otichain

#whitepaper

Otichain is a **decentralized blockchain project** built on Bitcoin's UTXO[1] model, with support for smart contracts, based on the Ethereum Virtual Machine[2] and guaranteed by a **Proof of Stake consensus model**.

www.otichain.com

01.01 Framework
Introduction

The concept of 'cryptocurrency' as a method of exchanging wealth without the need for a supervisor started with Bitcoin in 2008. At its introduction, Bitcoin was simply a white paper with a new idea. But the idea caught on and grew from a fledgling idea into a truly global phenomenon, giving rise to a financial, social, and cultural revolution.
Blockchain technology is the basis for most cryptocurrencies.
A blockchain is a growing public database/registry that uses cryptography to secure blocks together in a growing chain of blocks in which the information stored is impossible to alter or delete.

What gives blockchain technology its appeal can be refined into four main factors:

1. Transparency - Everyone has access to the distributed register with all transactions.
2. Trustless - A trust factor is distributed among the different nodes of the network through an economic game of incentives that require nodes to follow a set of protocols to authenticate new blocks of data on the blockchain.
3. Decentralized - The blockchain is not based on a single point of authority but rather on a network of nodes that must reach a consensus.
4. Immutable: once data is confirmed in the blockchain, that data must be authenticated by multiple nodes to confirm any future data.

The Otichain blockchain is an open source decentralized distributed-ledger capable of recording transactions between two parties in an efficient, verifiable, and permanent manner.

Otichain supports Bitcoin's UTXO model and Ethereum's EVM. Resulting a blockchain that is secure, flexible, fast, and low cost.

It is constantly being tested and improved by promoting the solution to companies, government agencies, entrepreneurs, and private individuals.

