain

Tokenization 3.0

- Tokenization of assets requires the formation of registers, depositories, and companies that store the data and rights concerning real estate and equities (Data Store security)
- IoT is made up of sensors and smart devices that automatically count, weigh, identify and transfer information to the decision center
- E.g. RFID sensors transfer data to blockchain and make cargo transportation more transparent
- Tokenization of assets will provide important opportunities for related industries as well as important connections between the blockchain and fiat economies

why we need tokenization?

- **Shared understanding** – how to align interests and motivations to collaborate and make progress in ecosystems?
- **Innovative funding** – how to fund ecosystems beyond traditional VC financing or (bank) loans?
- **Change management** – how to understand and facilitate the change implied with new ways of interacting?
- **Messaging and engagement** – should the narrative around tokenization change to enable innovative ecosystems?
- **Knowledge and skills** – what skills do organisations need to transition to tokenised ecosystems?
- **Problem-solution fit** – how to ensure addressing real problems where tokenization can help realise in new solutions?
- **Tokenization and the law** – what are the legal requirements around purpose-driven tokenization?

Why do we need token financing?

- There are many reasons why we need token financing. One of the main reasons is that it offers companies a variety of benefits, including the democratization of value.
- Token financing simplifies raising funds across borders, opening up new markets, and, with that, potentially new customers.

DeFi

- Decentralized Finance (DeFi), is one of the core sectors that keeps itself busy with creating new protocols with a seamless UI/UX experience, improved interoperability, decentralized exchanges, and self-sovereign identity.

Regulations

- Any industry confronted with disruptive technology faces the challenge of establishing a legal framework that sets the rules of the game to protect investors, consumers and companies and get rid of bad actors.
- The same applies to the blockchain ecosystem. Therefore, we to create a robust regulatory system that embraces these forms of new technology.

Token ecosystem

- *A well-designed token ecosystem unlocks value by bringing parties together in new ways and stimulates the target behaviour by having cryptographic tokens as built-in incentives.*

SHARED UNDERSTANDING

Coming from multi disciplinary worlds, it's most important that we understand each other.

INNOVATIVE FUNDING

It starts with technology itself. We need great software first.

CHANGE MANAGEMENT

Adoption is not technology. It begins with awareness and acceptation. How do we get there?

MESSAGING & ENGAGEMENT

We need to explain the added value of Tokenization to speed up adoption.

KNOWLEDGE & SKILLS

With giving people relevant skills & knowledge, perhaps with case studies, we'll tackle the fear surrounding Tokenization."

PROBLEM-SOLUTION FIT

We need usability, improbability and legal clarity in general. Let's paint a picture using prototyping.

TOKENIZATION AND THE LAW

"You can get people to do stuff if you'll reward them with tokens. This is a superpower."

Trent McConaghy

We need unification of regulation. To do so, we need more co-operation and simplification.

"Tokenized ecosystems are a lot like evolutionary algorithms. This was all with simulated evolution. Reward the mechanism that does what you want it to do."

Trent McConaghy

Use cases

- Tokens offer multiple, technical, advantages over traditional funding. First of all, they are programmable. This means that governance and rules can be embedded within the token.
- For example, the longer you hold a token, the more dividend you will receive. This allows you to drive the behaviour of your investors while raising funds.
- In addition, tokens are transparent, secure and traceable, giving regulators more control to ensure correct behaviour.

Use cases

- Anything can be tokenised and made liquid, including real estate (fractional ownership), CO2 rights, mobility, futures, art or even entire clubs and sport contracts to increase fan engagement.

Fan Tokens

- Redefining Fan: It’s a range of different tribes who consume the same brand as you and me, but just in a different way. And therefore you need different products for those different fans.
- The reason that fan tokens exist is not just for the domestic/local fans, it's really to try to go after the non-local fans, the 99% of fans that are not in a stadium

Token contract

- A *token contract* is simply an Ethereum smart contract. "Sending tokens" actually means "calling a method on a smart contract that someone wrote and deployed".
- At the end of the day, a token contract is not much more a mapping of addresses to balances, plus some methods to add and subtract from those balances.

