Cryptocurrencies, central bank digital currencies and DLT: developments, implications and security

Ayse Zoodsma-Sungur, 7 June 2018

DeNederlandscheBank
EUROSYSTEEM

Overview

1) Common drivers of FinTech innovations
2) Terminology
3) First things first: Distributed ledger technology
4) Cryptocurrencies
5) Central bank digital currencies (CBDC)

Common drivers of Fintech innovations

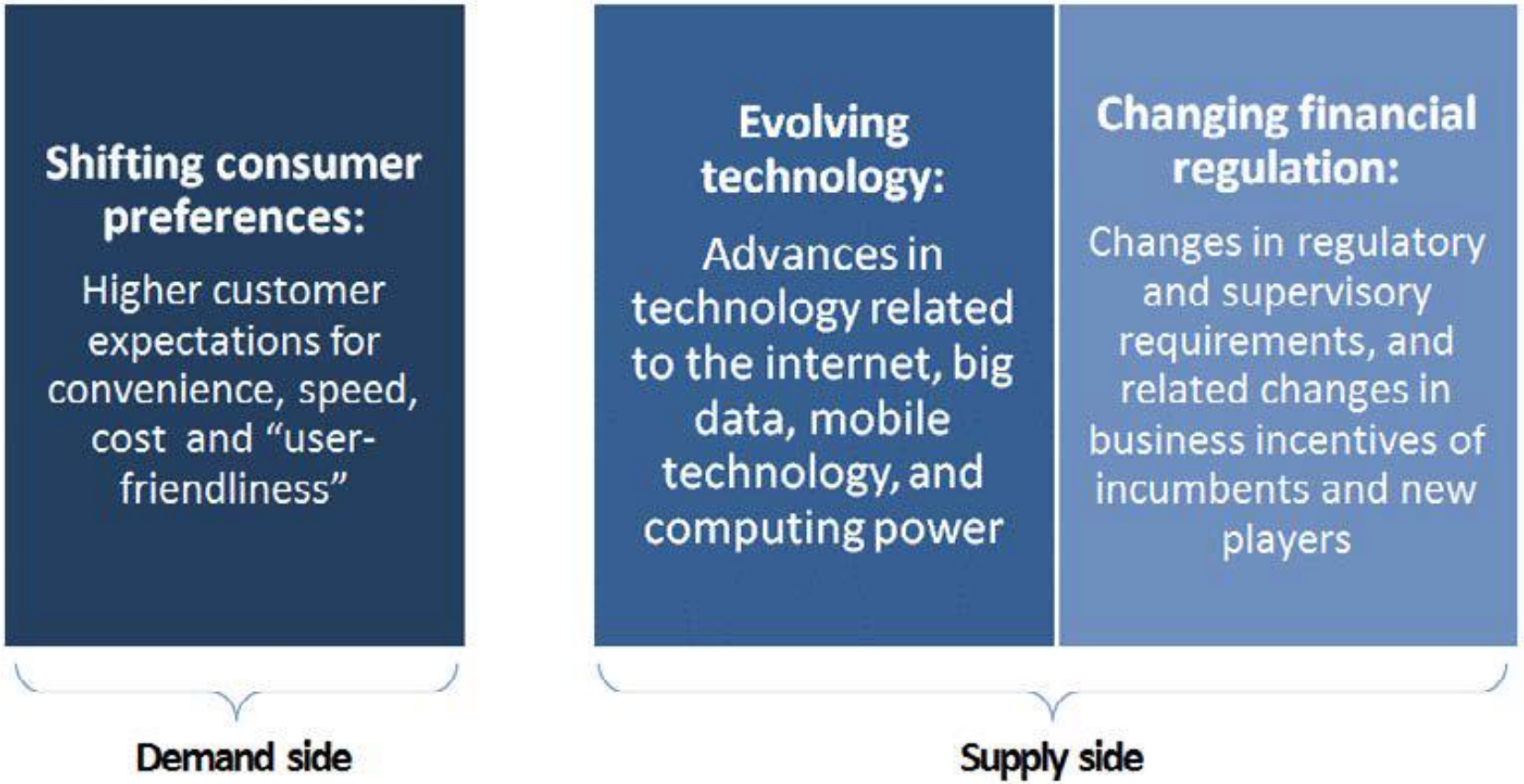
Innovation in financial services is not a new phenomenon.

Over the past few decades, innovations have included;

- credit cards in the 1960s,
- debit cards and cash dispensing terminals (ATMs)
- telephone banking in the 1970s and 1980s,
- internet banking and branchless banking
- mobile telephony, internet-based operators, and both hardware and software providers

Q: Are the latest wave of innovations different than previous ones?

Common drivers of Fintech innovations 2



Terminology

For the purpose of this presentation, FINTECH*:

> "FinTech is technologically enabled financial innovation that could result in new business models, applications, processes, products, or services with an associated material effect on financial markets and institutions and the provision of financial services".

This definition includes, among others,

- peer-to-peer lending,
- equity crowdfunding,
- financial applications of DLT,
- financial applications of machine learning, robo-advice, etc.

*Slightly adapted definition used by the Financial Stability Board.

Distributed ledger technology (DLT)

Distributed ledger technology (DLT)

DLT is a type of database that is spread across multiple sites, countries or institutions.

