Cryptocurrencies: From Bitcoin to the Algorand Protocol and the Peer-to-Peer Basics 🖥️🔛🖥️

Before we deepen our discussion around the Algorand Protocol, we need to understand how Bitcoin came about, which brought this use of cryptography to the field of finance and the monetary system. It is also important to understand what the notorious blockchain is, which in the Portuguese language means "cadeia de blocos" and let us understand here some key words to better understand the context of our conversation. Here are some of them

Point-to-point: A computer network architecture where each point or node of the network works both as a client and as a server, allowing the sharing of services and data without the need for a central server.

Wikipedia generic definition

Decentralization: It is an administrative system that seeks to transfer certain powers and competencies, characteristic of central power and concentrated in one location, to other smaller, peripheral or local sectors.

Concept in the online dictionary (dicio.com)

You can see below two different types of networks, the first is server-based and the second is a peer-to-peer network scheme.

Centralized Server Based Network

Decentralized Peer to Peer Network

Let's take it slowly, we are just understanding some concepts to better develop a line of reasoning. When we go to the original Bitcoin concept we come across a peer-to-peer network and then we come to one of the fundamental pillars of the Bitcoin protocol, which is also not disassociated from the Algorand Protocol which is the main subject of this publication. And why didn't they disassociate themselves? Simply because they both refer to the decentralized aspect due to the fact that they come from point-to-point networks and not based on a central server. From then on we can go further and say all these terms that we are dealing with relate instructively to blockchain, since through the ideas of Satoshi Nakamoto (creator and founder of Bitcoin) and his contemporaries, all the innovation contained in blockchain came to the surface, being this the main technological innovation that emerged there that we will see more closely ahead. The idea of creating a system without a central authority and with the possibility of transferring anything without an intermediary, with an authentic validation and without the possibility of duplication or fraud can be considered something very useful and interesting, but no doubt that the possibilities arising from immutability is the apex of his work. As we enter this philosophy we realize that decentralization is much more than an idea, much less a simple community formed by individuals who want to make a system without intermediaries, protect their interests, or something similar, but this has its genesis in a philosophy of life, and let's say an ideology that can be linked to sociological aspects beyond the algorithms and computing contained in it.

After all, what is Blockchain?

Blockchain, in a direct Portuguese translation to "cadeia de blocos", is a very adequate name for a concept of technology that is on the rise; it is the use of a shared register system that has a list of transactions chronologically ordered and that is validated by the logic of the computers involved in this network. This term emerged from the meeting of the universe of technology with that of finance and has been gaining more and more attention from people in a short space of time. Because it is something new and a little complex, which involves finance, it must be demystified so that there is no doubt about what it is.

Briefly we can consider it as a public ledger (similar to the accounting one) that makes the register of each transaction there divulged of whatever it is (for example the popular Bitcoin), and this register ends up being something reliable and immutable. This procedure registers the information of the amount, who sent it, who received it, when the transaction was made and in which place of

the book it was registered. This makes it transparent, being a strong point of blockchain technology.

How the information is stored

Thus, the information of a group of transactions is stored in blocks, marking each block with a time and date record and each time period a new transaction block is formed, which is linked to the previous block. Each group contains a file and a hash, which guarantees that the information of this data block has not been violated.

How does the network work?

The blocks, which are dependent on each other, form a chain of blocks, making it perfect for recording information that requires trust. The network itself is formed by other computational elements that verify and register the transactions in the block, through a certain computational power at first. There are different consensus mechanisms, but let's take Bitcoin as an example, where in the PoW (Proof of Work) mechanism, there is an incentive to continue collaborating to make the network sustainable and more secure, thus receiving a reward in the form of a fraction of digital currencies.

How is the transaction validated?

The miner can only add a transaction to the block if a simple majority (50%+1) of the network agrees that that transaction is legitimate and correct. The name of this is called consensus. In the case of Bitcoin, consensus is measured through computational power.

Two block strings can be formed at the same time, the deadlock will be resolved when the network needs to choose one of the strings. In the end, the chain with the greatest amount of work wins.

In short, blockchain technology is a public and distributed accounting book that records all virtual currency transactions in a block chain, which anyone can participate in. The information recorded in it is reliable, immutable and transparent as long as most of the network remains honest.

If someone tries to change some information in one of the blocks, automatically, the block hash will be changed. This means that the modified hash will not be compatible with the copy of the original that will be in the next block, so it is easy to identify changes attempts.

Why is blockchain such a popular term nowadays?

In addition to being a technology that allows the creation of revolutionary products, such as cryptocurrencies that are digital currencies that have no ballast in any country, for example, blockchain can also be used for validating documents - such as contracts and stock exchange - financial transactions, marketing music or movies, tracking shipments and even votes.

