



UNIRIS

Be the master of your identity

What if technology could finally simplify your daily life without jeopardizing your security?
What if you were told that you already have this technology?

The Uniris promise is to provide access to all technologies with a simple touch of a finger while protecting your identity. The Uniris team has developed an ultra-secure and tamper-proof technology that is as secure as the chip of a bank card. It allows you to replace any password, key, or other authentication devices by simply reading inside your fingers.

To operate on a global human scale without control or the intervention of any person, company, or organization, this "open source" technology is based on a new generation network called "Blockchain". To reach a large scale and mass adoption, we have improved the Blockchain technology so that it can replace any application or service: open your car or your door, identify yourself or pay online without risk to your data or goods, always have your medical record accessible yet protected ... This technology just works from the very first use regardless of where you are.

To function and reward people who host a network server (miner) that verifies any transaction on the Uniris blockchain, a Blockchain is built around a cryptocurrency (UCO in the case of Uniris). This currency is created at the start of the project to finance all developments, thus making each investor a real contributor in the construction of this New World from its inception.

Join us as an investor, developer, ambassador and become an active builder of the future of global connections.

Table of Content

Page 2 Project Overview

Page 3 Competitive Landscape

Page 4 More than Paris Olympics 2024, an almost Unlimited Market

Page 5 The UCO cryptocurrency programmed to grow

Page 6 Token distribution, Funds Allocation and Mining

Page 7 Roadmap

Page 8 Team

Technical Appendix

Page 9 Technical Overview

Page 10 A Blockchain for Global use

Page 11 Smart-contracts designed to improve any application or service

Page 12 Decentralized Identity and Biometrics

Page 13 Governance

Page 14 Patents to open source community

Page 15 UCO Transfer Overview



Uniris blockchain offers the first integrated services platform capable of meeting a fundamental need: **giving everyone back the control over technology**. In this way, Uniris is part of the promise of a safer, more inclusive, and truly decentralized world.

4 years of research and 12 strong international patents endow Uniris with the technological attributes that its predecessors have lacked - scalability, speed, reliability and simplicity of native biometric recognition. These patents will be given to the open source community to foster participation and hence accelerate the pace of innovation.

Designed for mass adoption, Uniris relies on a new form of unbreakable validation consensus (ARCH), which is ultra-secure and allows an unlimited number of transactions. Uniris embeds biometry in a native way using a method of identification that is tamper-proof and accessible to all. This technology uses the incredible complexity of the inside of the fingers, unique to each individual without the need to store any biometric data.

Our cryptocurrency, the UCO, is the backbone of the network that fuels the transactions and monetizes the contributors' investments, pays the miners, and develops the ecosystem built for the people by the people. **Our blockchain platform aims to replace and to improve all current applications with a comprehensive and open ecosystem**, allowing people to move from the trust imposed by centralized systems (Facebook, Google, Amazon, Banks...) to a decentralized system where everyone will retain control of their data, property, and privacy.

Uniris gives back to humanity control over technology, and to each individual, control over their identity.

Numbers at a Glance ...

Transaction service outperforming the market standards, closely integrated with biometrics'

Ergonomics: a single platform for all blockchain applications

Scalability: > 1 million transactions/sec

Instantaneous: < 5 sec validation time

Security: 0.0000001% risk of fraud even with 90% of malicious nodes

Sustainability: 3.6 Billion times less energy consumption than Bitcoin
0.1% average transaction costs

Yellow Paper : <https://uniris.io/UYPSt.pdf>

Blockchain & Biometry certified for access control to the Paris 2024 Summer Olympics

Born to be Viral

Smart-contracts unchained

Modifiable and able to run autonomously, able to rely on the metadata about the "state of the world" (weather, stock market, news, reports ...) or manage a vote on a global scale. The most advanced and easy-to-program smart-contracts on the market, with the complexity of identity already integrated.

The fastest, safest, and most energy-efficient Blockchain

Safer than a nuclear power plant (10^{-9}) and consuming 3.6 Billion times less energy than the Bitcoin network, open source, permission-less blockchain offering a network controlled by all.

Decentralized identity guaranteeing privacy

As neutral link between humans and machines, Uniris provides the first tamper-proof biometric authentication without any key storage while ensuring maximum interoperability (FIDO2/W3C).

Applications
Blockchain
Identity



A Reliable Cryptocurrency backed by the most Advanced Smart-Contracts

Technology with a cryptocurrency set to gain value through a programmed balance of supply and demand.



Communities and Organizations

Uniris replaces social media networks, LDAP which are prone to leaks and loss of control, with a simple address book and integrated messaging service.



End-to-End E-Commerce

Website, inventory management, reservations, payments, loyalty programs, shipping : It has never been easier to create an e-commerce platform



Smart-City

From automatic access to a hotel room or a car in the street without a key, to the metro without a ticket. Finally, it is possible to have a fluid interaction with our environment.



Programmable Fintech

From community loans with automated repayment, to automated and impartial insurance, to payments by the touch of a finger.

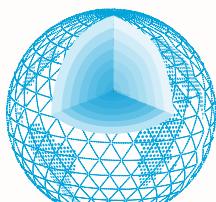


Secure Health Records

A truly secure medical record under your sole control, with the information provided by certified practitioners - no need to remember everything or be afraid of medical errors.



Competitive Landscape and Uniris Advantage



 **UNIRIS**
BLOCKCHAIN

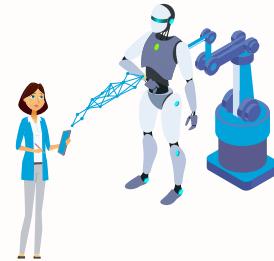
The safest, most scalable, and energy-efficient Blockchain thanks to the ARCH consensus

For the first time in history, the Blockchain represents a technology that can work without a central decision-making body. A system that is not only impartial but also transparent and inalienable. The new form of Consensus, ARCH, created by Uniris, is based on an unpredictable election of a small subset of nodes (miner) to validate and store transactions (197 per 100,000 nodes). The network uses supervised multicasting so that each node will always know where to look for data via the most efficient network path, allowing a linear increase in the number of transactions/sec according to the number of network nodes (~100x). The table below presents the main differences with the other Blockchains :