01.02 Framework

Goals to be achieved with otichain blockchain

I. **Authentication** of original goods

II. **NFT** as Certificates of authenticity of a digital artwork

III. **Digital Twin**

IV. Cost-effective cryptocurrency transactions for **mass adoption**

V. Improvement of customer **loyalty programs**

VI. Improving **inventory management**, inventory finance and **supply chain monitoring**

VII. **Massive, cost-effective cryptocurrency transactions**

VIII. Management, **security and sharing of customer data**.

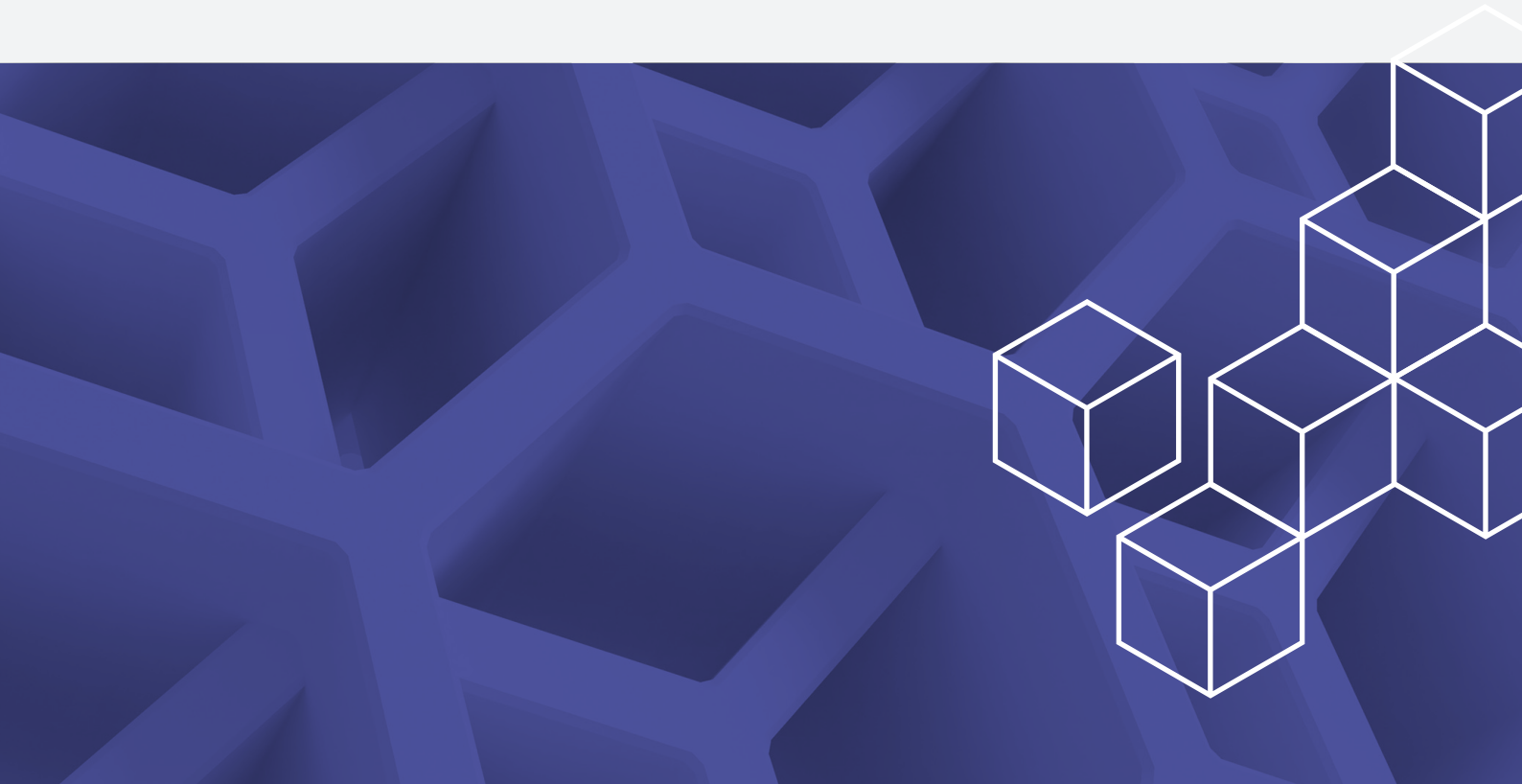
01.02 Framework

Authentication of Original goods

Transparency is the key element of blockchain technology. It enables peer-to-peer transactions, whereby even the smallest change is recorded within the blocks. Anyone can view the transactions that have taken place on the blockchain and therefore there is no possibility of fraud or creating fakes. In addition to this, the customer can verify the authenticity of the product and its history, such as the date of production and other information that could influence their purchase decision.

In this way, it will not be possible to buy counterfeit and fake items and the manufacturer will be able certify the origin of the product and track and trace every single raw component.

The technology also enables real-time and precise take-down of possible counterfeits for probatory evidence in view to successfully claim the copyrights and the industrial property rights and act in proper legal courts.



01.02 Framework

Goals to be achieved with otichain blockchain

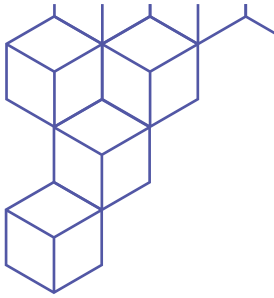
NFT as Certificates of authenticity of a digital work

NFT as Certificates of authenticity of a digital work
NFT stands for Not Fungible Token, where 'Not Fungible' means unique and irreplaceable. For example, a bitcoin is fungible: if we exchange one bitcoin for another, we will have exactly the same thing. However, a work of art certified with an NFT is not fungible. If we exchange it with another one, we will have something completely different. Most NFTs are part of the Ethereum blockchain. In this system purchases are made through cryptocurrencies.

A non-fungible token (NFT) is a unit of data stored on a digital ledger, called a blockchain, that certifies a digital asset to be unique and therefore not interchangeable.[1] NFTs can be used to represent items such as photos, videos, audio and other types of digital files. Access to any copy of the original file, however, is not restricted to the buyer of the NFT. While copies of these digital items are available for anyone to obtain, NFTs are tracked on blockchains to provide the owner with a proof of ownership that is separate from copyright.

Digital TWIN

A digital twin or "Digital DNA" is a virtual replica of physical resources, potential and effective (physical twin) equivalent to objects, processes, people, places, infrastructures, systems, and devices.
They are used for various purposes, particularly in production, logistics and predictive maintenance.
Therefore, with respect to the Italian Industry 4.0 paradigm, this kind of approach is the state of the art.



Improvement of customer loyalty programs

Customer loyalty plans are a market worth almost $2 billion, a figure that could triple by 2023, growing at least 20% more each year. 74% of Italians are enrolled in a loyalty plan with at least one retailer offering this type of initiative (EU and World average 66%). 44% are members of between 2 and 5 loyalty, one consumer in six (17%) is enrolled in more than six loyalty program.
The data emerges from Nielsen's Global Survey "Retailer Loyalty: Card-carrying consumer perspectives on retail loyalty-program participation and perks" based on a sample of more than 30,000 individuals in 63 countries.
Consumers face the challenge of monitoring the numerous loyalty program they are registered to and many of the loyalty points created each year are not used, thus leading to balance sheet liabilities. A blockchain application would help users easily redeem points across different merchants and platforms (e.g. Android, iOS and web) while minimizing operational costs, decreasing the possibility of fraud and improving customer satisfaction.

