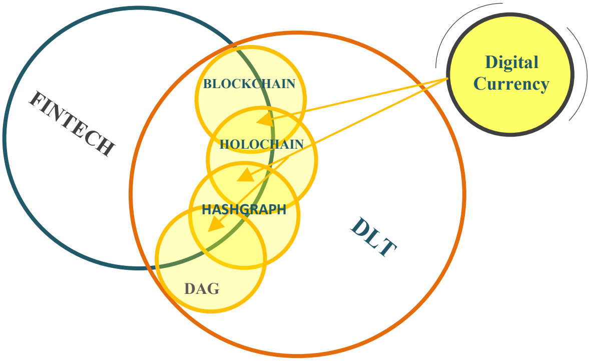
صنـدوق النقـد العربـي
ARAB MONETARY FUND

DIGITAL CURRENCY TECHNOLOGIES

Introductory Booklet series
(Issue No 23)
Intended for the young generation in the Arab Region



Prepared by

Eng. Hichem Rouibi

Arab Monetary Fund
2 0 2 1

The views expressed in this release reflect the point of view of the author of the booklet, not necessarily the view of the Arab Monetary Fund

All correspondences are addressed to:

Economic Department

Arab Monetary Fund

P.O.Box 2818 - Abu Dhabi, United Arab Emirates

Phone : +97126171552

Fax : +97126326454

E-mail : Economic@amfad.org.ae

Website: https://www.amf.org.ae

This booklet targets youth seeking to gain a better understanding of Digital Currency technologies and non-specialists in the economic and financial sector

TABLE OF CONTENTS

1. Introduction

The mankind has sought to find ways to exchange goods and services in safe and effective ways. This has resulted in the continuous development of payment methods in several ways, including creating rare and uniquely manufactured tools that are difficult to imitate, whether using precious metals, coins, or paper afterward. Later, banking accounts, checks, electronic cards have emerged until Digital Currency were developed in an entirely virtual form. Thanks to advancements in computing and the massive development of software, databases, processors, and other equipment, that made mining Digital Currency possible .

Those currencies that aren't issued by central banks or backed by them were developed by taking advantage of the progress of Distributed Ledger Technology, allowing protecting their ownership, and transferring them from one person to another. Not only that but also providing methods to ensure their independence so that there is no party or central authority entrusted with the task of issuing or controlling these currencies (at least theoretically). This aspect may be viewed negatively, but on the other hand, it has clear advantages that were made possible by using modern technologies for the first time in history in mining currencies since the beginning of the minting of traditional official currencies.

Countries are now accelerating the adoption of Central Banks Digital Currencies (CBDCs) -which is a digital currency issued by the central banks- as legal tenders, encouraging more individuals and institutions to use them and thus more countries to adopt them as per the principle so-called snowball.

2. Goals and Scope

2.1 Goals

This booklet aims to provide a reference for the most important Digital Currency technologies as well as their expected development in the coming periods to facilitate acquiring technical knowledge in this field and targets technical and non-technical individuals interested in this field.

It comes in line with the Arab Monetary Fund's initiative to spread awareness on economic and financial sector in the Arab region, including Digital Currency, which is of great importance at the current stage, whether for ordinary individuals or even professionals.

The booklet sheds light on Digital Currency Technologies and the possible risks that may arise from the change of any of these technologies, the emerging of a new one at the expense of others, or even the possibility of their extinction.