	Validation Time	txns/sec	Consumption/txn	Security	Privileges	Data Security (replication algo)	Transactions Ref.	Global	P2P Layer
Bitcoin (POW)	10 min	7	420 000 Wh/txn	51 %	no	Everywhere	UTXO	yes	Gossip
Ethereum 1 (POW)	15 sec	20	36 000 Wh/txn	51 %	no	Everywhere	Account	yes	Gossip
Ethereum 2 (POS)	15 sec	15000	360 Wh/txn	66 %	yes	Sharding by transactions groups	Account	yes	Gossip
EOS (dPOS)	0.5 sec	3996	7 Wh/txn	66 %	yes	Sharding by Blockchain	Account	Split per Blockchain	Gossip
Tezos (dBFT)	1 min	40	-	66 %	yes	Everywhere	UTXO	yes	Gossip
HashGraph (DAG)	5 sec	10	-	66 %	no	Random Sharding	UTXO	no	Gossip
Stellar (FBA)	5 sec	1000	-	Quorum	yes	Everywhere	Account	yes	Gossip
Zilliqa (POW + pBFT)	2 min	2828	-	66 %	no	Random Sharding	Account	yes	Gossip
Hyperledger (BFT / CFT / Kafka)	35 sec	20000	-	66 %	yes	Everywhere	UTXO/Account	no (private)	Gossip
Libra (BFT)	10 sec	1000	-	66 %	yes	Everywhere	Account	yes	Gossip
Harmony (POS + FBFT)	136s	10 Millions	-	66 %	yes	Random Secured Sharding	Account	yes	Gossip (UDP QUIC)
UNIRIS (ARCH)	5 sec.	Unlimited	0.0001167 Wh/txn	97.5 %	no	Geo-Secured Heuristic Sharding	UTXO	yes	Supervised Multicast

Smart-contracts: autonomous robots of the digital age

Smart-contracts are in computing what robots are in real life: they perform actions according to events. The Uniris smart-contracts take a technological leap forward. They are autonomous and can be triggered from internal events (date, transactions) or real life (the Oracle channel: verified by consensus and cross-referencing of information) such as weather, stock market, news. They adapt to their environment. Entirely modifiable, they are natively able to manage operations like stock management, payments, web hosting ... without creating any reality outside of the confirmed transactions (UTXO).



Language	Editable/updateable	Triggering auto	Oracle	Stocks & non financial tokens	Inherited constraints	Multi-Owner/Delegation
Bitcoin	Interpreted	no	external	external	no	no
Ethereum	compiled (blind validation)	restricted	external	external	special programming	special programming
EOS	compiled (blind validation)	restricted	external	external	special programming	protocol
Tezos	interpreted	no	external	external	special programming	special programming
HashGraph	compiled (blind validation)	restricted	external	external	special programming	special programming
Stellar	no code (txns & multisig)	no	external	external	native	Multi-signature only
Zilliqa	interpreted / compiled	no	external	external	special programming	special programming
Hyperledger	interpreted / compiled	native	external	external	special programming	special programming
Libra	compiled (blind validation)	no	external	external	special programming	special programming
Harmony	compiled (blind validation)	no	external	external	special programming	special programming
UNIRIS	interpreted	native	native (internal)	internal	native	native per transaction

A decentralized identity that respects our privacy

Decentralized identity avoids the need of entrusting one's identity to a third party, who might find itself in a conflict of interest and exploit our identity without our knowledge, such as Google, Facebook or our favorite merchant site. The person retains sole control of his/her identity, which is stored on a multitude of nodes ensuring its durability and integrity. This decentralized identity thus guarantees privacy and its interoperability with the rest of the applications. Coupled with the possibilities offered by smart-contracts, it becomes a central element of our interactions with the world: Access to major public events (Olympic Games, concerts, etc.), transport, hotels, messages, without ever having to reveal the details of our identity.



The end of passwords and unnecessary media

Embedded in the blockchain, the biometric technology provided by Uniris allows anyone to identify themselves without difficulty and without storing any biometric data. This is an access control that is forgery-proof and without disclosure. How does it work?

The biometric data from inside one of our fingers will generate several cryptographic keys that will never be disclosed and from which our digital identity will be encrypted. Only the person capable of regenerating one of these keys will be able to decipher their digital identity and hence prove their identity. Beyond the technological elegance of generalizing biometrics without risk to our private lives, this method makes it possible to solve the major problem of Blockchains which is mass adoption.

	Biometrics data stored	GDPR	Software vulnerabilities	Identification method	Falsifiable Biometrics	Learning morphological evolution	Identification Scale
Biometrics on Smartphone (iOS, Android ...)	Yes (local)	Local	Yes	threshold	Yes	No	100 000
Industrial/Defence Biometrics (Idemia, Fujitsu ...)	Yes (Servers)	Local	Yes	threshold	Yes	No	100 000
UNIRIS Biometrics	No	Global	No	crypto-biometrics	No	Yes	Humanity



An almost unlimited market

The river always chooses the most efficient route

The trust revolution will unleash a new generation of services

Traditional method (in silos)

Service/Apps
real Business
from 2 to 10%
per transaction



Payments
processors

Customer Identity
management,
databases, hosting,
high availability,
security, backups,
API, supply chain ...

Annual IT Costs
Between 50k & 100 Million €



Payments
processors

Customer Identity
management,
databases, hosting,
high availability,
security, backups,
API, supply chain ...

Internet (TCP/IP)



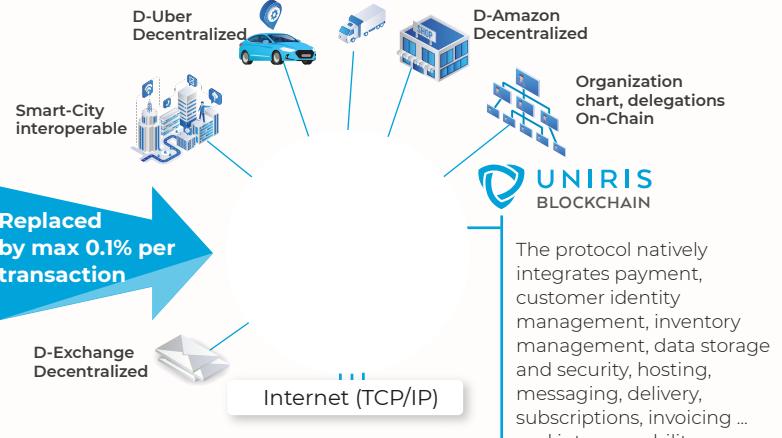
...
...

...

...

...

...



In the pre-historic model of the web (still prevalent since origin), each new service recreates its elementary operating blocks each time: portal, customer identification, customer databases, service management, hosting, storage, backups, payments. Amazon, Facebook, Google, and others do not share anything, leading to:

- An appalling consumption of computational power
- An abundance of login/passwords for users who end up copying their passwords everywhere thus giving them away
- Risks of fraud or cyberattack that can shake the planet

The Blockchain + Decentralized Identity model finally rationalizes this operating model by directly integrating all the layers necessary for the creation of new services.