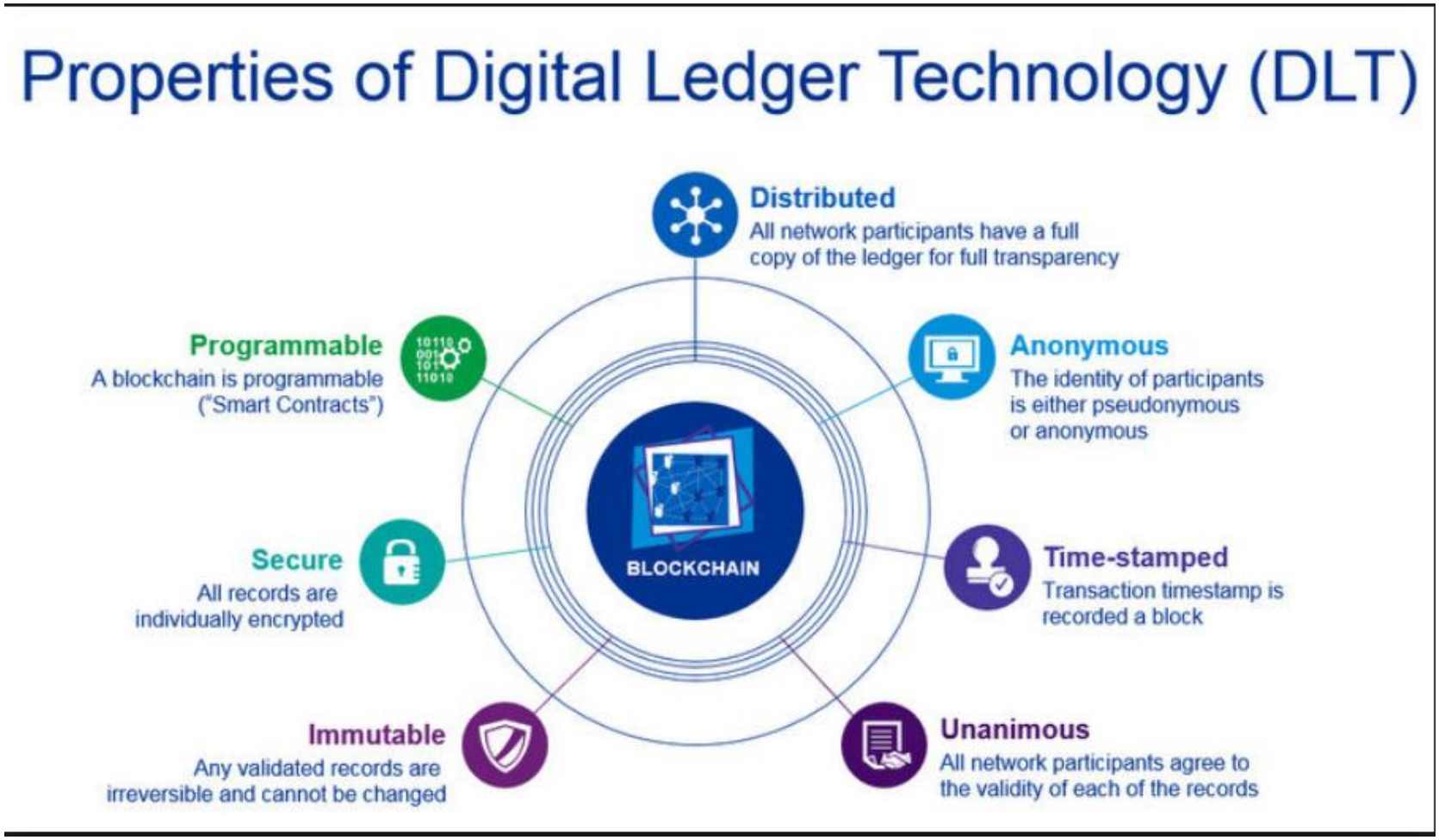
It is **decentralised** in nature, no need for an intermediary to process, validate or authenticate transactions.

Each party (e.g., individual, organisation or group) is represented by their computer, called a **node**, on the network.

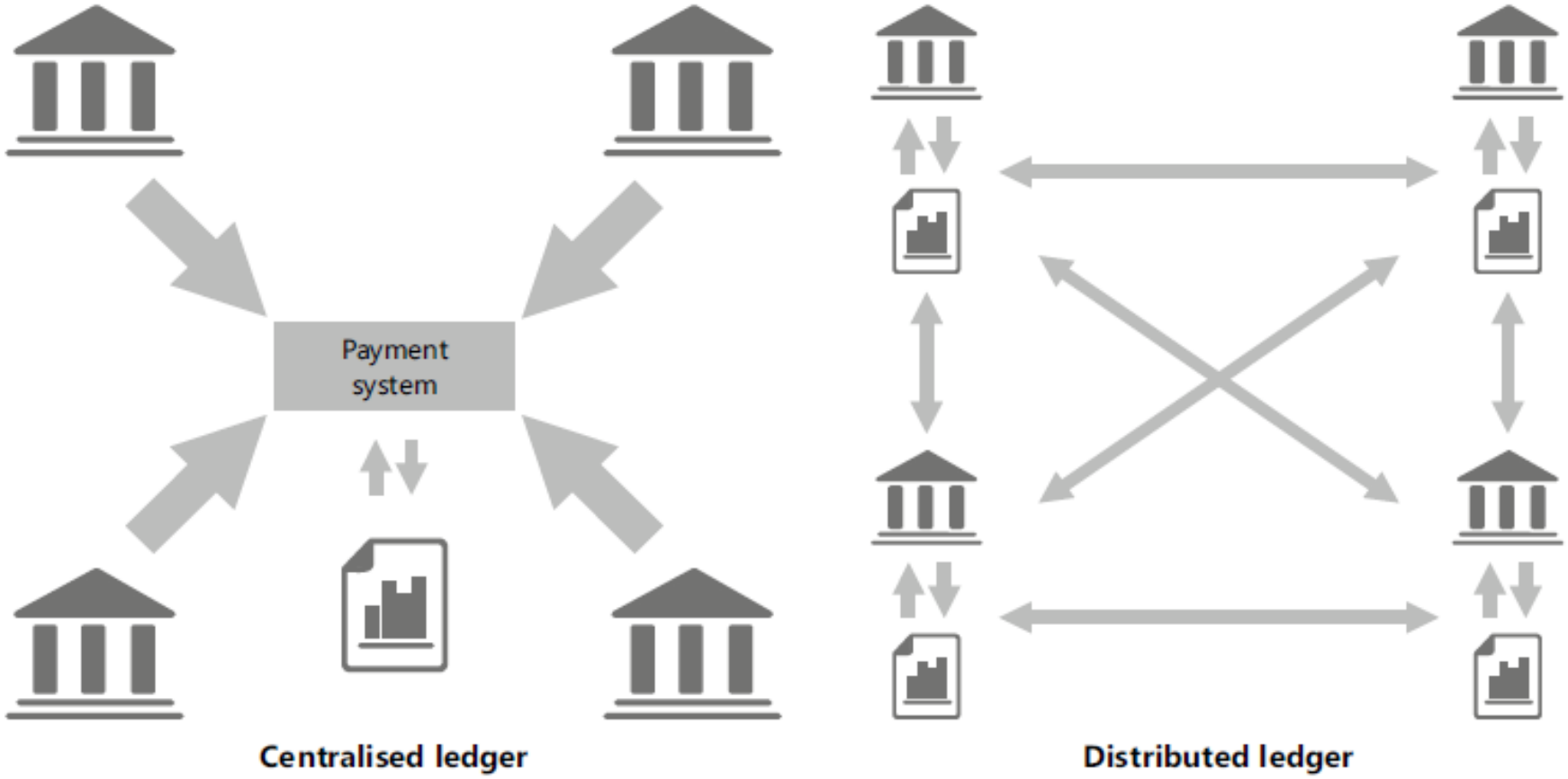
Each node keeps its own copy of all transactions on the network, and nodes work directly with one another to check a new transaction's validity through a process called **consensus**.