Token contract

- It is these balances that represent the *tokens* themselves. Someone "has tokens" when their balance in the token contract is non-zero. That’s it!
- These balances could be considered money, experience points in a game, deeds of ownership, or voting rights, and each of these tokens would be stored in different token contracts.

Fungibility

- *Fungible goods* are equivalent and interchangeable, like Bircoin, Ether, fiat currencies, and voting rights.
- *Non-fungible* goods are unique and distinct, like deeds of ownership, or collectibles.
- when dealing with non-fungibles (like your house) you care about ***which ones*** you have,
- while in fungible assets (like your bank account statement) what matters is ***how much*** you have

Token standards

- the community has developed a variety of **standards** (called EIPs or ERCs) for documenting how a contract can interoperate with other contracts
- ERC20: the most widespread token standard for fungible assets, (somewhat limited by its simplicity).
- ERC721: the de-facto solution for non-fungible tokens, often used for collectibles and games.
- ERC777: a richer standard for fungible tokens, enabling new use cases and building on past learnings. Backwards compatible with ERC20.

ERC20

- An ERC20 token contract keeps track of *fungible* tokens: any one token is exactly equal to any other token; no tokens have special rights or behavior associated with them.
- This makes ERC20 tokens useful for things like a **medium of exchange currency**, **voting rights**, **staking**, and more.

ERC721

- what if not all tokens are alike?
- This comes up in situations like **real estate** or **collectibles**, where some items are valued more than others, due to their usefulness, rarity, etc.
- ERC721 is a standard for representing ownership of *non-fungible* tokens, that is, where each token is unique.

ERC777

- Like ERC20, ERC777 is a standard for *fungible* tokens, and is focused around allowing more complex interactions when trading tokens.
- The standard also brings multiple quality-of-life improvements, such as getting rid of the confusion around decimals, minting and burning with proper events, among others, but its killer feature is **receive hooks**.
- A hook is simply a function in a contract that is called when tokens are sent to it, meaning **accounts and contracts can react to receiving tokens**.

ERC777 hooks

- This enables a lot of interesting use cases, including atomic purchases using tokens (no need to do approve and transferFrom in two separate transactions), rejecting reception of tokens (by reverting on the hook call), redirecting the received tokens to other addresses (similarly to how PaymentSplitter does it), among many others.

ERC777

- Furthermore, since contracts are required to implement these hooks in order to receive tokens, *no tokens can get stuck in a contract that is unaware of the ERC777 protocol*, as has happened countless times when using ERC20s.
- The ERC777 standard is **backwards compatible with ERC20**, meaning you can interact with these tokens as if they were ERC20, using the standard functions, while still getting all of the niceties, including send hooks.

What is an ICO?

- An ICO or Initial Coin Offering is the initial offering of a digital cryptographically secure piece of data (**a digital token**) created on a blockchain as part of a decentralised software protocol
- An ICO is a **popular way to raise money** for a new project/start up by distributing a percentage of the initial currency supply to early supporters of the relevant project

ICO

- Unlike conventional crowdfunding, however, tokens are usually tradable via online exchanges. This **liquidity helps attract investors**, and means that the overall ICO process has similarities both with conventional crowdfuning and with an Initial Public Offering
- An initial coin offering (ICO) is a type of capital-raising activity in the cryptocurrency and blockchain environment. The ICO can be viewed as an initial public offering (IPO) that uses cryptocurrencies.

VC, CrowdFunding vs ICOs

- **VC, Crowdfunding**
  - Slow settlements
  - Many intermediaries
  - Costly process
  - Opaque process
  - Lack of liquidity for investors

- **ICOs**
  - Can raise money in seconds (e.g. Filecoin raised $252 Million in 30 minutes; Brave’s 'Basic Attention Token' raised $36 Million in 30 seconds)
  - No intermediaries involved
  - Low cost of token issuance
  - Transparent process
  - Offers immediate liquidity to investors
  - Paperless process

Steps - ICO

- **1. Identification of investment targets**
- **2. Creation of tokens (**existing blockchain platforms that run existing cryptocurrencies such as Ethereum allow the creation of the tokens with minor modifications of the code.**)**
- **3. Promotion campaign**
- **4. Initial offering**

Stablecoins

- Cryptocurrencies are constantly subject to exchange rate fluctuations and are characterized by high price volatility.
- For making crypto money more useful and more stable, a special type was created: stablecoins.
- Stablecoin is a cryptocurrency whose value is tied (pegged) to some valuable asset ("stable" asset or basket of assets).