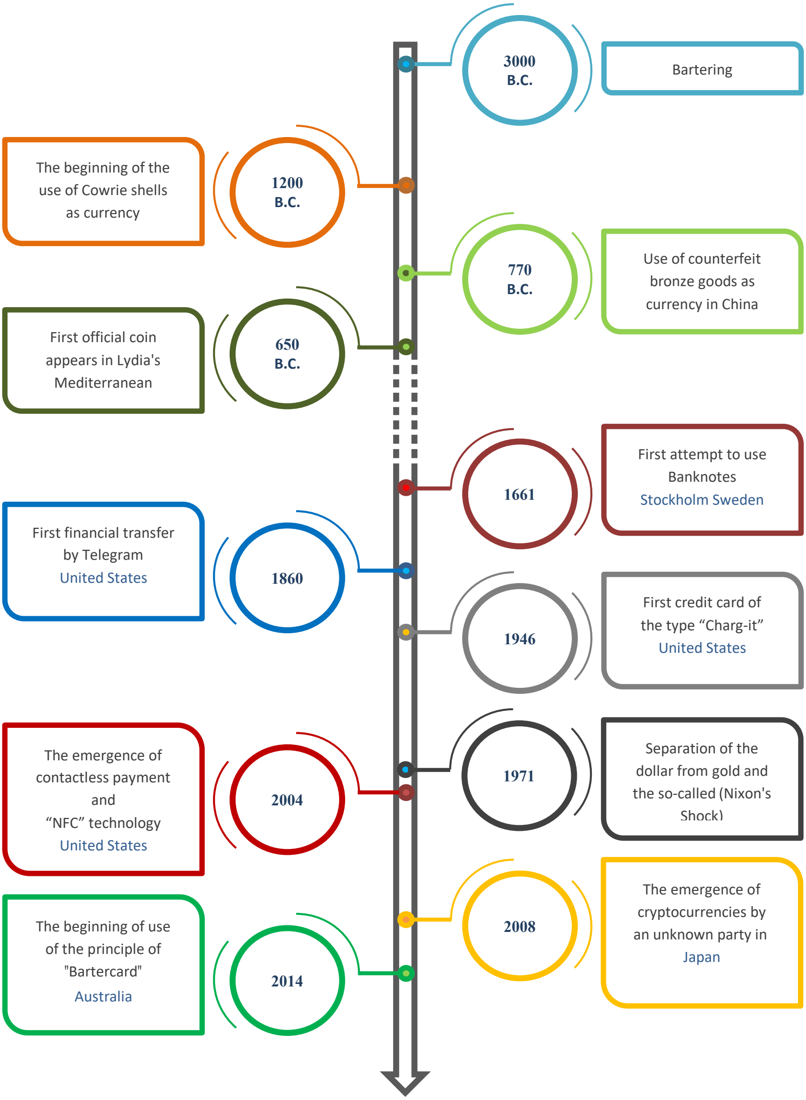
2.2 Scope

This reference includes all technical aspects related to Digital Currency and their modern technical systems available to date, excluding any other type of payment systems.

3. Timeline of development of payment methods

Human began using some means to exchange products and benefits such as salt, seeds, etc., long ago. Figure (1) highlights a brief history of the development of payment methods in general and the appearance of the need for such tools to facilitate the exchanging and trading of goods since thousands of years, until the emergence of Digital Currencies which have no printed or material equivalent, thanks to computer technology and in particular distributed ledger technology.

Figure (1): Timeline of the payment methods development



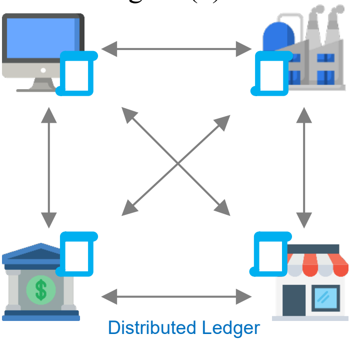
3000 B.C.
Bartering
1200 B.C.
The beginning of the use of Cowrie shells as currency
770 B.C.
Use of counterfeit bronze goods as currency in China
650 B.C.
First official coin appears in Lydia's Mediterranean
1661
First attempt to use Banknotes
Stockholm Sweden
1860
First financial transfer by Telegram
United States
1946
First credit card of the type "Charg-it"
United States
1971
Separation of the dollar from gold and the so-called (Nixon's Shock)
2004
The emergence of contactless payment and "NFC" technology
United States
2008
The emergence of cryptocurrencies by an unknown party in
Japan
2014
The beginning of use of the principle of "Bartercard"
Australia

Source: The Author of the booklet based on sources no. 6, 7, 8 and, 12 mentioned in the references.

4. Distributed Ledger Technology (DLT)

It is the infrastructure consisting of hardware and software that allow simultaneous access to the data. Unlike the traditional database, validating and updating records on the distributed ledgers technology works on a computer network spread over multiple entities or locations.

Figure (2)

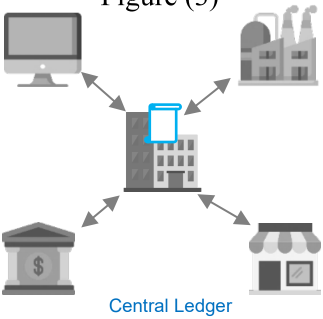


Source: The Author of the booklet based on sources

Encryption is used in distributed ledger technology to store data securely, which uses signatures and encryption keys to allow access to authorized users only.

The technology also creates an immutable database, which means that once information is stored, it cannot be deleted, and any updates are permanently recorded while preserving the original. Unlike traditional databases, DLT does not have a central place to store

Figure (3)



Source: The Author of the booklet based on sources data, as the name indicates, making it more secure, transparent, and trusting between the parties using it compared to traditional databases.

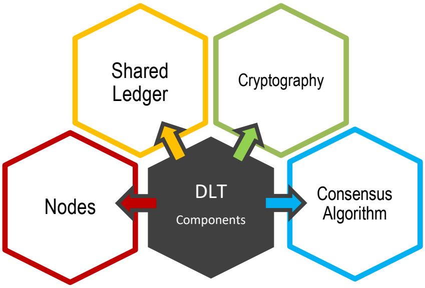
4.1. Source of DLT

The emergence of distributed ledger technology is related to the development of peer-to-peer networks (P2P) used for databases in general. The concerned parties communicate without a central authority to coordinate between them, making distributed ledger technology possible through this type of network. While, consensus algorithms are used to coordinate the so-called nodes to compensate for the need for the central authority used in traditional databases.

4.2. Components of DLT

Distributed ledger technology consists of four essential elements that enable it to achieve its goals for which it has been developed and are common to most types of this technology, as detailed in this booklet.

Figure (4)



Source: The Author of the booklet based on sources

4.2.1. Cryptography

Cryptography refers to the process of transforming ordinary data into incomprehensible data and vice versa. It is a way to store and transfer data in a unique form to only be read and processed by the destination receiver.