Each of these transactions is **encrypted** and sent to every node on the network to be verified and grouped into timestamped blocks of transactions.

Distributed ledger technology (DLT) 2



Distributed ledger technology (DLT) 3



Source: Santander InnoVentures (2015).

Distributed ledger technology (DLT) 4

DL **can be open**, verifying anonymous actors in the network,

or

they **can be closed** and require actors in the network to be already identified.

The best known existing use for the distributed ledger is the **Bitcoin**.

Simply, DLT refers to the **protocols** and **supporting infrastructure** that allow computers in different locations to propose and validate transactions and **update records in a synchronized way across a network.**

Key takeaways

- DLT allows for decentralised processing, validation and authentication of transactions.
- DLT has several unique and valuable characteristics that over time could transform a wide range of industries.

Distributed ledger technology (DLT) 5

DLT has several attractive features , among others:

- Transactions can be made to be **irrevocable**, and clearing and settlement can be programmed to be **near-instantaneous**, allowing distributed ledger operators to increase the accuracy of trade data and reduce settlement risk.

- Systems operate on a **peer-to-peer** basis and transactions are **near-certain** to be **correctly executed**, allowing DL operators to eliminate supervision and IT infrastructure, and their associated costs.

- Each transaction in the ledger is openly verified by a community of networked users rather than by a central authority, making the distributed ledger **tamper-resistant**;

- Each transaction is automatically administered in such a way as to render the transaction **history difficult to reverse**.

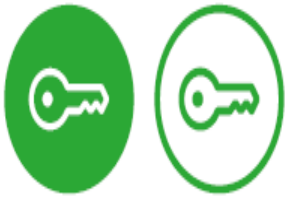
Distributed ledger technology (DLT) 6

1 Disintermediate

In a peer-to-peer model, every peer in the network is a server and client, thus eliminating the middlemen in processes between users.

Enables the facilitation of transactions without a central, privileged third party even in the absence of trust.

2 Secured by cryptography



Public key cryptography is a method for verifying digital identity with a high degree of confidence, enabled by the use of private and public keys.

Allows for increased security and protection of data and identity in the system.

3 Smart Contracts & Oracles

Smart Contracts are virtual agreements encoded on the DLT that can be automatically reconciled based on logical conditions.

Enables the secure automation of complex, logical agreements and the business processes using data gathered by Oracles.

Distributed ledger technology (DLT) 7

4 Immutable

Data on the DLT is immutable, and is thus resistant to double-spending, fraud, censorship and hacking efforts.

Creates a more secure, transparent network and creates new avenues for regulators.

5 Real-time settlement

DLT allows for near real-time settlement of transactions, removing friction and reducing risk.

Enables transactions to be made in near real-time between users on the network.