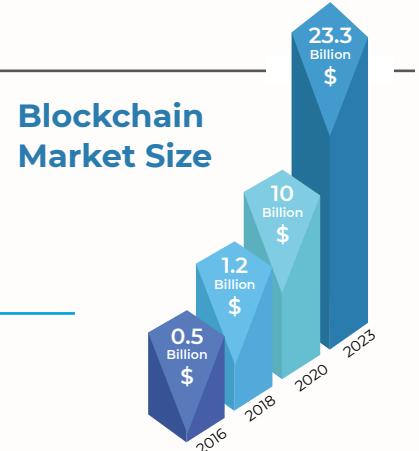
- Much less need for computer skills thanks to upstream integration
- Unique and universal identity, activated only by the holder, regardless of their physical or virtual location
- Removal of third parties in favor of the Blockchain to ensure the sustainability of the system
- Major economic and financial impact on the cost of each new service.

Market Study

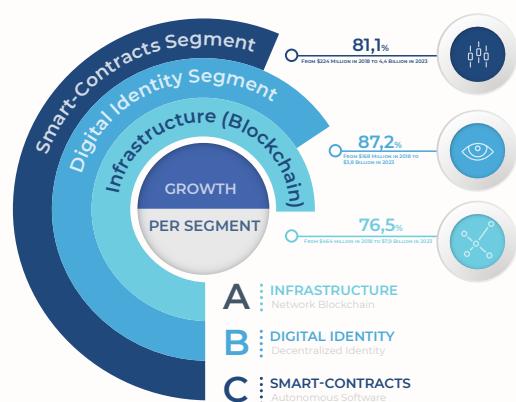
A globalized market with 80.2% growth between 2018 and 2023

The Blockchain market is conservatively estimated at 23 billion USD by 2023 compared to 1.2 billion in 2018 with an impressive annual growth rate of 80.2% between 2018 and 2023

This incremental statistic does not take into account the possible replacement of current services and application platforms, a very credible possibility.



Growth and market size by segment



The 3 market segments considered to be the most promising by 2023 are digital identity, smart-contracts, and infrastructures (Blockchain) - segments in which Uniris has the most advanced technologies.

Growth on all continents

North America

Market Share: 40.7%

Growth until 2023: 72.1%

Latin America

Market Share: 3.8%

Growth until 2023: 83.1%

Europe Russia

Market Share: 30.2%

Growth until 2023: 82.1%

Asia Pacific

Market Share: 18%

Growth until 2023: 90.3%

Africa Middle East

Market Share: 7.4%

Growth until 2023: 84.5%





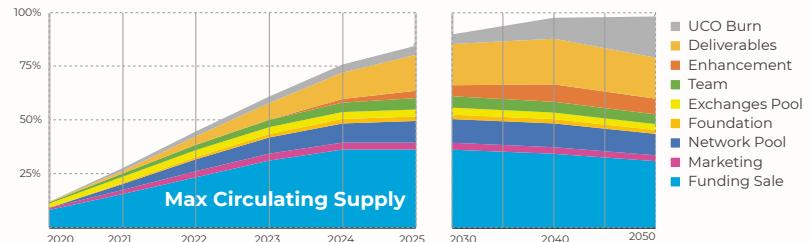
The Uniris Coin (UCO)

A cryptocurrency programmed to grow

The new economy of cryptocurrency tokens is based on the sound and universal principle of supply and demand, similar to commodities such as gold or diamonds. A cryptocurrency creates value on an open-source platform that will survive independently of the company that created it. Our foremost strategy is to create the technological conditions for "miners" who place their trust in our platform to create as much value as possible. In addition, we ensure the right balance of supply and demand.

CONTROL SUPPLY

Limit the offer: 10 billion UCOs and not one more. If someone invests in gold, while someone else discovers how to make it at a lower cost, then the price of gold will fall, because there will be more supply than demand. The Uniris Blockchain prohibits the creation of new UCOs because any transaction is based on the existence of a previous unspent transaction (UTXO)



Each new UCO on the exchange market will be associated with a new feature deployed on the network.

Limit Distribution: To avoid the effect of a massive influx of UCOs on the exchange markets that could lower the price due to a sudden increase in supply, Uniris is setting up a lock-up mechanism. With the exception of UCOs purchased during private (partly) and public sale, all other UCOs are locked and vested over a period of two to five years. During this time, the arrival of new applications on the network would lead to an increase in demand, offsetting the possible increase in supply.

Programmed deflation: The Uniris Blockchain will automatically destroy part of the UCOs resulting from transaction costs, thus creating a programmed deflation mechanism to increase the value of each UCO (the grey part of the curve).

CREATE DEMAND

The second principle is to create scarcity of the resource through demand. Beyond the biometric devices that will only be available for purchase in UCO, the challenge is to create a massive adoption of the solution (need to buy UCO to reach a real need). Our strategy is based on 3 axes (described in details in the Roadmap later):

Be the reference platform for smart-contracts production and Universal Digital Identity: Thanks to the unprecedented and long-awaited features of smart-contracts (autonomous, modifiable, integrated Oracle, scalable ...) and finally integrating a decentralized Identity usable by anyone, the Uniris platform propels the world of smart-contracts beyond the world of cryptocurrency.

Increase usage by offering the simplest and most advanced platform for service creation: Like an AppStore that allows you to multiply the number of applications and services on the network, the objective of Uniris is not to develop and deploy all the different applications, but to create an ecosystem that facilitates, finances, and supports the arrival of all these applications. The network will thus provide functionalities that are the necessary building blocks to replace the existing applications (see Roadmap).

The World at your Fingertips: The final objective of the project is to generalize biometric identification (or derivatives) on a global scale from a 100% open and transparent network that is finally trustworthy. From the opening of your house or car doors, through all the exchange mechanisms (finance...), to votes.

GROWTH HYPOTHESES OF THE UCO CRYPTOCURRENCY

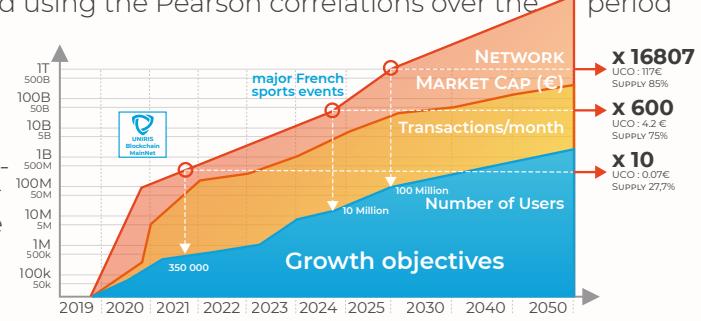
The most appropriate current method for assessing the value of a Blockchain (Market Capitalization) is based on Metcalfe's law that relates the value of the network to the number of users.