Stablecoins

- This asset could be fiat money, precious metals like gold and silver, oil or almost anything that has tangible value.
- Realization of a better monetary system: one that would be resistant to hyperinflation, free from centralized control, and more stable and robust than the monetary systems that came before it.

Ideal Stablecoin functions

- An ideal stablecoin should perform three main functions:
- Act as a means of exchange (buying and selling goods and services directly).
- Be a saving asset (allowing funds to be saved without loss of value).
- Be used as a unit of accounting (comparing the cost of goods and services).

Stablecoin examples

- **Commodity-backed -** Stablecoins backed by commodities such as precious metals (gold, silver etc.) are much less likely to be inflated than fiat backed stablecoins. It is harder to mine gold or silver than it is to "create money out of thin air." E.g. DGX (Digital Gold Tokens) – 1gm of Gold

Stable coin examples

- **Fiat-backed -** The value of stablecoins of this type is based on the value of the backing currency, which is held by a third-party regulated financial entity. Fiat-backed stablecoins can be traded on exchanges and are redeemable from the issuer. E.g. USDT (USD Tether) – 1 USD
- **Cryptocurrency backed** - issued with cryptocurrencies as collateral, which is conceptually similar to fiat-backed stablecoins. E.g. DAI – 1 USD

Seigniorage-style coins

- Seigniorage-style coins utilize algorithms to control the stablecoin’s money supply, similar to a central bank's approach to printing and destroying currency.
- Significant features of seigniorage-style stablecoins are:
  - Adjustments are made on-chain
  - No collateral is needed to mint coins
  - Value is controlled by supply and demand through algorithms, stabilising price
- (a less popular form of stablecoin)
- E.g. Basis (shutdown in Dec 2018)

Tether (USDT)