Improving inventory management and supply chain monitoring

With the increasing complexity of SKU (Stock Keeping Unit) management and shorter product life cycles, sales forecasting has become more difficult for apparel manufacturers. Their retailers and supply chain partners can implement blockchain technology that can provide a single source of information and use smart contracts to enable the automated execution of various tasks for product management and supply. Better visibility into the supply chain would increase operational efficiency and enable more accurate forecasting, preventing over-ordering and minimizing sales losses due to out-of-stocks.
Blockchain more efficiently replaces all traditional technologies for organizations and corporates that want to certify and monitor their supply chain.
Market research says that blockchain can reach a critical level of adoption and even gain consumer acceptance by 2025. Furthermore, with so much research and statistics in favor of blockchain, early adopters of the technology can distinguish themselves in their product sector.
Otichain is an all-inclusive, standardized environment that allows developers to focus their efforts on blockchain solutions. This will promote the creation of DApps and smart contracts open to all.
The blockchain offers enormous potential to reshape privacy and security and, ideally, transform the global economy.

02.01 Framework

Massive, cost-effective cryptocurrency transactions

Ethereum is metered on 2020 to about 12 transactions per second, while bitcoin has an average of 7 transactions per second. Otichain aims to solve the problem of scalability and energy efficiency that the two main blockchains currently suffer from. The consensus mechanisms, the protocol adopted and the sustainable impact aim to exceed 20,000 transactions per second and the energy consumption of each node to be just a few watts.

Otichain - Blockchain network

Bitcoin is a cryptocurrency and a worldwide payment system created in 2009 by an anonymous inventor known by the pseudonym Satoshi Nakamoto, who developed an idea he himself presented on the Internet in late 2008.

It uses a database distributed among network nodes that keep track of transactions (blockchain) and exploits cryptography to manage functional aspects, such as the generation of new money and the attribution of ownership of bitcoins.

The Bitcoin network enables the pseudo-anonymous possession and transfer of coins; the data needed to use one's bitcoins can be stored on one or more personal computers or electronic devices such as smartphones, in the form of a digital wallet, or kept with third parties that perform bank-like functions. The bitcoin wallet has an address identified by an alphanumeric code that has between 25 and 36 characters between numbers and letters; it is the only data to be communicated to receive a payment that will enjoy a certain degree of anonymity, but will at the same time be publicly and immutably visible on the blockchain forever. In any case, bitcoins can be transferred through the Internet to anyone with a bitcoin address. The peer-to-peer structure of the Bitcoin network and the lack of a central entity makes it impossible for any authority, governmental or otherwise, to block transfers, seize bitcoins without possession of their keys, or devalue them due to the introduction of new currency.

Otichain - Blockchain network

Similarly, Ethereum has enabled the creation of decentralized applications and their use in the blockchain, giving developers access to an open platform for the development of applications, smart contracts and much more.

From the Ethereum white paper:

"What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code."

With this vision, Ethereum has been the driving force in many aspects of blockchain development and the cryptocurrency industry. It offers the potential for a world where most systems could take advantage of blockchain technology and the functionality that comes with it. Whether it is the tokenization of assets or the ability to manage ICO fundraisers, it has enabled users to create a new Internet, the likes of which we could barely have imagined a few years ago.

02.02 Ecosystem

Proof of Work (PoW) vs Proof of Stake (PoS)

To verify and validate a transaction or block, Bitcoin, Ethereum and many other blockchain platforms use the Proof of Work (PoW) consensus model. In a PoW consensus system, the creator of a new block is determined by some mathematical algorithm. The biggest problem with PoW is that it requires a lot of computing and electrical power.
Proof of Stake (PoS) is a newer consensus model that determines the creators of new blocks based on the stakes, which is the amount of coins "locked" in participating wallets in order to provide security for the network. It reduces energy consumption compared to PoW and rewards staking wallets with minted coins in exchange for network protection.

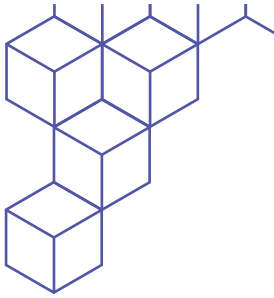
02.02 Consensus algorithm

Proof of Work(PoW)

Proof of Work (POW) is an algorithm that rewards the first person or group of people [pool] to solve a computational problem to achieve a distributed consensus.

While Nakamoto has improved on Adam Back's Hashcash work, he has created a validation system that relies on cryptographic hashing rather than the trust of a centralized system.