6 Trustless

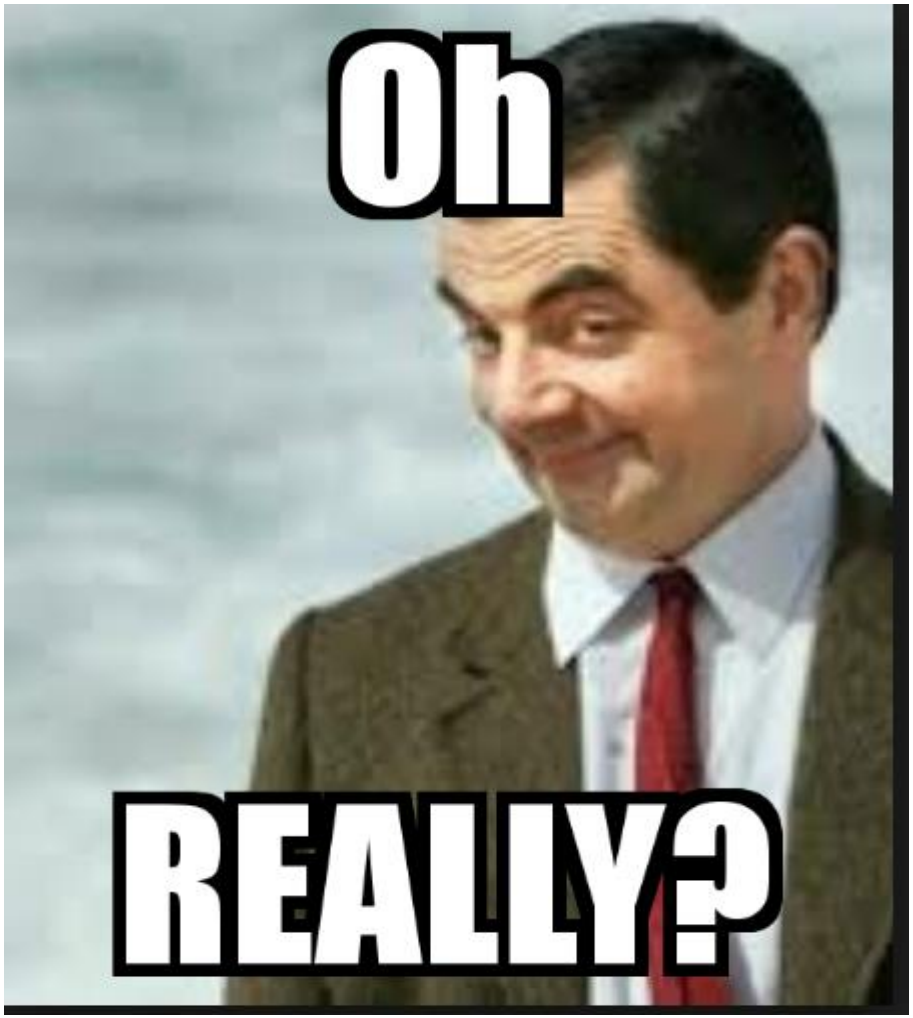
DLT is based on cryptographic proof, allowing any two parties to transact directly with each other without a trusted third-party.

Allows two or more trustless parties to transact directly with each other.

Distributed ledger technology (DLT) 6

Key takeaways

- Digital signatures enable DLT transactions to be tamper and fraud resistant.
- Many DLTs enable the use of smart contracts which are agreements encoded on the network that can be automatically executed when certain predefined conditions are met.



Distributed ledger technology (DLT) 6

But, all that glitters is not gold as:

- it is costly to operate (preventing double-spending without the use of a trusted authority requires transaction validators (**miners**)) to employ large amounts of computing power to complete "**proof-of-work**" computations);

- there is only probabilistic finality of settlement; and all transactions are public.

These features are not suitable for many financial market applications.

DLT use cases: when is DLT the answer?

Operational simplification

DLT reduces/eliminates manual efforts required to perform reconciliation and resolve disputes

Regulatory efficiency improvement

DLT enables real-time monitoring of financial activity between regulators and regulated entities

Counterparty risk reduction

DLT challenges the need to trust counterparties to fulfil obligations as agreements are codified and executed in a shared, immutable environment

Clearing and settlement time reduction

DLT disintermediates third parties that support transaction verification/validation and accelerates settlement

Liquidity and capital improvement

DLT reduces locked-in capital and provides transparency into sourcing liquidity for assets

Fraud minimisation

DLT enables asset provenance and full transaction history to be established within a single source of truth

Cryptos

Cryptos

A physical object, usually a coin or a note, represent cash. When this object is handed to another individual, its ***unit of value*** is also transferred, without the need for a third party to be involved.

No credit relationship arises between the buyer and the seller. This is why it is possible for the parties involved to remain ***anonymous***.

- advantage of physical cash is that whoever is in possession of it, is by default the owner of the unit of value.
- This ensures that the property rights to the ***units of value*** circulating in the economy are always clearly established, ***without a central authority*** needing to keep accounts.
- Furthermore, any agent can participate in a cash payment system; nobody can be excluded. There is a ***permissionless*** access to it.

Cryptos

2

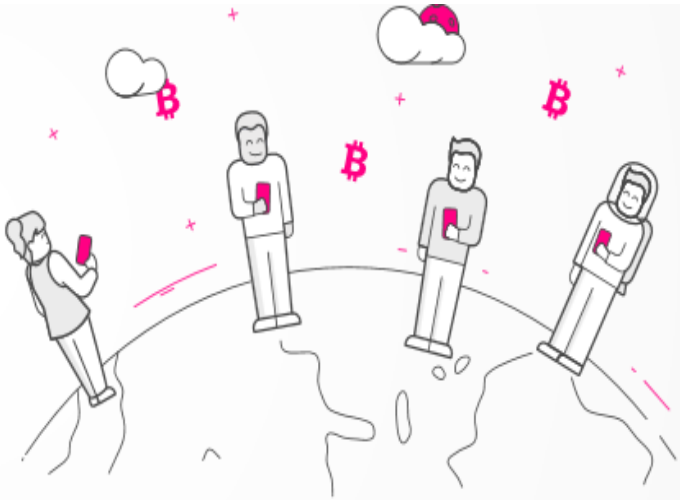
Cryptos are a type of private financial asset that depends primarily on cryptography and distributed ledger technology (DLT) as part of the perceived or inherent value.

Cryptos can have characteristics of privately issued digital means of payment (such as Bitcoin), or characteristics of digital tokens.

Cryptos were originally designed to facilitate transfer of value without the need for a trusted third-party intermediary.

As we learned, cryptocurrencies are digital systems that allow for the exchange of value without third parties.