Encryption was once an accurate synonym for coding, but at present it depends mainly on math and programming sciences.

Modern cryptography is based on confidentiality. No party can understand the information contained except the person to whom it is sent, and the information and responsibility cannot be changed, meaning that the sender cannot deny his intentions to transmit the information at a later stage. Through encryption, it is also possible to authenticate the operations where the sender and receiver can confirm the information contained. It is noteworthy that encryption is used in many banking, computer passwords, and e-commerce transactions. There are three types of encryption techniques in general as follows:

4.2.1.1. Symmetric key Cryptography

Both sender and receiver in this technology share the same key, and the sender key is used for the encryption of the original data and send it to the receiver, on the other end, the receiver applies the same key for the decryption of the data in the message and restore the original data.

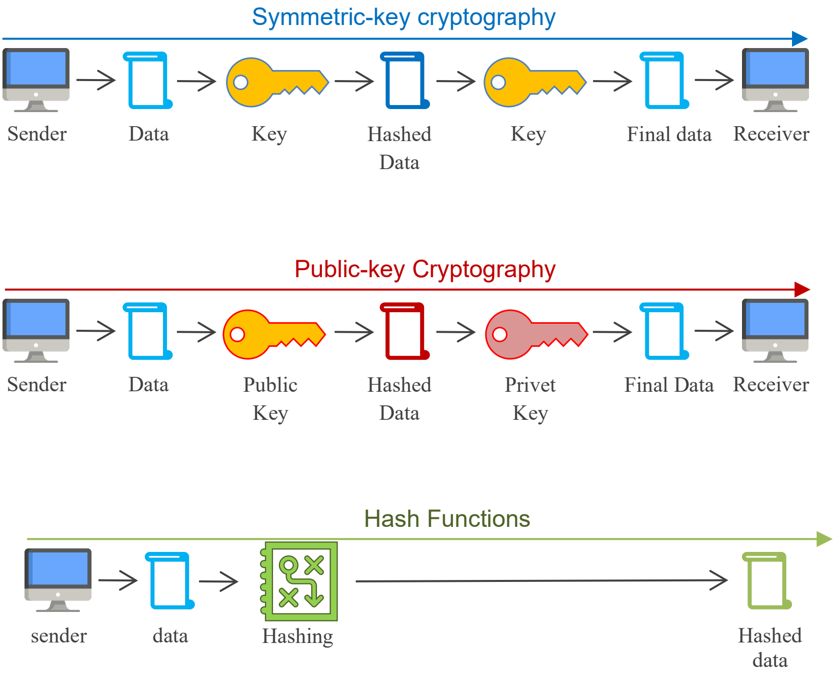
4.2.1.2. Public key Cryptography

Unlike the previous technology, this cryptography of the asymmetric type uses two keys, The public key, and the private key; the two keys are connected to give the value of a resulting fixed-length fragmentation based on the original data to be encrypted. That is what makes it almost impossible to retrieve the original data's contents without knowing the connection of the given values. The Public key is shared publicly as indicating the name, while the private key remains unknown to the public. To encrypt the data, the public key should be used while the private key should decrypt.

4.2.1.3. Hash Functions

This concept is the most revolutionary in the field of cryptography; it is a mathematical function in the form of algorithms that converts random length data into a fixed-length encoded output, so regardless of the original amount of data or file size, the output will always have the same size. Moreover, it is not possible to go in the opposite direction using the raw data from the encrypted one since the Hash functions are one-way.

Figure (5): Types of Cryptography



Source: The Author of the booklet based on sources 1 and 5 mentioned in the references.

Following is a list of the most important Hash functions used in Digital Currency and other areas:

Table (1): Most used Hashing Algorithms

- A5A v2
- Aergo
- Allium
- Argon2
- Argon2d
- Argon2i
- Balloon Hashing
- BCD
- BLAKE-256
- BLAKE2b
- BLAKE2s
- BTHash
- C11
- CryptoHello
- CryptoNight
- CryptoNight
- CryptoNightFast
- CryptoNightHeavy
- CryptoNightLite
- CryptoNightLiteV1
- CryptoNightV7
- Cunninghamchains
- DaggerHashimoto
- Dcrypt
- DEDAL
- ZHash
- Equihash 192 7
- Equihash 200 9
- Equihash 210 9
- Ethash
- Exosis
- Fresh
- Grøstl 512
- HEX
- HMQ1725
- Keccak
- LBK3
- LBRY
- Lyra2RE
- Lyra2REv2
- Lyra2REv3
- Lyra2vc0ban
- Lyra2Z
- Lyra2z330
- Lyra2Zoin
- MD5
- MTP
- Multi algorithm
- NeoScrypt
- Nist5
- Pascal RandomHash
- pGap
- PHI1612
- PHI2
- Polytimos
- Prime Constellation
- Prime Six
- ProgPoW
- Quark
- Qubit
- Scrypt
- Scrypt^2
- Scrypt ChaCha
- Scrypt N
- SHA 224
- SHA 256
- SHA 256d
- SHA 256T
- Shabal 256
- Skein
- Skein SHA2
- SkunkHash
- SoftCrypton
- SonoA
- Tensority
- TimeTravel
- TimeTravel 10
- Tribus
- UBQhash
- VerusHash
- X11
- X11 Binarium
- X11 Evo
- X11 Spread
- X13
- X14
- X15
- X16R
- X16S
- X21S
- Xevan
- Yescrypt
- YescryptR16
- YescryptR32
- YesPoWer

Source: The Author of the booklet based on sources 1 and 5 mentioned in the references.