A lot of research has been done on the subject of cryptocurrency valuation using Metcalfe's Law. Different variations were used to describe the price of Bitcoin and using the Pearson correlations over the period between 2010 and 2018, it was found that the value of the network is of the order of:

$$\text{value of blockchain} \sim n^{1.5}$$

(n representing the number of users)

This law thus makes it possible to obtain an approximation of the value of a network according to the number of users. For example, considering an event such as the Olympics Event, which alone brings together 8 million people, and knowing that the maximum number of UCO exchangeable on the market over this period will be 75% (7.5 billion UCOs), we thus obtain:



$$(10 \text{ million})^{1.5} = € 31.6 \text{ billion}, \text{ i.e. a valuation per available UCO of } € 31.6 \text{ billion} / 7.5 \text{ billion UCO } \sim € 4.2/\text{UCO}$$



Distribution, Allocations and Mining

A model that emphasizes value sharing

UCO Token Model

10 Billion UCO
maximum number of UCO

0.007 €/UCO
Initial Price ICO/IEO

25.1 Million €
Market Cap

UCO
Uniris Coin : Cryptocurrency token

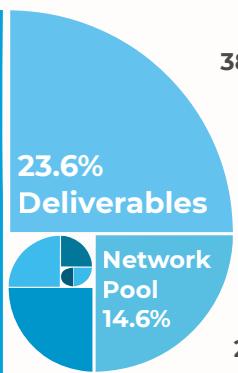
The number of UCO tokens, the initial value of the UCO, as well as the market capitalization, are initialized according to the means required for the implementation of the ecosystem according to the growth hypotheses and priorities of the project.

On the Uniris ICO (Initial Coin Offering), two actors have been privileged:

- **Early Investors:** the near-exclusivity of available tokens during the first two years will be those of the ICO.
- **The Contributors** mobilized up to the delivery of the ecosystem (10% of tokens at code delivery and 90% after the effective and functional deployment of the code).

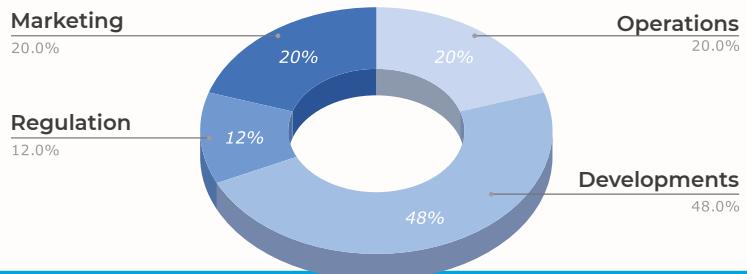
UCO Tokens Split

38.2%
UCO
Token Sale

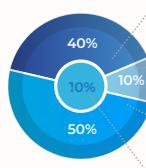


Funds Allocation

The purpose of private and public sales is to raise funds to develop the network and innovations published in the yellow paper. The diagram opposite shows the functional distribution of the funds collected.



Miners (nodes) and mining on the Uniris network



No need for boots and a construction helmet! Mining and proof of work on the Uniris network are no longer based on the computing power and electrical energy expended, but on a cryptographic verification to validate and secure the origin of a transaction (biometric devices, smartphones, hardware or software keys ...). As a direct result of the ARCH consensus, only 295 miners are needed to offer the same performance as the Bitcoin network, which has ~ 100,000 miners.



Cross-Validation Nodes

Nodes elected to verify the coordinator node calculations

Coordinator Node

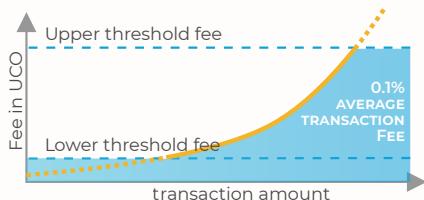
Node in charge of coordinating the validation of the transaction

Storage Nodes

Nodes from which the previous transactions have been downloaded

Network Pool

Oracle, tagging or prediction, geographical incentives, and Token Burn (destruction of part of the UCOs). The amount is levied on mining costs at the time of the recovery of the miners' funds, thus avoiding any point of contention on the validation of transactions.



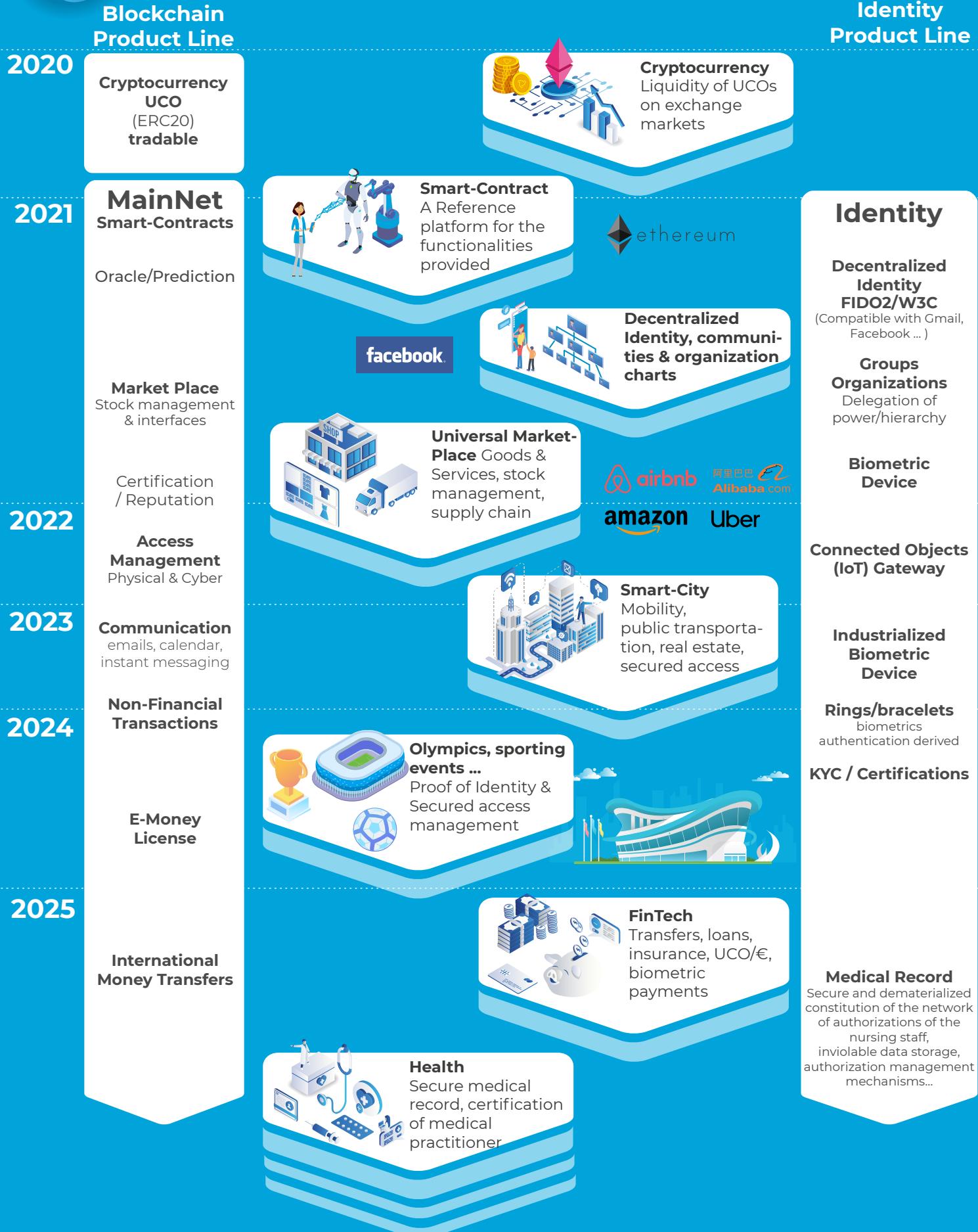
The fees are calculated according to the real costs of the network (size, complexity ...). The maximum and minimum fees are defined through the Oracle chain which is able to adjust these two limits according to the costs of electricity or the market value of the UCO cryptocurrency. Thus making it possible to perpetuate the financial model for both miners and users.