The Bitcoin network creates and distributes in a completely random manner a certain amount of coins approximately six times per hour to clients that actively participate in the network, i.e. that contribute their computing power to the management and security of the network. The activity of generating bitcoins is often referred to as mining, a term analogous to gold mining. The probability that a certain user will receive the reward in coins depends on the computational power he adds to the network relative to the total computational power of the network.



Initially, the client itself took care of the calculations required to mine bitcoins, using only the CPU. As the total computing power of the network increased and due to the competitive nature of bitcoin generation, this functionality became uneconomical and was removed. Today, there are specialized programs that initially exploited the power of GPUs and FPGAs, and now use dedicated hardware based on ASIC processors designed for this use. Since the average number of operations needed to successfully close a single block has become so large that it requires large amounts of resources in terms of electrical power and computational power, most miners join together in 'guilds' called mining pools where all participants pool their resources and then divide up the blocks generated according to their contribution.

02.02 Consensus algorithm

Proof of Stake (Pos)

Proof of stake (PoS) is a type of algorithm with which a cryptocurrency blockchain network aims to reach a distributed consensus. In PoS-based cryptocurrencies, the creator of the next block is chosen through various combinations of random selection and wealth or age (i.e. stakes).

The proof of participation must have a way to define the next valid block in any blockchain. Selection based on account balance would result in (undesirable) centralization, as the single richest member would have a permanent advantage.

Other projects use Delegated Proof of Stake or DPoS. The system uses a limited number of nodes to propose and validate blocks to the blockchain. This is intended to keep transaction processing fast, rather than using several hundred or several thousand nodes. For example, EOS uses a limited number of block validators, 21, whose reputation may or may not decline, allowing backup validators to replace previous nodes.

Incentives differ between the two block-generation systems. With PoW, miners could potentially not own any of the currencies they are mining and thus only seek to maximise their profits. It is unclear whether this disparity reduces or increases security risks. With PoS, however, those who 'locks' the coins always own the coins, although several cryptocurrencies allow stakes to be held on behalf of other nodes.

PoS has a significantly lower energy consumption than PoW.

otichain

Otichain is a **decentralized blockchain project** built on Bitcoin's UTXO[1] model, with support for smart contracts, based on the Ethereum Virtual Machine[2] and guaranteed by a **Proof of Stake consensus model.**

[1] A UTXO is an unspent transaction output. In an accepted transaction in a valid blockchain payment system (such as Bitcoin), only unspent outputs can be used as inputs to a transaction. When a transaction takes place, inputs are deleted and outputs are created as new UTXOs that may then be consumed in future transactions.
Each UTXO has a signature associated with it belonging to the owner. In Bitcoin, this signature must be present during a given transaction in order for the transaction to be considered valid.

[2] The Ethereum virtual machine is one of the key pieces in the functioning of the Ethereum blockchain. Its function is to allow the execution of smart programs or contracts in order to implement a series of additional features on said blockchain so that users can enjoy it.

Prototype

Prototype & Platform

Otichain is the evolution of Quantum, a project based on Bitcoin Core (the most secure blockchain currently in existence) where the EVM (Ethereum Virtual Machine) has been implemented for the creation/execution of fungible and non-fungible Smart Contracts and Tokens.

Compared to Quantum, we differ in the Proof of Stake algorithm, which has been replaced with the Blackcoin code and thoroughly modified.

In this way, the blockchain has become more democratic and no longer based on the "weight" of the wallet in stake.

In traditional PoS, nodes receive a fixed reward based on the amount of coins staked. The more coins there are on the staked node, the more blocks are gained and consequently (in absolute value), the more coins are gained. Although in relative value all participants will receive the same percentage of "locked" coins, in absolute value it means that the more coins held, the more blocks gained and the greater the consensus power. Theoretically, if a node had more than 51% of all circulating coins, it could change the blockchain.

In Otichain, on the other hand, the reward mechanism is distributed equally to all staked wallets (nodes), in proportion to the value of coins 'locked'. In this way, in each creation cycle, the node receives a block and a fraction of coins equal to what it has staked.

Business Values

0,00001 USD Average Network Transaction Fee
10.000+ transaction per second

Sustainability

Low Energy Consumption
Unlimited Staking possibilities

Otichain's consensus protocol is found to have a much-improved attack prevention of 51%, making it impossible to modify the blockchain even if you have all the coins in circulation.

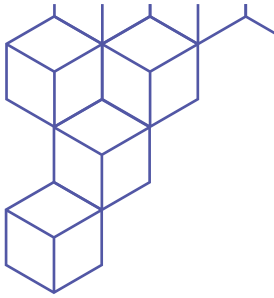
The limitation of this consensus is given by the number of nodes, which in order to have a fast-enough maturation of the reward, needs a not high number.