4.2.2. Nodes

A node is any system or device connected to a network, such as a file server, computers, printers, etc. The number of nodes will be the total number of devices and systems connected to the network. Each device/system in the network has a specific address, such as the MAC address, which helps track the source and destination of the data in the network.

There’s also another level of defining a node, where a folder or a file inside a storage component in a system or in a device called a Leaf.

4.2.3. Shared Ledger

Also called distributed records, it is a database shared concurrently and consensually across multiple sites, organizations, or geographic regions. Various parties can access it, and transfers are allowed to have public witnesses. The participant in each node in the network can access the data shared across those. The network can have a mirror copy of it, and any changes or additions made are reflected in the records and replicated to all participants' devices within seconds or minutes.

4.2.4. Consensus Algorithm

It is defined as a decision-making method that any group can use; the consensus algorithm aims to make the totality of the members of the concerned group support the decision of the majority, and that works best for the rest of them. It’s a form of a decision where members must accept the majority's decision, whether they like it or not.

The following example would clarify the consensus algorithm. If we have a group of 10 people who have to decide in their favor, they all can share their ideas that they think individually beneficial for the group. However, the group will adopt the majority's decision, which is most likely the most beneficial for the group, and the rest of the group will have to accept the decision.

Table (2): Consensus Algorithms

- Proof of Work
- Proof of Stake
- Casper
- Delegated Byzantine Fault Tolerance
- Delegated Proof of Stake
- Practical Byzantine Fault Tolerance
- Proof of Importance
- Stellar Consensus Protocol
- Proof of Burn
- Proof Of Service
- Proof of Weight
- Open Representative Voting

- Proof of Activity
- Simplified Byzantine Fault Tolerance
- Proof of Elapsed Time
- Proof of Previous Transactions
- Proof of Capacity
- Leased Proof-Of-Stake

Source: The Author of the booklet based on sources 11 and 16 mentioned in the references.

Following are brief definitions of the most used Consensus Algorithms:

4.2.4.1. Proof of Work (PoW)

It is one of the first consensus algorithms used in Digital Currency development to prevent malicious uses in computing systems. Later in 2004, "Hal Finney" has adopted it to secure Digital Currency transactions by using the SHA256 hashing algorithm, hence developing the idea of (Reusable PoW).

After its introduction in 2009, Bitcoin became the first widely adopted application of the idea of "PoW," which formed the basis for the development of many other cryptocurrency obtained through mining.

4.2.4.2.The Proof of Stake (PoS)

Unlike the PoW based on how much mining you do, PoS Concept refers to your ability to mine or validate transactions based on how many coins you hold.

4.2.4.3. Casper:

It is a new consensus algorithm that combines both the proof of stake algorithm and the proof of work, developed by the famous cryptocurrency "Ethereum", which represents a revolution in the world of cryptocurrencies, and a new technology with which the Ethereum currency competes with other currencies in terms of volume and transfer fees.

4.2.4.4. Delegated Proof of Stake (DPoS)

This consensus algorithm has been developed to secure the network by representing the transactions; it is designed to implement democracy-based rules benefiting from the technology, using voting to protect the network from centralization and wrong usage.

4.2.4.5. Leased proof of stake (LPoS)

This consensus algorithm is a version of a proof of stake mechanism used in the Waves platform that allows stakeholders to lease their shares to full nodes and earn a percentage of the fees as a reward.

4.2.4.6. Proof of elapsed time (PoET)

A consensus mechanism algorithm is often used on authorized blockchain networks to determine the rights to miners or block winners on the network; each node in a network of decentralized records generates a random waiting time in which it goes to sleep.

4.2.4.7. Practical Byzantine Fault Tolerance (pBFT)

This Consensus algorithm was Introduced in the late nineties and was designed to work more efficiently in asynchronous networks to have low overhead time.

4.2.4.8. Simplified Byzantine Fault Tolerance (SBFT)

In this consensus algorithm, a minimum of (2f+1) of nodes must accept the block, (F) is the number of nodes with faults detected by the algorithm, in such a minimum system, a number of nodes must accept the new block in the network. For example, if the faulty nodes are five, a minimum of 11 nodes must accept any block.

4.2.4.9. Delegated Byzantine Fault Tolerant (dBFT)

A fault-tolerant Byzantine consensus mechanism allows for broad participation in the consensus through proxy voting; the NEO token holder can choose the bookkeeper who supports it through voting.

4.2.4.10. Proof of activity (PoA)

This mechanism Combines the Proof of Work component with Proof of Stake, where mining begins traditionally with miners competing to be the first to solve a puzzle and claim their reward. The difference is that the mined blocks do not contain transactions.