But despite the buzz, there is still a mistrust on the part of the population. According to Trust Barometer, which measures trust in certain institutions and technologies, only 55% of respondents trusted blockchain.

More and more businesses are appropriating this technology, but we need to wait for the next chapters of this subject to see what the real impact of blockchain in the world we live in, in finance, in public governance, in society in general.

Main Elements

Distributed ledger technology: All network participants have access to the distributed ledger and its unchanging record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort typical of traditional business networks.

Unchangeable records: No participant can change or corrupt a transaction after its registration in the shared ledger. If a transaction record includes an error, a new transaction must be included to reverse that error and both transactions will be visible.

Smart contracts: To speed up transactions, a set of rules, called an intelligent contract, is stored in the blockchain and executed automatically. As an example, an intelligent contract can define conditions for corporate insurance-guarantee transfers, include terms for travel insurance payment, and more.

Types of Blockchain

Unauthorized public: Anyone can participate in the blockchain's consensus mechanism. In addition, anyone with an internet connection is able to perform transactions and view the entire transaction log.

Public allowed: Anyone with an internet connection is able to perform transactions and view the transaction log, but only a restricted part of the nodes can participate in the consensus mechanism.

Private allowed: The ability to perform transactions and view the log in this blockchain is restricted only to nodes participating in the network. The owner of the blockchain is who defines the users of the network and which nodes can participate in the consensus mechanism.

Unauthorized private: There are restrictions on performing transactions and viewing the log, but the consensus mechanism is open to any node.

Other Considerations

The web 3.0, maintained by Blockchain can offer a truly decentralized internet, provide anonymity and guarantee privacy to users. Companies will stop using centralized servers for data storage. Through this technology companies can, for example, authenticate their users by their keys without storing personal data of the clients. In web 3.0 the data trafficked is encrypted and the decision to share the information with platforms or third parties becomes the user's. The use of Blockchain in web 3.0 also provides a lower propensity of service interruption for running in a distributed environment, being an excellent alternative for applications that generate great negative impacts due to service interruption.

One of the biggest problems of Blockchain is the lack of standardization in its use, which generates enormous challenges and even difficulties for people and companies. Another factor is the need to depend on a general collaboration to implement it in some company. For that, it is necessary to involve employees, information technology, operators and other institutions to improve usability.

Blockchain Use Cases

Besides having emerged to revolutionize financial transactions, the data unit operated by Blockchain is not necessarily currency related. There are already different business models spread around the world studying and testing the application of this technology in blocks. Get to know some of the possibilities of application of Blockchain that may transform our day to day life:

- Notary services, contracts and registrations;
- Copyrights and intellectual property;
- Contracts in games, streaming services;
- Shared economies;

- Supply chain;
- Visual Identities;
- Intelligent devices and internet of things;
- Simpler financial services;
- Blockchain as a service (BaaS);
- Elections and more secure democratic public governance.

Algorand Protocol

After being immersed even superficially in the origins of Bitcoin and its original technology, which is the blockchain, we will now immerse ourselves in the Algorand Protocol, which is the main objective of this publication, since such technology offers a complete range of solutions among those mentioned above that refer to the application of the block chain. Now that you understand better what the blockchain is and what it's for, it's easier to understand what Algorand proposes, what its differences and potentialities are in relation to Bitcoin and other similar technologies and how this can impact the future background in what concerns data and information processing, something that is considered very valuable in a general way in the current globalized times and also in what concerns finances. When we enter the economic field we can understand that such technology has impacted even the financial environment by opening possibilities for more agile, accessible and facilitated borderless economies.

Algorand removes the technical barriers that for years have undermined the adoption of a far-reaching blockchain:

- decentralization;

- scale;

- security.

With Algorand it is possible to build a stable platform, through its consensus mechanism without the need for permission and Proof of Stake (Pure PoS). This allows full participation, protection and speed within a truly decentralized network. With blocks completed in seconds, Algorand's transaction speed is on par with large financial payment networks such as Visa and Mastercard. With this Algorand is the first blockchain to provide the purpose of immediate transaction, without bifurcations and without uncertainties, because there is no possibility of a fork. The era of bordersless economy and decentralized is increasingly closer now with Algorand Protocol. Algorand is there and it is an open tool for anyone, being able to create intelligent contracts and many other possibilities that we have already mentioned in our article through its tools for developers. Now it's up to you, make good use of this range of possibilities!

Decentralization
The Algorand blockchain is entirely decentralized, without a powerful central authority or any control point. An exclusive user committee is randomly and secretly selected to approve each block, so that the nodes (nodes) are executed by entities representing different fields, coming from different countries. In this way we can consider it:

- Fair and transparent, because the control is distributed among all the individual participants of the network;

- It needs, because there is no risk of the data being manipulated, lost or destroyed;

- Secure, fault tolerant without exposing any special group of users to attacks.