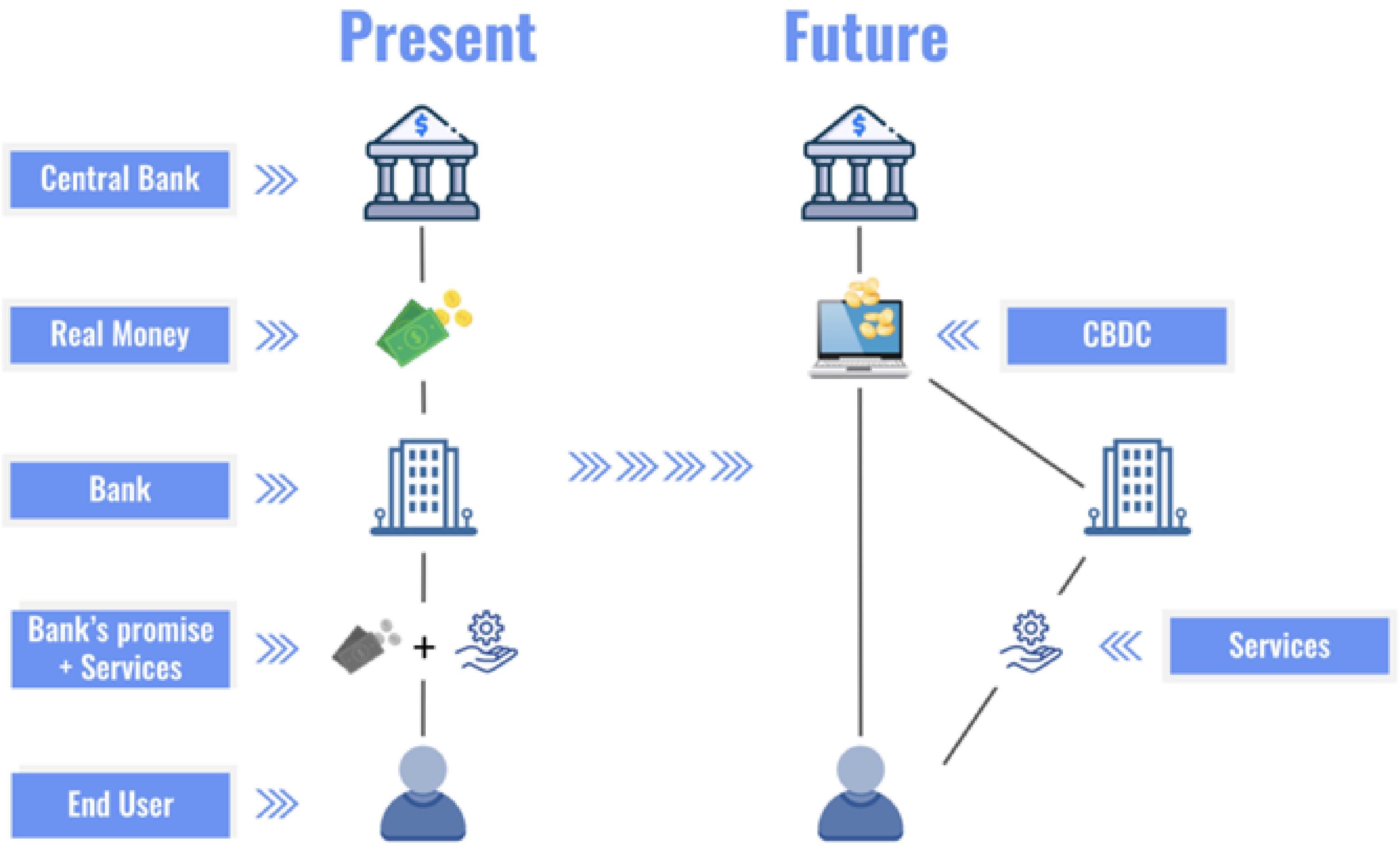
- Issued by Circle Inc. since 2015
- Price ~1 USD
- Discrepancies – 1 USD = 82.74 INR, 1 USDT = 87 INR
- Circulation supply ~68.32 B
- Financial Stability Oversight Committee to add new rules for stablecoins and to regulate stablecoin issuers like banks

Assets

- Anything, both tangible and intangible, that can be owned and exchanged for value, is considered an asset.
- There are a variety of assets in financial markets from physical assets such as commodities (oil, electricity, food), infrastructure (real estate, machinery, trains), and exotic luxury goods (art, cars, collectibles), to non-physical assets such as patents, copyrights, and goodwill.
- By having so many contrasting and private record-keeping systems, it becomes difficult to price assets based on holistic market observations.