4.2.4.11. Delegated Proof of Importance (DPoI)

It is a consensus algorithm that integrates the concepts of DPoS with the idea of social interactions that naturally generate economic activity between individuals or organizations.

4.2.4.12. Proof of Space (PoSpace)

This consensus works by allocating nontrivial disk space to solve a challenge presented by the service provider, and it is also called proof of capacity (PoC).

4.2.4.13. Proof of Burn (PoB)

This method ‘burns’ coins by sending them to an irretrievable address. Instead of using expensive storage equipment and a random selection, miners can earn a lifetime privilege to mining on the system.

4.2.4.14. Proof of Weight (PoWeight)

While the probability of discovering the next block in PoS is represented by the percentage of tokens gained in the network, in a PoWeight system, some other relatively weight is used.

4.2.4.15. Open Representative Voting (ORV)

This consensus allows every member to delegate a representative to vote on his behave, even if he is offline.

4.2.4.16. Stellar Consensus Protocol (SCP)

The Stellar Consensus Protocol provides a means to reach consensus without relying on a closed system for accurately recording financial transactions.

4.2.4.17. Proof of Service

The master nodes control the registration and revocation of certificates using a custom Proof of Service consensus algorithm that ensures that these nodes can agree on which entries should be appended to the blocks.

4.2.4.18. Proof of previous transaction (PoPT)

It is used for JC Ledger and is based on the so-called Joint Cloud and can improve the reliability and convenience of cloud resource exchanges by enabling collaboration between multiple clouds. The biggest challenge to implementing JC Ledger is the Consensus concept. Current consensus algorithms for public blockchains such as Proof of Work or Proof of Stake do not apply to the shared cloud, as they require immense computing power.

4.3. Types of Ledgers used in DLT

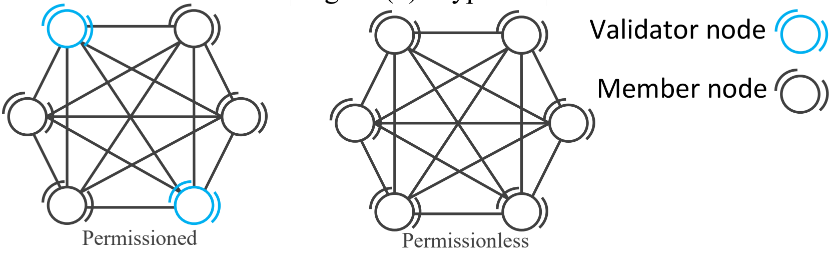
4.3.1. Permissioned

It is also called “Private” as it requires a unique security system for DLT. It maintains an access control layer to allow specific actions to be implemented only by some identifiable participants.

4.3.2. Permissionless

It is also called “Public”, or an open network open to all to participate in the consensus algorithm process used by DLT to validate transactions and data. It is completely decentralized across unknown parties.

Figure (6): Types of



Source: Jürgen, B. and Udo, M. (2016). “Towards a framework for the evaluation and design of distributed ledger technologies in banking and payments”, Goethe, March.

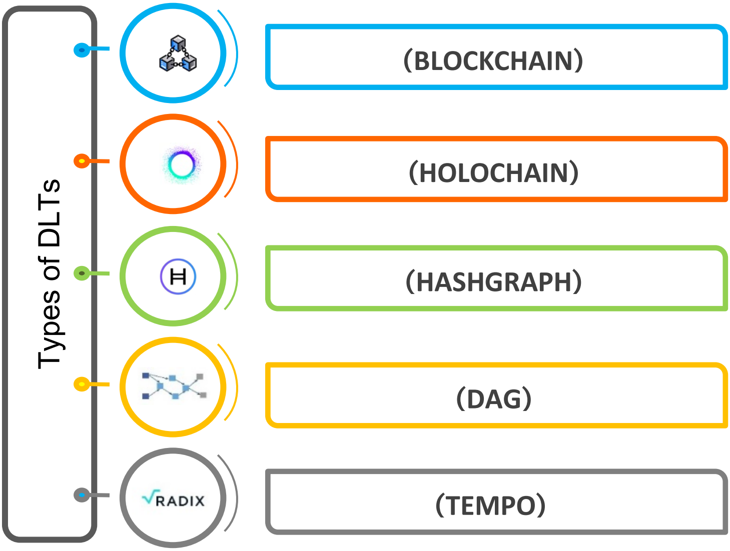
4.3.3. Hybrid

It is a combination of public and private ledgers in which DLTs are used but hosted in a private network, meaning that the private DLTs control restricted participation.

4.4. Applications and types of DLT

Distributed ledger technology consists of many technologies that share the same principle of decentralization of data. Still, they are different, and some are developed from each other, as explained in detail in this section.

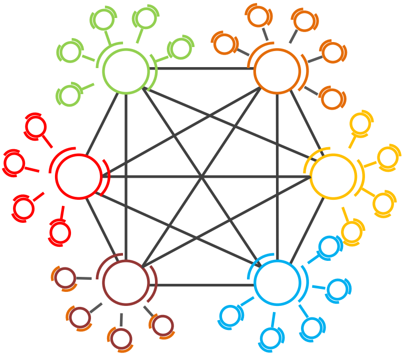
Figure (7): Types of DLTs



Source: The Author of the booklet based on sources 2, 10, 14 and 15 referred to in the references.