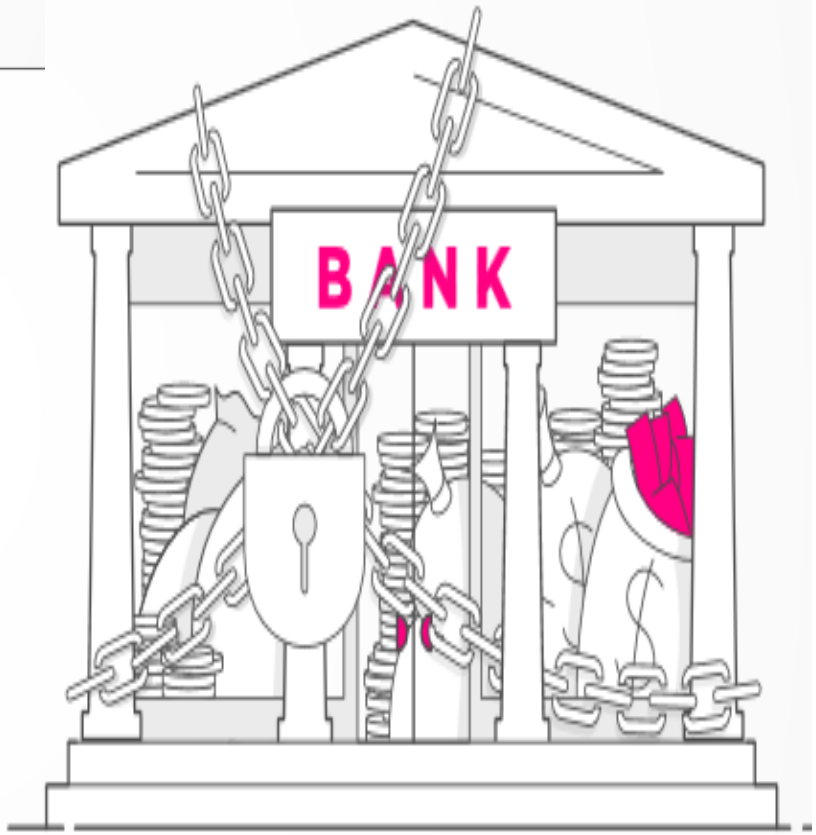
They can be used by anyone, anywhere in the world. There are no dollars, Euros, pesos, or Yen – cryptocurrencies are global.



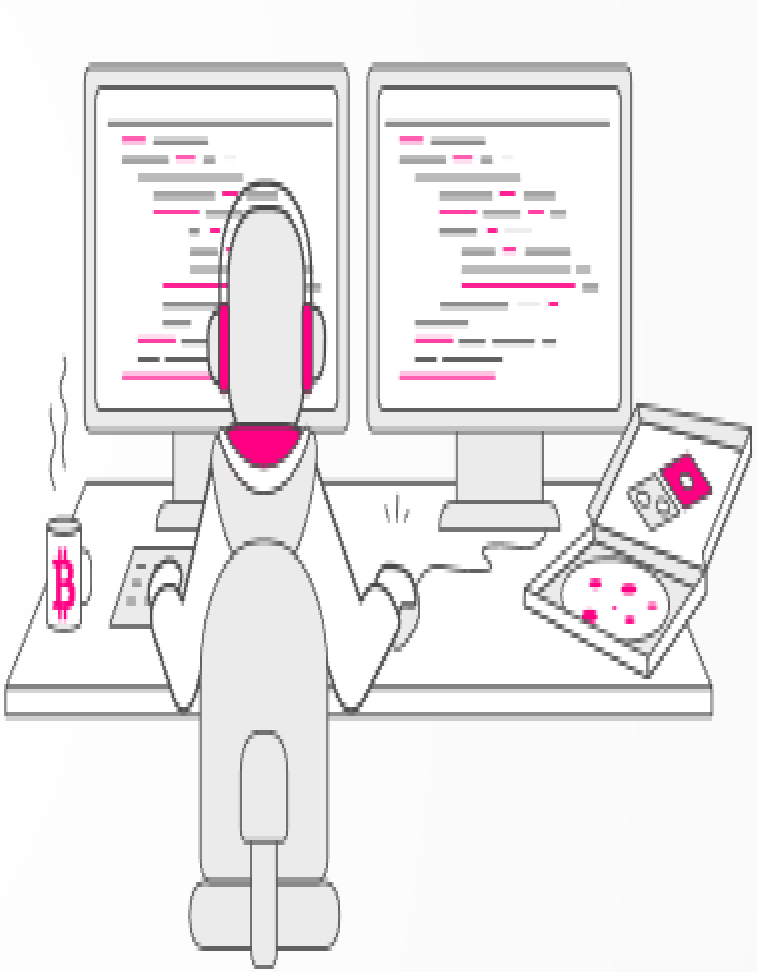
Cryptos

Traditional systems that exchange value (like money) are controlled by banks and governments – which makes them "centralized."

Most cryptocurrencies are not controlled or regulated by any single entity like a bank - which makes them "decentralized."



Cyrptos



In 2008, a mysterious person calling himself Satoshi Nakamoto invented the first cryptocurrency, Bitcoin. To this day, Satoshi remains anonymous and nobody knows who he is.

Cryptocurrencies are designed to let you store, send, and receive value (like money) without any third parties (like banks or credit card companies).

All cryptocurrencies share one important feature: They let you exchange money, files, and other things of value WITHOUT using any third parties.

Cryptos

5

After bitcoin invention, many more followed. They focus on different goals, but they all share the same purpose: remove the middlemen.

If you follow the cryptocurrency markets, it may seem like you're hearing about a new type of digital money every day.

There are 1,658 cryptos, according to investing.com's current list as of Thursday afternoon.