Towards CBDC

- Central Bank (issued) Digital Currency



Present

Future

Central Bank

Real Money

Bank

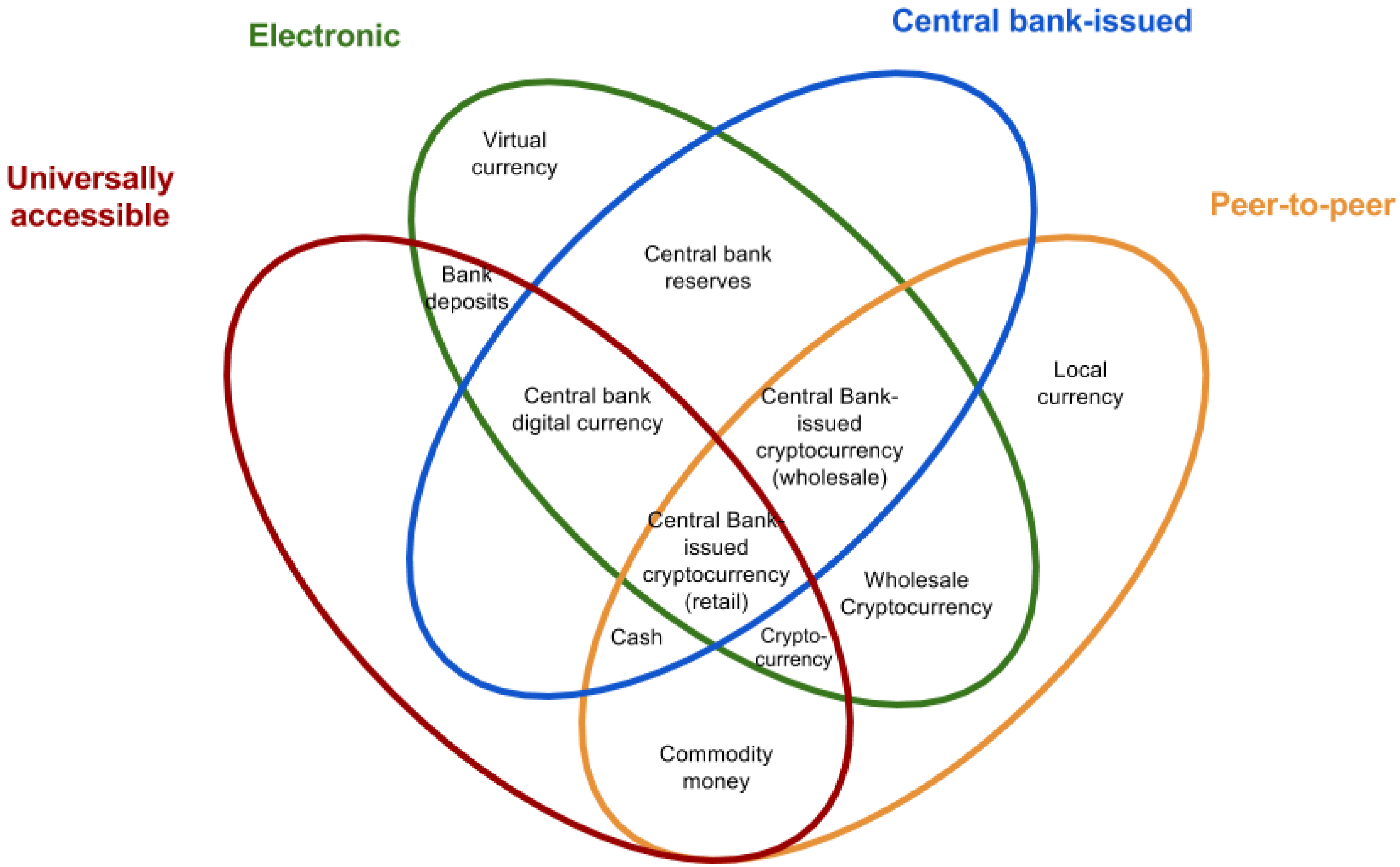
Bank's promise + Services

End User

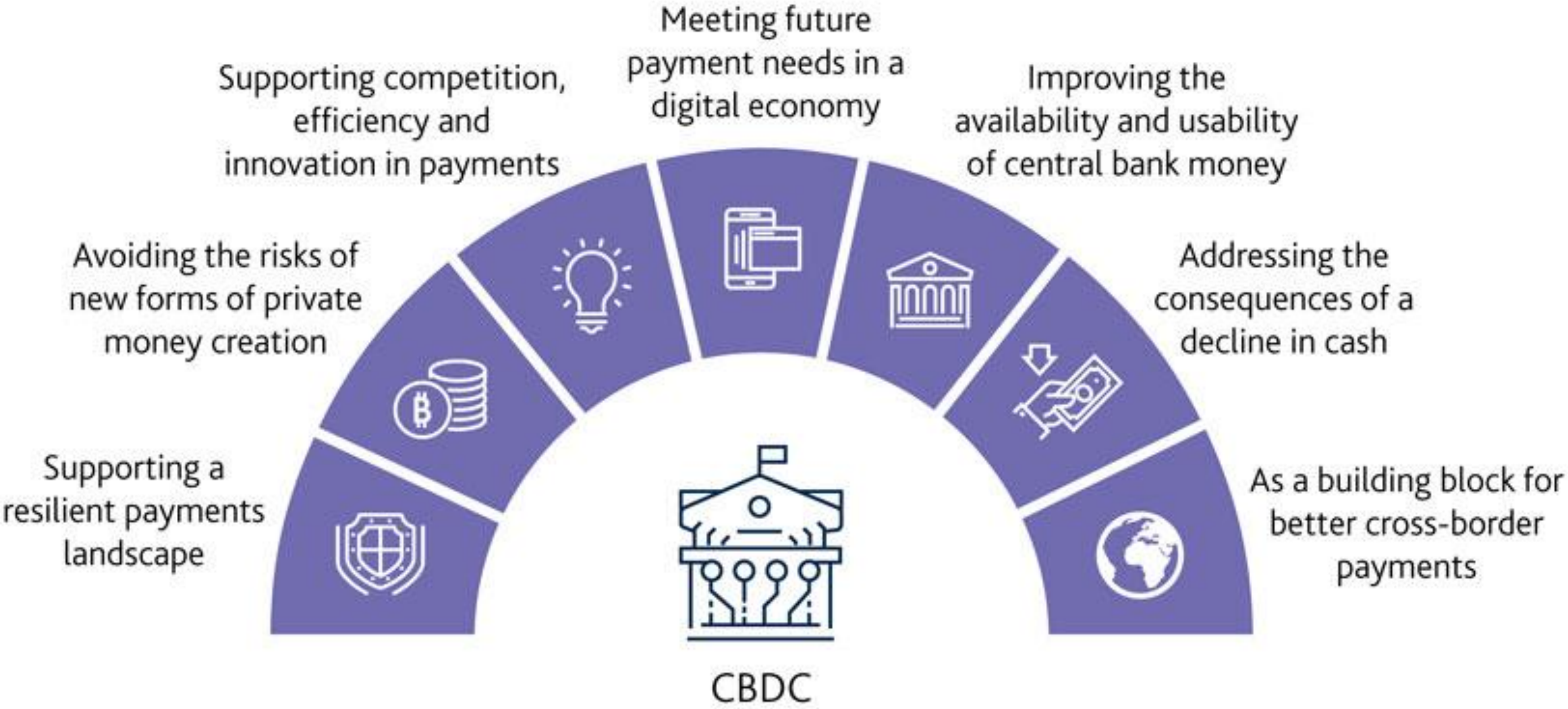
CBDC

Services

The money flower: a taxonomy of money



Adaptation from Bank for International Settlements (2017)



Supporting a resilient payments landscape

Avoiding the risks of new forms of private money creation

Supporting competition, efficiency and innovation in payments

Meeting future payment needs in a digital economy

Improving the availability and usability of central bank money

Addressing the consequences of a decline in cash

As a building block for better cross-border payments

CBDC

Source: Bank of England

News 13 Feb

- **Draft EU Rules Will Force Banks to Give Cryptocurrencies Highest Risk Rating**
- banks would need to give all their crypto asset exposure a proposed risk weight of 1,250% until December 2024, meaning they will be forced to hold an equal amount of capital matching the crypto they hold.
- BTC and ETH are having the first negative week in 2023 (Feb 2nd week – price reduced!)

Group 2

- Well-known cryptocurrencies such as Bitcoin (BTC) and Ethereum (ETH) would be considered to be Group 2 cryptoassets
- Group 2 assets are then subdivided into two groups by the committee: Group A, which covers crypto holdings that are made via ETFs or other derivatives, which can be traded on regulated public markets, and Group B where this isn’t the case.
- Group 2 B assets will be given a proposed risk weight of 1,250%, whereas Group 2 A will be subject to lower requirements.

Group 1

- However other forms of crypto assets, such as tokenized versions of traditional assets like equities, some types of stablecoins which don’t rely on algorithms to maintain their price, and potential Central Bank Digital Currencies (CBDCs) would fall under lower capital requirements and are considered to be in Group 1.
- A bank’s total exposure to Group 2 crypto assets must not exceed 2% of the bank’s capital

Assignments

- Burning coin (Wallets) – how to create one?
- Block Chain Analysis – what parameters are there? What are the historical tx (e.g. Pizza buying (May 2009))?
- Check explorers of Different tokens (crypto currencies) – Bitcoin, Ether, Solana, Avax, Monero, Link – and study differences