4.4.1. Blockchain

Figure (8)



Source: The Author of the booklet based on sources

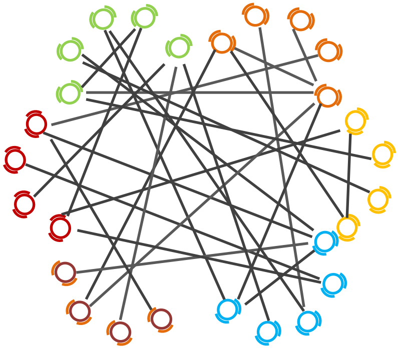
It is one of the types of distributed ledger technology and a new generation of databases in which data is decentralized; blockchain combines information in groups (Blocks) that have specific storage capabilities and, when filled, are connected by chains in prepackaged mass to form a series of data known as blockchains, which are collected in a larger node, The new information that follows that newly added block in a new block that will also be added to the current series once filled.

The types of blockchain differ according to the different records used in them, as detailed in point 3.4 in this reference, in addition to the consortium type, which is the most common. The consensual work is done by a pre-defined group and is of the first permissioned type.

4.4.2. Holochain

This technology provides a framework for communication and transmission applications to add data, including banking assets, to blockchains, where chains are collected for integration, division, and interaction. This information is stored in a decentralized manner, with data-related encryption associated with numerical biometrics.

Figure (9)

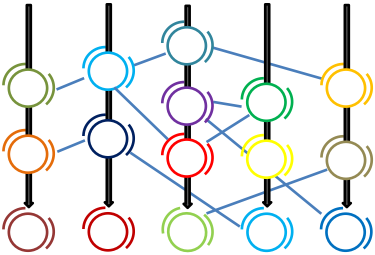


Source: The Author of the booklet based on sources

If someone interferes with data, technology observes the difference between data and encryption, and the data that has been changed is rejected. At the same time, digital signatures ensure that the ownership information of Holochains is not encrypted but will act as a decentralized file system.

4.4.3. Hashgraph

Figure (10)



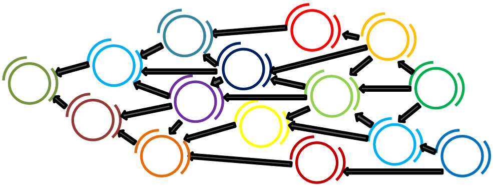
Source: The Author of the booklet based on sources

A distributed ledger technology offers technical advantages to overcome some blockchain defects such as low-speed barriers. This DLT is not only competing with blockchains but goes beyond it to compete with some well-known service providers .

Created by Leemon Baird, co-founder of Swirlds, the important advantage of encryption statement technology is that it does not need to validate transactions. Instead of clusters such as blockchains, transactions are timed using targeted non-periodic charts.

4.4.4. Directed Acyclic Graph (DAG)

Figure (11)



Source: The Author of the booklet based on sources

It is a different type of data structure assuming itself as a database linking different pieces of information, consisting of areas and lines connecting it to its orientation in the same direction, which is periodic as its name indicates, i.e., you cannot return to the starting point if you start and follow the statement at a given moment.

The periodic statement directed is a graphical data structure in a topological order that extends the sequence only before a distance, often using this technique to process and schedule data and find the best way to problem-solve and is used for applications requiring thousands of transactions per second and scalability.

4.4.5. Tambo

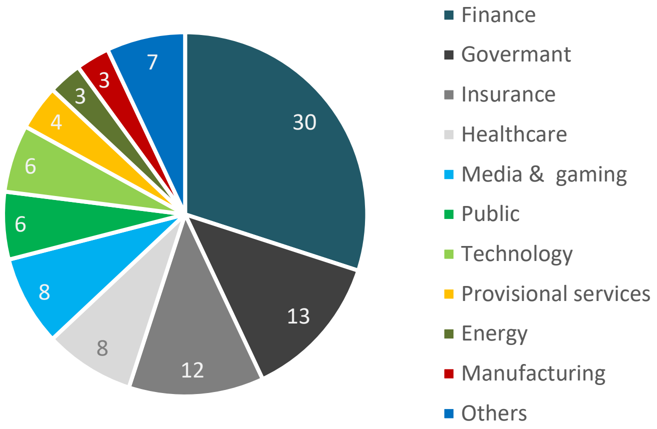
The DLT named "Tambo," also called Radix, is specifically designed to support Radix cryptocurrency and make it a low volatility asset, hence, enabling traders, other companies, individual users, and developers to use this cryptocurrency with relatively small price fluctuations.

One of the advantages of this technology is that it does not need expensive computers, mining equipment, or significant capital to participate in running the node, participate in its consensus algorithm, and process its transactions.

4.5. Fields using DLT

Distributed Ledger Technology is used in several areas, Digital Currency may be on top, but it is not the only one. The technology is also used in the real estate sector, media, supply management, fraud detection, transportation, health, and energy, figure (12). It is expected that the use of the technologies mentioned in this booklet or any types that may be developed in the future will expand to include many other sectors and fields, or even new areas due to its numerous advantages.