This will allow anyone to own a storage node and receive the associated remuneration, but only miners chosen by the network itself may become miners of validation. This election, transparent through a smart-contract, aims to maximize the geographic distribution of miners, but also ensures a sufficient level of income for all miners elected (thus avoiding the risk of mining farms jeopardizing the robustness of decentralized networks). The first miners will be elected as a matter of priority from among the early investors who have made it possible to finance the development of the network.

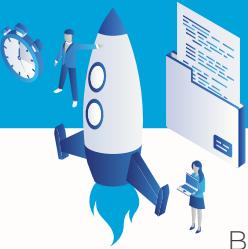


Roadmap for the future

The Uniris network, the essential building block and catalyst for the creation of a New World of Services with proven trust, interoperability, accessibility, and control by all.



The Team !



Created in 2017, after 2 years of fundamental research by Sébastien, Nilesh and Christophe, UNIRIS SAS is partially owned by the École Polytechnique (Paris Saclay), financed by BPI France and Investors of the smart-city up to one million euros. At the end of the ICO (public sale of UCO cryptocurrency) an entity will be created as an association to organize the community and by 2025, let the Public Blockchain spread its wings.

The last few months have allowed us to develop some of the modules of the Blockchain as well as a prototype of the biometric device, which has enabled us to be **certified by the Strategic Committee of the Security Industries Sector** to provide the **access control** during major French sports events until 2025.

UNIRIS SAS
Capital of 98 562,74€
RCS: 828 015 131
16 bd St Germain PARIS

Our team is a unique blend of complementary, cohesive, and experienced personalities from companies such as Thales, Mastercard, Barclays, Orange, Mozilla, Google, PwC, and researchers from the École Polytechnique, CNRS. Most of us knew each other well before the creation of the project, professionally or personally, which has allowed us to save a considerable amount of time in the implementation of each components of the solution.

Executive Team



[in Sébastien CEO & co-Founder](#)

Previously in charge of 2 of the largest Orange projects: Identity (100M users) and Mobile Banking in Africa (turnover from €10M to €4 billion) - Thales Cybersecurity Expert - Blockchain Speaker (since 2013)



[in Nilesh COO & co-Founder](#)

ex-CTO PAYBACK, Head of Software Development and Support for MasterCard Payment Processing Platforms, Head of Barclays Digital Payments Technology



[in Christophe CSO & co-Founder](#)

Ex-Special Forces - Technip
Security Manager (Niger), RGPD
safety consultant



[in Samuel Blockchain Architect](#)

Software Architect and
Ethereum Developer (Identity,
ICO ...) Michelin/Viseo/Deloitte



[in Akshay R&D Maths](#)

École Polytechnique - Researcher in Maths, Blockchain and Biometrics



[in Virginie Community Manager](#)

Head of Web Content Management and Communities for the Gueudet Group - Publishing



[in Victor CBizDevO](#)

Coordinator/BizDev Crypto-Mondays & Chain Accelerator - MIT
BlockChain Biz Innov&Apps

Advisors to technology, strategic and communication boards



Bernadette

Research Director CNRS/ École Polytechnique, Specialist in distributed systems - Grand Prize of the Academy of Sciences



[in Anne](#)

Board Director - Orange, holding Peugeot, Pernod-Ricard and Imprimerie Nationale, Executive Director Innovation Cisco, Menthis



[in Gilles](#)

Evangelist Open Source & Blockchain - Quantum Cryptography Expert (Quantum ID / Wipro)



[in Peter](#)

Mozilla's Ex-CMO, Google Building the Open Source Community



[in Camille & in Valentin](#) (Othello)



[in Baptiste](#)

Mata Capital tokenization of real estate investment transactions - Economy & Partnerships

A big thank you to all those who have accompanied us since the beginning of this adventure: the entire program team HEC Challenge+, the accelerator of the École Polytechnique X-UP, the StationF Founders Program, GICAT, CEPS, Cap Gemini, our investors without whom this would not have been possible: Stéphane, Frédéric, the BPI and all our investors from the private sale. A big thank you also to all the people, ambassadors and advisors who made it possible to refine both the technological and human dimensions of this project.

Partners

Uniris partnerships focus on innovation and community growth. Research institutes give us access to cutting-edge technologies and help validating of our innovations.



STATION F

GICAT

HEC
PARIS

bpifrance

l'ÉCOLE
POLYTECHNIQUE
UNIVERSITÉ PARIS-SACLAY

The Underlying Technological Revolution



Economy Designed to Grow

Pre-mined cryptocurrency is designed for large-scale use and hence massive adoption. The Economic model provides perpetual token burn (mechanically favoring the early investors through programmed deflation).

Suitable for all Apps

Our ecosystem is designed to improve all current apps (eCommerce, website hosting, voting and access to the Olympic Games) with smart contracts that can be modified, autonomous, self-triggered and with unfailing reliability.

Sustainable Governance

Thanks to the decentralized identities management and smart-contracts, balanced governance is ensured by all involved parties (Users, Miners, Investors, Core developers, and DApps providers). The source code and the 12 patents are owned by the community to provide the perfect balance between the virtuous circle of Open Source and the protection against forks, allowing the network to grow and survive for centuries.

Decentralized Identity

The missing link between Humans and new technologies. Uniris provides the first tamper-proof biometric authentication without any key storage while ensuring the latest W3C Authentication Standards.

Geo-Secured Data

The Uniris network can survive any disaster as a result of its Heuristic Replication Algorithms, Geographic and Network Coordinates, Beacon Chains, Oracles & Prediction Module.

Unbreakable Consensus

The ARCH consensus (Heuristic Rotating Atomic Commitment) considerably increases the security and the trust of the Network (fraud risk based on aviation-grade security).

Unlimited P2P Network

Permissionless network without privileged miners based on a new P2P protocol "Supervised Multicasting" eliminating all network bottlenecks.