The formula is: generated block * number of seconds * number of nodes = accumulation time of new coins

The second difference with Quantum is the value of the network fee (gas) for smart contract transactions and executions. This value was deliberately set at an infinitesimal value, in order to allow its use by large corporate, organization, and institutions where the number of transactions is extremely high, but the cost of the same must be as low as possible although in a super secure environment.

These fees, instead of being allocated to the block holder, are allocated to a 'foundation address' which collects them for the maintenance of the network.

The Stake mechanism is the only incentive tool for nodes, so the production of stake coins will be continuous and not finite in number, in order to endlessly incentivize the consensus mechanism.



Smart platform

The virtual machine for smart contracts - EVM

As a UTXO-based smart contract platform, Otichain uses the same remote procedure calls (RPCs) as Bitcoin. Having chosen this framework and further selected a PoS consensus model for its ability to facilitate a decentralized app creation platform, the traceability and consistency of blockchain transactions is guaranteed.

Ethereum, on the other hand, uses an account-based system (like a mail address) in which account status and balances are managed in these objects called 'accounts'.

Ethereum's blockchain uses stack-based virtual machines called EVMs. These 256-bit EVMs execute smart contracts recorded in the Solidity language.

Since the Otichain platform is based on the UTXO model, an interface is needed to translate the UTXO model into an account-based model. The EVM integration interface allows smart contracts developed on Ethereum to work on Otichain without requiring any changes to them. This allows developers and users to work easily with the Bitcoin and Ethereum protocols.

This makes OTI a hybrid cryptocurrency that can be used in a wide range of sectors worldwide.

The OTI gas model

OTI has imported the gas model from Ethereum. In the gas concept, each executed transaction has a price. When a transaction occurs, more than enough gas is spent and the remaining gas is refunded to the sender at his OTI address. When a smart contract is created, the gas limit and price are determined in OTI. All or part of the gas is reimbursed.

The main features of the Otichain network include:

Compatibility with the Ethereum virtual machine, enabling compatibility with most existing Solidity-based smart contracts. No special compiler is required to deploy a smart contract on Otichain.

A Proof of Stake consensus system optimized for Otichain's consensus model. Any user can help protect the network. No authority, master node or minimum amount is required.

The Decentralized Governance Protocol is fully implemented and functional, allowing certain network parameters to be changed without forks or other network disruptions. This currently controls parameters such as block size, gas prices, etc.

It uses the UTXO transaction model and is compatible with Bitcoin, allowing existing tools and workflows to be used with Otichain. This enables the use of the SPV protocol, ideal for lightweight wallets on mobile phones and IoT devices.

Otichain's consensus algorithm guarantees the use of low-energy nodes and simultaneously a high number of transactions per second.

The structure of network fees and gas required for the operation of smart contracts has been developed to be fully Enterprise-ready, ensuring a cost of operation and maintenance close to 0 (zero).

Oticore has been developed to be user-friendly in anticipation it will also be released in a specially designed plug and play hardware version.

Management, security and sharing of customer data.

Inclusion of certificates over the different stages of the chain.
A blockchain-based smart contract is a self-executing code on a blockchain that automatically implements the terms of an agreement between parties Blockchain-based smart contracts could offer a number of benefits, such as fast, dynamic and real-time updates, low cost of operation, high accuracy and fewer intermediaries. Rights holders publish ownership information on the blockchain, consequently use policies for registered works are written into smart contract that automatically transfer usage rights. The association of public and private key permits to royalties and fees to be delivered instantly, transparently, and automatically based on the stakeholder information contained in the blockchain database, thus permitting i.e., to an open platform to facilitate infinite potential roles, application, and business models.

Legal Disclaimer

The information in this white paper is purely descriptive and not binding. Please note that this document includes forward-looking statements, statements of intent, discussion of plans, estimates or other information that could be considered forward-looking. While these forward- looking statements represent our judgment and expectations about what the future holds, they are not an offer or solicitation to purchase any product, good or service.

All statements are subject to risks and uncertainties that could cause the actual results of Otichain's development to differ. No information in this white paper has been reviewed or approved by any regulatory authority.

In addition, we intend to use the Otichain blockchain as our open source development platform, contributing these technologies under permissive licenses for the benefit of human society, not focusing merely on the profit of anyone affiliated with the project. Therefore, do not place undue reliance, especially in any financial decision, on these forward-looking statements, which are subject to change.

aim ™ RAIN ALLIANCE 1trueid®

otichain

www.otichain.com