Figure (12): Fields using DLT (%)



Source: Mandelbrod, M. (2012). "Layered Hashing Algorithm for Real-time Systems", Feb.

5. Smart Contracts

While Distributed Ledger Technologies were primarily seen as a support technology for cryptocurrencies, they have evolved much further to include Smart contracts. In this context, smart contracts are among the most important techniques mentioned in this book, especially the Distributed ledger technology with its contents of Encryption, Records, Nodes, and Algorithms. Smart contracts are self-executing contracts in which the terms of the agreement between the buyer and seller are written directly in the lines of software (code). Agreements contained therein are in a network of decentralized records as indicated by its name and explained in this booklet, where code controls the implementation and transactions are traceable and irreversible.

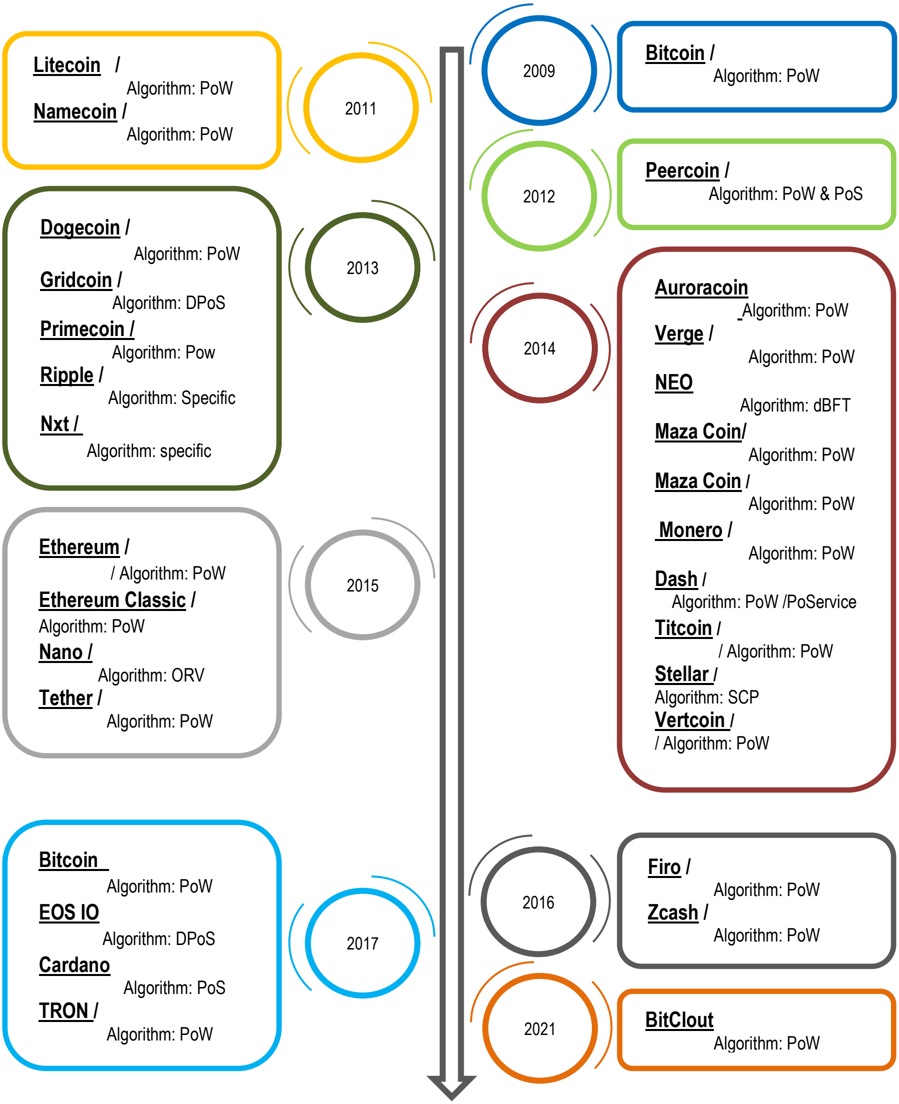
Smart contracts allow for the execution of trusted transactions and agreements between disparate and anonymous parties without the need for a central authority, legal system, or external enforcement mechanism.

6. Cryptocurrencies

It is completely virtual currency and is not represented by any physical mean, and is secured by cryptography, making fraud or double spending almost impossible. Cryptocurrencies operate on decentralized networks based on Distributed ledger technology (as detailed in this booklet). A distinctive feature of cryptocurrencies is that they are often not issued by any central authority, which in theory makes them immune of being controlled by any central authority.

Except for the famous cryptocurrency “Bitcoin,” the rest of the currencies are called “Altcoins”, and there is also a third category of cryptocurrencies, which is Stablecoins, where their value is linked to another, more stable cryptocurrency, or to other assets. Or commodities that are traded on the stock exchange, such as precious metals. The most important of which are explained in the following figure, in order of their emergence year.

Figure (13): Timeline of Some Cryptocurrencies



Source: Josias N. (2021). "Blockchain & Cryptocurrency Regulation", Global Legal Group, Feb.