The UNIRIS Blockchain

Designed for global use



A Truly Decentralized and Unlimited Network

Given the universal constraints both material and physical, billions of transactions cannot be integrated into a single branch of chained blocks. Similarly, regardless of the consensus method, it is not possible to ensure universal consensus on billions of transactions by polling all nodes of the network. Finally, the functioning of the current distributed networks (P2P) is such that it is not possible to guarantee the freshness (consistency) of data on an asynchronous network, unless the network is slowed down excessively by the calculation of the nonce of the block (PoW), as is the case with the Bitcoin network.

Uniris solved these problems in the following ways:

Infinite Chains of Transactions vs a single chain of blocks: Instead of chained blocks of transactions, each block is reduced to its atomic form, i.e. each block contains one transaction and each transaction will be chained in its own chain.

ARCH Consensus: the absolute consensus: ARCH or "Atomic Rotating Commitment Heuristic (ARCH)" is a new generation of Consensus. The detailed explanation of each concept of ARCH is as follows:

Atomic Commitment is the form of "absolute" consensus that implies 100% concordant and positive responses or the refusal of the validation of transaction.

Heuristics is the set of algorithms, software, and parameters that manage the entire network, allowing the network to elect, in a decentralized and coordinated way, the nodes in charge of validating and storing transactions chains.

Rotating, the network being fully distributed (no central or privileged role), the nodes elected for each operation are constantly changing so that no node can predict which node will be elected until the transaction arrives.

Predictive, Optimized, Geo-secure Replication System capable of self-repair: Instead of synchronizing transactions in a disorganized way across the entire network, each transaction chain will be stored in a reproducible and ordered way on a set of nodes - thus each node, independently, will know all the nodes hosting a given transaction and will thus be able to relieve the network by interrogating only the closest "elected" nodes. The election of storage nodes also includes the geographical position to ensure data security even in the event of a disaster in one or more geographical areas.

Distributed Network (P2P) without saturation point: Based on Supervised Multicasting, the peer-to-peer network uses a self-discovery mechanism based on incoming connections and the network transaction chain mechanism to maintain a qualified and trusted vision while generating a minimum of new transactions on the network.

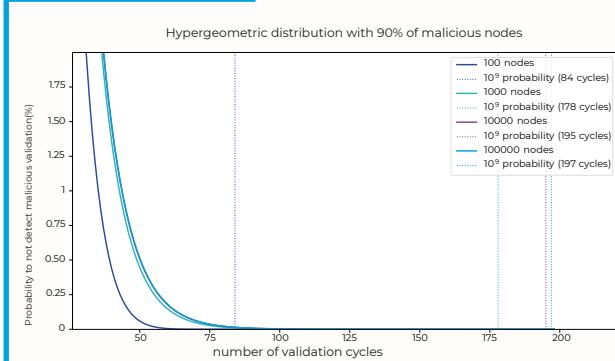
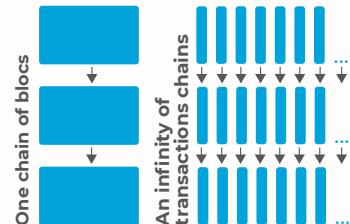
Beacon Chains: Since no node has the physical ability to know the status of each transaction in an unlimited network, the Uniris network uses a set of specific transaction chains, each containing a subset of the addresses of the last transactions for a given date, allowing any node to automatically resynchronize itself in the event of a disconnection.

Oracle Chains: The "State of the World" Oracle chains are updated by consensus every time information is updated (for example, when a new weather report is broadcast, news ...).

Prediction Module: To enable a decentralized network to survive decades or even centuries, it must be able to adapt to threats and react accordingly. For this purpose, the Uniris network has a prediction module capable of linking a network disturbance (e.g. unavailability of nodes in a geographical area) to an event (e.g. storm in that area via Oracle).

Mining, Proof of Work & Energy Consumption: The election of nodes and network synchronization being ensured by the Heuristic algorithms, proof of work is used to check that the nodes causing the validation and the device causing the transaction are authorized (e.g. biometric device), allowing authentication to be completed by its context (e.g. electronic voting requiring the real identity of a voter). Since the random election of nodes is no longer linked to energy expenditure, the network energy consumption is reduced by 3.6 billion times compared to the Bitcoin network.

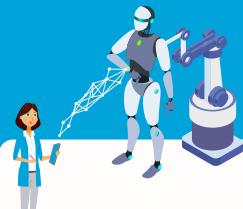
All these elements are explained in a detail inside the Yellow Paper : <https://uniris.io/Yellow-Paper.pdf>



$$1 - \left[\lim_{N \rightarrow +\infty} P[X = k] \right] = 1 - \left[\lim_{N \rightarrow +\infty} \sum_{k=1}^p \frac{\binom{Q}{k} \times \binom{N-Q}{n-k}}{\binom{N}{n}} \right] \approx 10^{-9} = n \approx 200$$

The Uniris network is based on hypergeometric distribution laws which, from an unpredictable election and a formal consensus, make it possible to obtain with certainty (99.9999999%) the same answer by querying 197 nodes as would be obtained by querying 100,000. In other words, this mathematical law makes it possible to obtain a universal consensus from a small part of the nodes - this property thus enters into the heuristics concept widely used on the whole network. The risk of the related availability is ensured by strict management of the disruptive nodes, which are banished after investigation of the origin of the disagreement.