This is up from 1,638 on Monday and less than 1,600 just a couple of weeks ago. And it's up from *one* crypto in existence until just a few years ago (bitcoin).

The largest cryptocurrencies by market cap are

Cryptos

6

Cryptocurrency Name (Code)	Current Price in U.S. Dollars	Market Capitalization
Bitcoin (BTC)	$8,313.40	$139.57 billion
Ethereum (ETH)	$607.14	$59.34 billion
Ripple (XRP)	$0.67	$26.58 billion
Bitcoin Cash (BCH)	$926.25	$15.69 billion
Litecoin (LTC)	$163.03	$9.00 billion
Cardano (ADA)	$0.18	$4.70 billion
NEO (NEO)	$69.74	$4.47 billion
Stellar (XLM)	$0.23	$4.30 billion
EOS (EOS)	$5.15	$3.76 billion
Monero (XMR)	$213.66	$3.37 billion
Dash (DASH)	$416.22	$3.30 billion

Cryptos

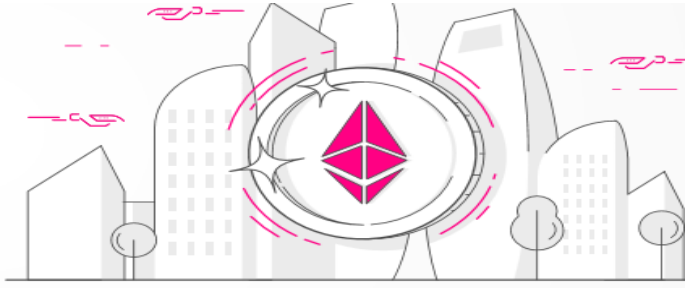
Cryptocurrency Name (Code)	Current Price in U.S. Dollars	Market Capitalization
NEM (NEM)	$0.36	$3.18 billion
IOTA (MIOTA)	$1.08	$2.98 billion
Tether (USDT)	$1.00	$2.22 billion
Tron (TRX)	$0.03	$1.96 billion
Ethereum Classic (ETC)	$18.43	$1.83 billion
VeChain (VEN)	$3.83	$1.83 billion
Lisk (LSK)	$11.46	$1.20 billion
Nano (NANO)	$8.78	$1.17 billion
OmiseGO (OMG)	$11.29	$1.15 billion

ATA SOURCE: WWW.INVESTING.COM. PRICES AND MARKET CAPITALIZATIONS AS OF MARCH 15, 2018 AND PRICES ARE ROUNDED
O THE NEAREST CENT WHERE APPROPRIATE.

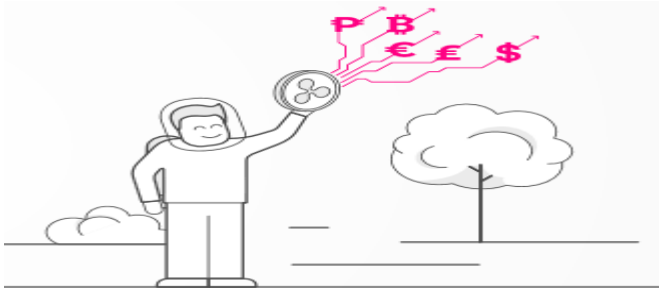
Cryptos

8

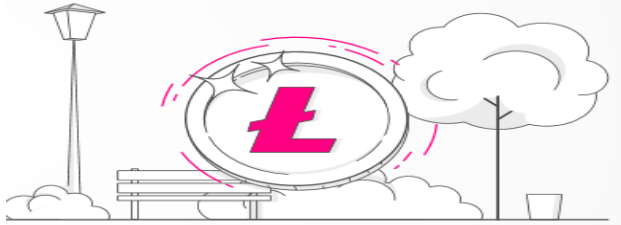
Ethereum is focused on removing middlemen from digital applications. So instead of using Apple's and Google's app stores, you can use apps online through a decentralized community.



What's really interesting about Ripple is that the type of money you put in doesn't have to be the same that comes out. Ripple works like a universal translator for money. You can send Euros and the other party can receive dollars. A global network that's constantly moving money around makes this possible.

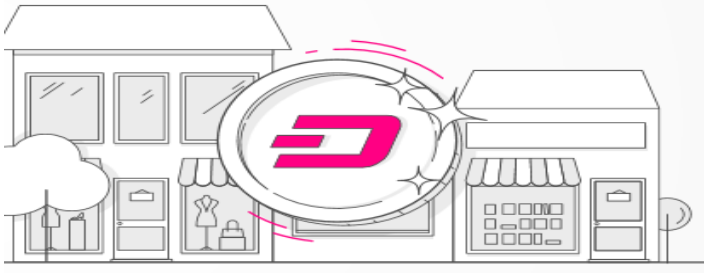


Litecoin is based on the ideas behind Bitcoin but is ocused on being able to process more payments in a shorter period of time. The goal is to make cryptocurrency ready for millions of everyday transactions.

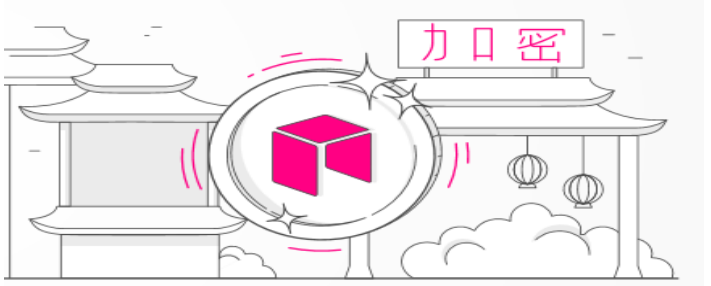


Cryptos

Dash is focused on creating a cryptocurrency that can be used as digital money more conveniently. That's why its name is short for digital cash. It also has built-in community systems to pay for ongoing development and to vote for updates.