No permission required
Public and Open to All

Users do not need approval from a trusted authority to use the Algorand blockchain. There is a single class of users and no closed gates. Every participant

can read each block and have their opportunity to write a transaction in a future block.

Low Cost to Participate

The Algorand platform requires minimal processing power and modest IT resources to function. All online users who have Algos are automatically eligible to participate in block consensus.

Pure Proof of Participation

Algorand uses a pure proof of participation (PPoS) consensus protocol built on a Byzantine agreement. This means that the system can achieve consensus without a central authority and tolerates malignant users as long as the immense majority of participation is not in the hands of such users. The influence of users in choosing new blocks is proportional to their participation in the system (number of Algos). Users are selected secretly and randomly to propose blocks and also to vote on block proposals. All online users have the chance to be chosen to propose or vote. The probability of a user being chosen will be directly proportional to his participation.

Rewards

At Algorand, power is in the hands of users with participation. Each user receives an amount of rewards proportional to their participation for each block committed to the chain. We do this to encourage users to join the Algorand platform and accelerate our journey towards decentralization. In this way, if you have Algos in your wallet automatically you receive rewards for proof of participation, or also called stake. Click on the image below to access the Algos reward calculator and see how many Algos you can earn as a kind of "savings".

Algorand Staking Rewards Calculator

https://algoexplorer.io/rewards-calculator

Open Source

Algorand's node repository is open source and publicly available for anyone to audit, use and build upon. The platform is founded on the principles of transparency, inclusivity and collaboration, and maintained by a community dedicated to the vision of a decentralized and borderless future.

Evolution of the Protocol

Algorand is established on the idea that the system should allow changes and avoid inflexible policies, thus enabling both the community and the protocol to evolve. The Algorand platform employs the consensus method for protocol changes, which facilitates the continuous evolution of the protocol and eliminates bifurcations that can fracture the community. This capability is driven by Algorand's consensus protocol that allows users to reach consensus on anything. Not only about the next block, but also about the protocol evolutions.

- Proposed changes are posted to the blockchain;
- The community uses the Algorand consensus protocol to vote and accept or reject an amendment;
- By accepting, the community agrees with the block where the changes were made;
- All pass to the new protocol at the same time.

Founder

Silvio Micali is part of MIT faculty, Electrical Engineering and Computer Science Department, since 1983. Silvio Micali's interests in research are cryptography, zero knowledge, pseudorandomic generation, secure protocols and design of locking mechanisms and chains. In particular, Silvio is the co-inventor of probabilistic encryption, Zero-Knowledge Proofs, Verifiable Random Functions and many of the protocols that are the foundations of modern cryptography.

In 2017 Silvio founded Algorand, a fully decentralized, secure and scalable blockchain that provides a common platform for building products and services

for a borderless economy. At Algorand, Silvio oversees all research, including theory, security and cryptographic financing.

Silvio is the winner of the Turing Award (in informatics), the Gödel Award (in theoretical informatics) and the RSA Award (in cryptography). He is a member of the National Academy of Sciences, the National Academy of Engineering, the American Academy of Arts and Sciences and the Accademia dei Lincei.

Silvio received his Laurea in Mathematics from the University of Rome, and his Ph.D. in Computer Science from the University of California at Berkeley.

Use Cases

Fondazione Ugo Bordoni: Using Algorand to Experiment with 5G Spectrum Allocation, AI, Networks and Digital Services;

IBMR.io: Southeast Asia Microfinance and Token Platform at Algorand 2.0;

SIAE: Open and Efficient Solutions for Blockchain Copyright Management;

Blockchain.com: Multifase Integration Including Support for Algorand Standard Future and Active Portfolio;

Stonize: Providing Faster and Safer Settlement and Discharge Processes and Delivering Decentralized, Scalable and Secure Digital Security Services to Clients;

World Chess: Plans for Hybrid Public Offering at Algorand's Blockchain and the London Stock Exchange;

DUST Identity: Ensuring Digital Integrity, Physical Security and Visibility End to End for Supply Chains;

Reach: Enabling Developers to Build Decentralized Applications at Algorand ;

Parsiq: Providing Businesses with Better Monitoring and Analysis of their Own Ecosystem;

AssetBlock: Tokenizing Real Estate Assets on Algorand's Platform;

Securitize: Using Digital Securities to Issue, Transact and Perform Corporate Actions;

IDEX: Helping Next Generation Decentralized Exchanges at Algorand;

Bleumi: Helping Companies to Build on Algorand's Platform;

PureStake: Providing Safe and Reliable Infrastructure to Developers and APIs at Algorand;

Flipside Crypto: Enabling Analytical Data for Decentralized Applications at Algorand;

Syncsort: Helping Data Driven Companies Leverage Decades of Technology Investment;

OTOY: Democratizing Computing, Distributing Power.