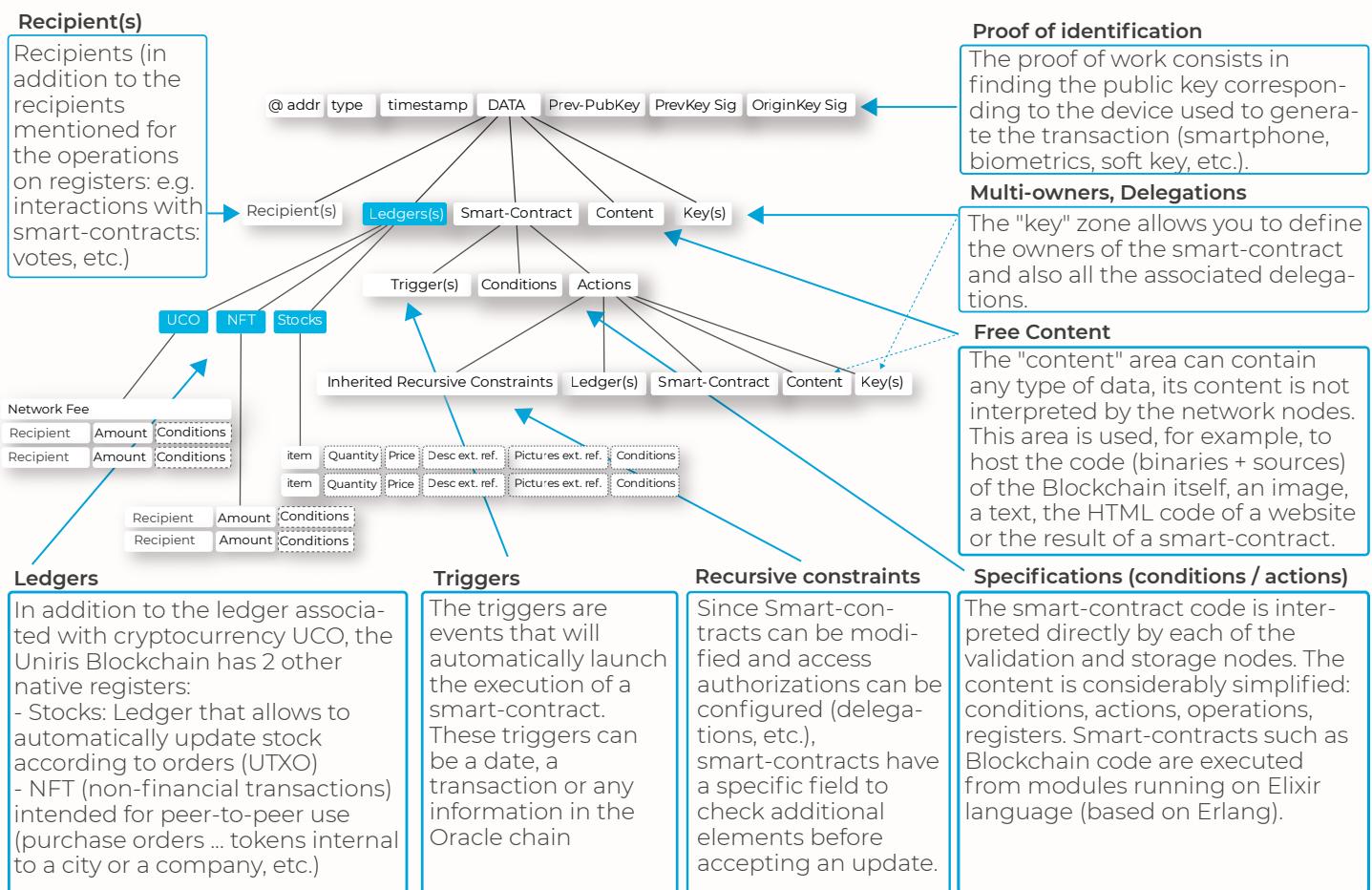
Smart-Contracts

Designed to improve any application or service

First created by the Bitcoin network for updating a shared ledger, then enhanced by the possibility to perform programmed actions through smart-contracts up to the ability to completely operate systems, the Blockchain technology continues to reinvent itself. Unlike smart-contracts compiled on Ethereum, the smart-contracts on the Uniris network are directly interpreted and atomically validated by the miners. Every transaction or smart-contract is stored on a specific group of nodes (rotating heuristic election : ARCH) that can then synchronously load a set of new features: for example, to know the stock status, the number of votes, and the transactions in the same smart-contract (any transaction to a smart-contract is notified and stored on the group of nodes), or automatically trigger an action on the arrival of an event (date, weather, etc.) thereby supporting any real use case.

To ensure the security and irrevocability of smart-contracts, these are entirely based on the UTXO model (release of the unspent transaction) that can be spent/used as an entry into a new transaction. In other words, smart-contracts are not depending on the state of an internal database but only on the transactions already validated.

Whether it's a simple transfer, a rule of access to a building, an online store, hosting a website, a country-wide vote, or even all the code used on the network itself, any transaction follows the following pattern:



Smart-contract example for a marketplace

```
@Alice2:
UCO : 90 to @MyShop2
STOCK : { "item": "t-shirt"
"items": [{"color": "white", "size": "S", "quantity": "1"}]}

@Alice1 : ...
```

In the UTXO model, the only references are the validated transactions, for example, for a merchant site the stock status is not changed in the smart-contract itself but is reconstructed from the validated transactions. The experience of a user or a merchant is absolutely identical since each state is irrefutable and unambiguous.

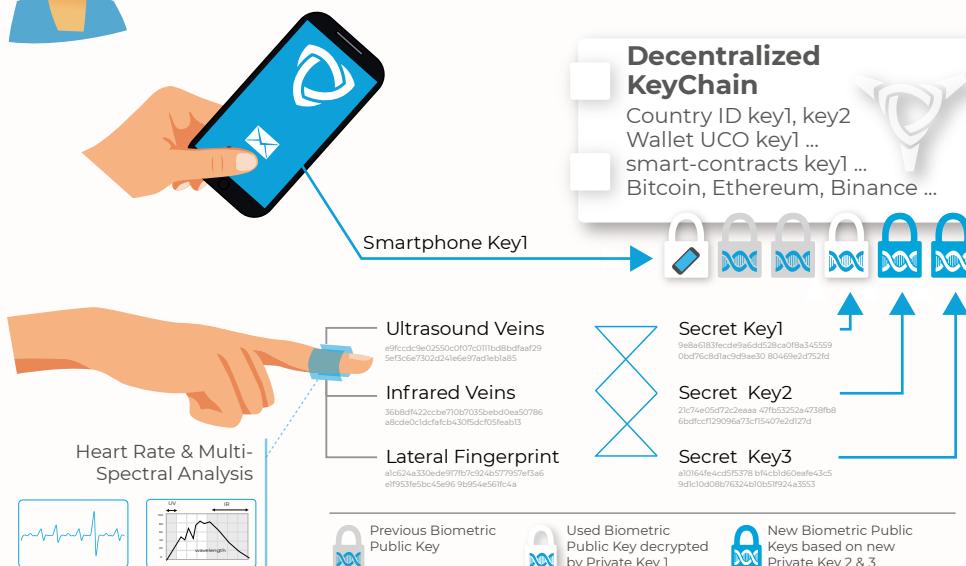


```
{
  "address": "@MyShop2",
  "type": 3,
  "timestamp": 1557131179,
  "DATA": {
    "Ledger": {
      "UCO": [{"fee": 1}],
      "STOCK": [
        {
          "category": "t-shirt",
          "description": "t-shirt eco 200g",
          "price policies": [{"threshold": 10, "policy": "10%"}],
          "vouchers policies": [{"vouchers": "NFT TOWN", "policy": "20%"}],
          "default price": 100,
          "pictures": [{"url": "https://myshop.com/tshirt.png"}],
          "items": [
            {"id": "tbl", "color": "blue", "size": "M", "quantity": "50"},
            {"id": "tbl", "color": "blue", "size": "L", "quantity": "25"},
            {"id": "tw1", "color": "white", "size": "S", "quantity": "25", "price": 90}
          ]
        },
        {
          "category": "pants",
          "description": "pants eco blue",
          "size": "M",
          "price": 120,
          "quantity": "10"
        }
      ],
      "PrevPubKey": "MyShop1PubKey",
      "PrevSig": "Alice1Sig",
      "OriginKey Sig": "DeviceAliceSig"
    }
  }
}
```



Decentralized Identity and Biometrics

The Grail of Mass Adoption



An authentication that cannot be used without our knowledge

Unlike fingerprints, irises, or faces which can easily be reproduced and falsified from a photo on Facebook or in the street - it is impossible to reconstruct the inside of a finger. The device checks vital signs during each authentication to ensure that the finger has not been cut off and that the person is fully aware and consenting before any transaction validation.