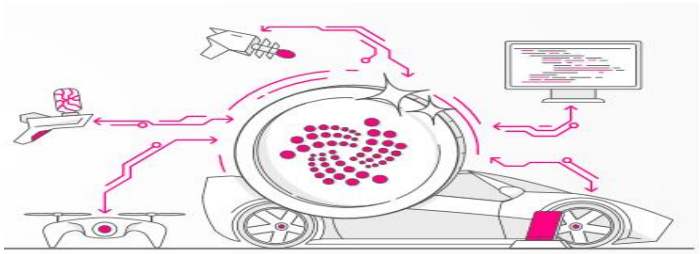
NEO is the first cryptocurrency launched in China. It's similar to Ethereum in that it's designed to remove middlemen from applications. But it's also designed to help manage your digital identity.



Monero is building very private, digital cash. It's designed to be completely anonymous and untraceable. The main goal of Monero is to put you in charge of your money – banks and governments can no longer control or even monitor it.

Cryptos

IOTA is a cryptocurrency that's built to run the Internet of Things (IoT). This refers to all internet-connected devices like your smartphone, smart thermostat, smartwatch, and smart TV. The number of these products is growing quickly and IOTA plans to help run them.



DeNederlandscheBank
EUROSYSTEEM

Cryptos

Last but not least!

Get the terminology RIGHT!

From a legal perspective, crypto is not money or currency as they do not fulfill the functions of money: **a medium of exchange**, **as a store of value**, and as **a unit of account.**

ECB defines cryptos as*:

- a digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money.

*Virtual currency schemes –a further analysis (2015)

Cryptos

What does BIS CPMI say*?

- Mostly they are **assets** with their value determined by supply and demand, similar in concept to commodities such as gold.

However, in contrast to commodities, they have zero intrinsic value.

- Unlike traditional e-money, **they are not a liability of any individual or institution**, **nor are they backed by any authority**.

As a result, **their value relies only on the belief that they might be exchanged for other goods or services, or a certain amount of sovereign currency, at a later point in time.**

*Digital currencies November 2015

Cryptos 13

What does European Parliament say?

The European Parliament adopted the revised Anti-Money Laundering Directive (AMLD5) on 19 April 2018, defining virtual currency as

"a digital representation of value that is not issued or guaranteed by a central bank

or

a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money,

but

is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically".

Cryptos

As demand for cryptos grows, global regulators are divided on how to keep up.

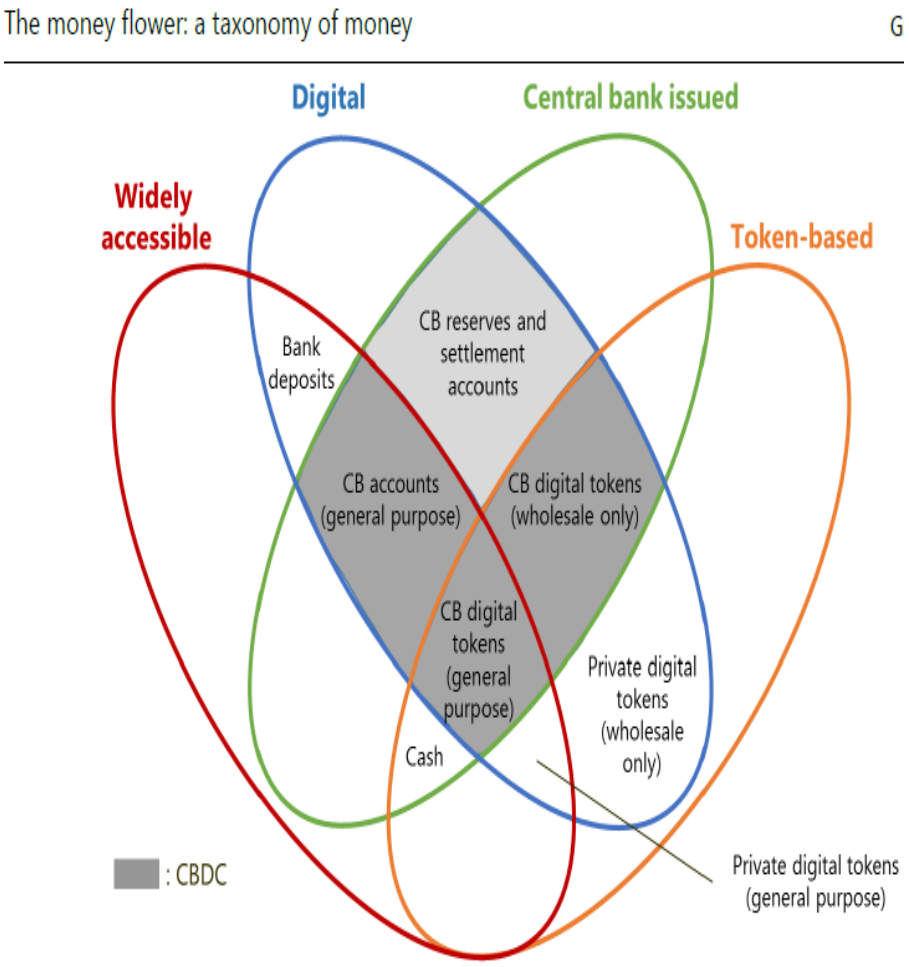
There is a call for more cooperation to look at various issues posed by this topic.

These issues are, among others, :

i) money laundering, ii) financing of terrorism, iii) consumer protection,
iv) financing of illicit activities, etc.