7. Conclusion

All countries are now clearly heading towards digital transformation. With the tremendous development in the field of electronic banking and payment systems, there is no doubt that the field of cash and currencies is also heading in the same direction. We already barely use banknotes and coins nowadays, as most invoices and purchases payments are made by cards of all type or by entering their data into a computer or mobile phone.

Despite the risks of inflation where currency issuers have had limits in their mint and value determination, despite the current determination of the level of currencies but Digital Currency will be an ideal solution to the lack of liquidity faced by some governments and also the huge demand that's coming.

Proponents of Digital Currency confirm their positive role in reducing the risks of inflation and restricting the absolute authority of central banks around the world in issuing currencies that may sometimes not be in line with developments in the real economy which creates inflationary pressures. Some of these currencies, most notably Bitcoin, have a predefined level of money supply, allowing the currency's value to be maintained over time and even increase.

Also, cryptocurrencies of the type “Stablecoins” may be a compromise that official authorities may find suitable for adoption to cope with the development of modern payment technologies and the need for central banks to restrict the use of cash, especially in the wake of the Covid-19 pandemic.

It has also become clear that several governments are heading towards issuing central bank digital currencies as a legal tender which will be allowed to be widely traded and accepted approved in court rulings. Each government or economic alliance may issue its cryptocurrency with the significant number of Digital Currency is expected to be issued.

Furthermore, with the advancement of DLT, which is adopted widely in much more areas than Digital Currency as previously mentioned, focus and attention should be placed on catching up with the world in taking advantage of the opportunities they offer on the one hand, and mitigating the risks that may result from them on the other hand.

8. References:

1/ Al-odat, z. , ali, m., abbas, A. & khan, s. (2020), “Secure Hash Algorithms and the Corresponding FPGA Optimization techniques”, ACM Computing Surveys , Sep.

2/ Bott, J. & Milkau, U., (2016), “Towards a framework for the evaluation and design of distributed ledger technologies in banking and payments”, Journal of payments strategy & systems, Nov.

3/ Fu, X., Wang H., Shi P,. (2021),"Proof of Previous Transactions (PoPT): An Efficient Approach to Consensus for JCLedger”, IEEE Transactions on Systems, Man, and Cybernetics Systems, Apr.

4/ Garrick, H. and Michel, R. (2017), “GLOBAL BLOCKCHAIN BENCHMARKING STUDY”, Golf Australia , Feb

5/ Gennaro, R., Gertner, Y., Katz, J. and Trevisan, L. (2005). “Bounds on the Efficiency of Generic Cryptographic Constructions”, SIAM Journal on Computing, Feb.

6/ Glyn, D. (2003), “ History of Money”, Economic Affairs. Dec

7/ Jamie, R. (2017),"Satoshi Nakamoto's Brilliant White Paper Turns 9-Years Old”, Bitcoin.com, Oct.

8/ Jenks, J. (1966) “Chapters on the History of money”, Financial Analysts Journal, Sep.

9/ Josias N. (2021). “BLOCKCHAIN & CRYPTOCURRENCY REGULATION”, Global Legal Group, Feb.

10/ Kauflin, J. (2019), “Hedera Hashgraph Thinks It Can One-Up Bitcoin And Ethereum With Faster Transactions”, Forbes.com , March.

11/ Laphou, L., Zecheng, A., Songlin h., Songtao g., yuanyuan y. and bin x, (2020). “Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling”. The Hong Kong Polytechnic University, Feb.

12/ Liuliang, Y. and Hong, Y. (2004), "Chinese Coins: Money in History and Society.”, Long River Press, Nov

13/ Mandelbrod, M. (2012), “ Layered Hashing Algorithm for Real-time Systems.” Theory of Computing Systems. Feb

14/ Maull, R., Godsiff, P., Mulligan, C., Brown, A., and Kewell, B. (2017). “Distributed ledger technology: Applications and implications”, Strategic Change , Sep.

15/ Md Arafatur, R., Balamurugan, B., Neeraj, K. and Gayathri N. (2020) “Blockchain, Big Data and Machine Learning: Trends and Applications edited”, Feb.

16/ Rui, Z., Rui X. & Ling L. (2019), ”Security and Privacy on Blockchain.” ACM Computing Surveys, Jan.

17/ Sakai, K. Qiong, H. Zongyang, Z. (2017) “identity-based non-interactive key exchange revisited and more and Yu Chen”, International Journal of Information Security, Feb.

18/ Shermin, V. (2019), ”Token Economy How Blockchains and Smart Contracts Revolutionize the Economy”, Shermin Voshmgir; Edition ed, Jun.

19/ Team of ARFWG, (2020), “Financial Technology Glossary”, Arab Regional Fintech Working Group, Nov.

20/ Timoney, M, (2002), “Bartering Set to Enhance the Credit Function”, Credit Control, Dec.

For obtaining Arab Monetary Fund publications

Please contact:

Arab Monetary Fund

Knowledge Network

P.B. 2818

Abu Dhabi - United Arab Emirates

Phone Number: (+9712) 6215000

Fax Number: (+9712) 6326454

E-mail: Publications@amfad.org.ae

Available electronically on the Fund's website through the following link:

https://www.amf.org.ae