Central bank digital currency (CBDC)

Central bank digital currency (CBDC)



Bech and Garratt's money flower introduces a taxonomy of money that is based on four key properties:

- issuer (central bank or other);
- form (electronic or physical);
- accessibility (universal or limited); and
- transfer mechanism (centralised or decentralised).

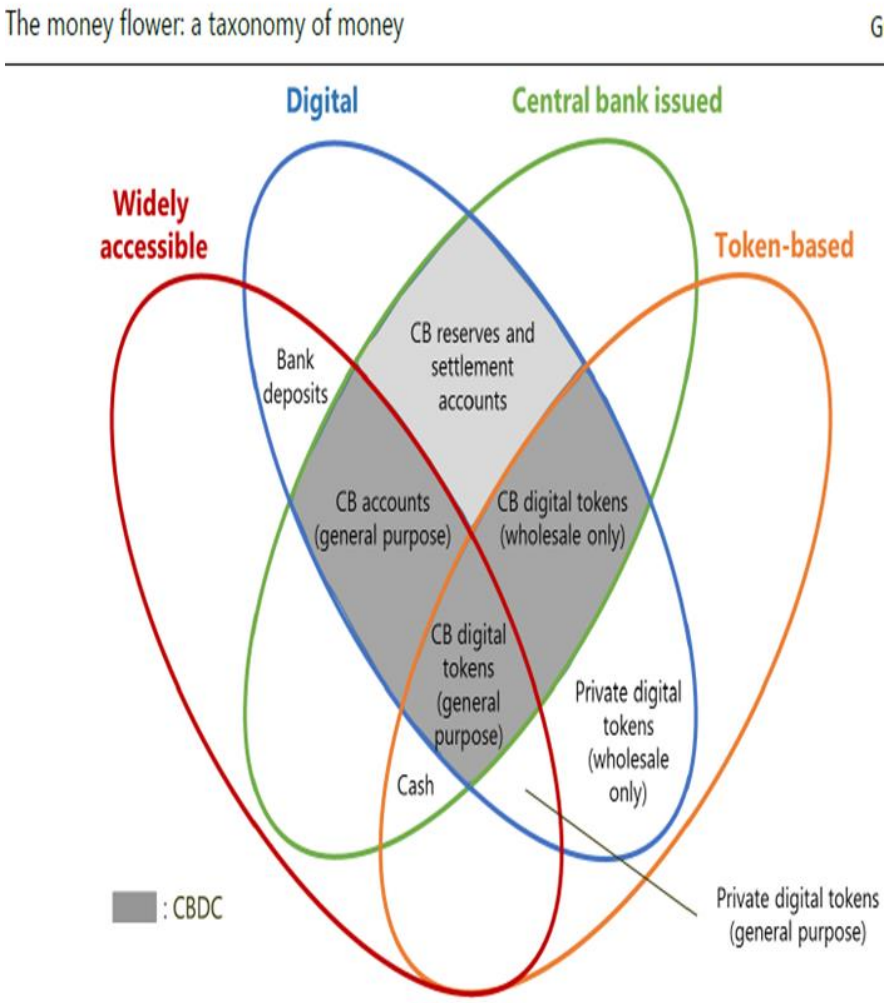
It defines a CBDC as an electronic form of central bank money that can be exchanged in a decentralized manner known as peer-to-peer, meaning that transactions occur directly between the payer and the payee without the need for a central intermediary.

Central bank digital currency (CBDC) 2

This distinguishes CBDCs from other existing forms of electronic central bank money, such as reserves, which are exchanged in a centralized fashion across accounts at the central bank.

The flower distinguishes between two possible forms of CBDC:

a widely available, consumer-facing payment instrument targeted at retail transactions;
and a restricted-access, digital settlement token for wholesale payment applications.



Central bank digital currencies (CBDC) 3

A number of major central banks are actively exploring whether they might issue digital currencies of their own.

While providing greater access to digital forms of central bank liabilities is not an entirely new idea (eg Tobin (1985)), the recent debate has been motivated by a number of factors.

These include, among others, :

- interest in technological innovations for the financial sector;
- the emergence of new entrants into payment services and intermediation;
- declining use of cash in a few countries; and
- increasing attention to so-called private digital tokens.

Possible objectives and motivations for CBDC 4

- A central bank may have multiple objectives for issuing CBDC, such as
  - promoting a sound payment system
  - maintaining monetary and financial stability
  - objectives related to capital markets development and financial inclusion

- Frequently cited motivations are the provision of
  - settlement instrument for potential DLT-based clearing and settlement platforms
  - digital central bank alternative to cash for use by consumers

Possible opportunities for CBDC 5

Opportunities:

Wholesale coin could facilitates credit-riskfree settlement?

Fill the gap caused by a decline of cash usage?

Resilience: alternative payment circuit or technology?

Competition: alternative to bank deposits?

Monetary policy? transmission, interest

Financial inclusion through modern technology?

Possible risks for CBDC 6

- Financial stability: financial structure, risks to banks
- Monetary policy
- Cyber risks
- Will it be used and how?
- Operational cost and risks

Some questions for us all

Potential implications for the interbank settlements – balancing potential efficiency gains against increased or new risks CBDC for retail transactions – a substitute for physical currency

Implications of a retail CBDC

How likely is your central bank going to issue CBDC

Has your central bank engaged, or will engage in academic, policy or operational work related to the development and use of CBDC?

How would CBDC be technically implemented?

Do you see DLT (distributed ledger technology) as an appropriate technology or is there an alternative solution?

Who would be the participants in the system?

How would transactions be initiated, validated, and processed and by whom?

How would users interact with the system (for example, via third-party wallet providers or accounts at a central bank)

Does your central bank also follow developments on private digital currencies or hybrid arrangements (for example, private issuance backed or supported by a central bank)? If yes, what specific work is your central bank conducting?

Thank you