Without key storage

All current biometric identifications are based on the same principle:

- capture of biometric data and storage of that recognition data (pattern)
- comparison of the measurement with the pattern
- if the match exceeds a certain threshold then the person is identified (software)

Identification by the Uniris biometric device is no longer based on a recognition threshold and therefore no longer needs to be stored for comparison.

As shown in the figure above, private cryptographic keys are generated on the fly (and then deleted), allowing the user to retrieve and decrypt their decentralized "key ring". Tolerance on identification is ensured by the learning mechanism described on the right. Finally, authentication is no longer software but cryptographic, making any attempt of software attack useless.

Decentralized Identity and Biometrics

No one will be able to steal your keys, you will be able to delete them, but you will never forget or lose them.

- Tamper-proof authentication
- No key storage (GDPR by design)
- Vital signs monitoring
- Learning morphological changes
- Designed for the world population

An authentication of the world population independent of the system

Unlike biometric identification on a smartphone that will only work on one smartphone - Uniris authentication works for any person and on any device. As no keys are stored, it is compatible with the most stringent data protection regulations (GDPR, CNIL, etc.), making biometrics available for large-scale use.

Automatic lifelong learning

As shown in the figure above, the keys are generated in pairs from the biometric measurements. If one of the measurements is different (cut, burn, etc.) then only one key will match and can validate the authentication while the two new keys will be added to encrypt (via associated public keys) the decentralized key ring, thus learning a person's new biometric measurements without ever having to store the keys.

Proof of the origin of the authentication via Proof-of-work

Identification on the Uniris network is not limited to biometric devices and, as shown in the figure above, each access method (smartphone, USB key, software key, etc.) will have its own certification method (see Yellow Paper Season 1).

The identification method being associated with the transaction (see smart-contract schema: "OriginKey Sig") and the proof-of-work will thus allow adjustment of the required security with any smart-contract or portfolio - for example:

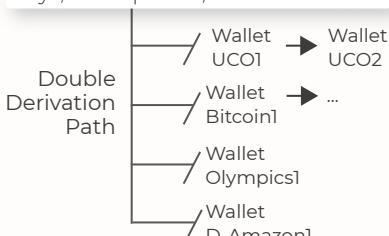
- A transaction of less than 1000 UCO can be carried out from a specific smartphone but only from a biometric device beyond that value.
- Entry into a sensitive building may be made by NFC during office hours, and by biometrics outside those hours.



Decentralized and Interoperable Identity

Decentralized KeyChain

Seed generated randomly and encrypted with an AES key itself encrypted with biometric public keys, smartphone, etc..



Technically, the decentralized identity of a person or a connected object is made up of randomly generated Seed (root key) from which it is possible to generate all keys according to a path of derivation. So, for any access to a service or an application, a key will be calculated on the fly from the seed (root key) and the first public key associated with a service or an application. Thus allowing creating an infinite number of identities without even having to store related keys. All features associated with this decentralized identity will be detailed in the Yellow Paper Season 4: Automated address books, email,

Anonymisation & Accountability by Design

As all transactions are public, the network has a mechanism called the "Wheel of Privacy" to remove correlations between the sender, the recipient, the time, and the amount of transaction. This mechanism is used in particular for electronic voting and allows everyone to keep their vote private without compromising the consistency of the vote logs.



Governance (DAO)

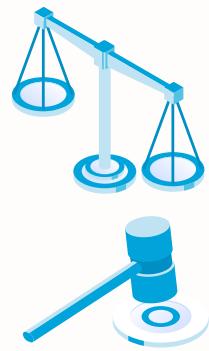
A Governance that integrates the best of everyone

On-Chain and Off-Chain decentralized governance

A DAO (Decentralized Autonomous Organization) is a decentralized organization whose governance rules are automated, immutable, and transparently embedded in a blockchain.

Governance is probably the greatest challenge facing Blockchains. The Bitcoin network now has the most advanced decentralized governance with the famous expression "code is law", nevertheless this governance is based on only a single type of actor - "the owner of the miner", or by extension, the largest pool of miners. It is indeed the code enforced by the largest computing power and hence the professional mining farms that effectively govern the Bitcoin network.

Although this governance is decentralized, it ignores a huge part of the ecosystem, starting with the users themselves, the application providers, the technical contributors, and even the Blockchain itself constrained by the code installed on the highest computing power.



In order for the network to survive over time and adapt to changes in society, the governance of the Uniris Blockchain is based on several technical and functional fundamentals:

Decentralized Identity & Proof of Identity



An essential prerequisite for a human-inclusive governance: the ability of the ecosystem to uniquely identify a person and to integrate that person into a relevant group of actors.

Code «On-Chain»



The code used by the nodes is hosted by the Blockchain itself, so the network is certain that all the nodes will immediately apply the decided updates (via Elixir hot-reload modules and from the information stored in the "smart-contract content" area). The Uniris Blockchain is also equipped with the ability to test the impact of a new feature in real-time.



Modifiable Smart-Contract

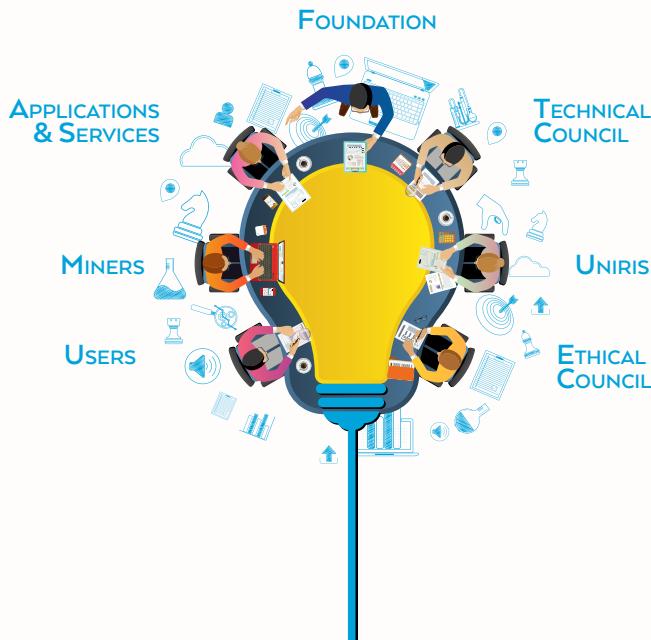
Each smart-contract is stored in the form of a specific transaction chain allowing the network to version (git...) all updates, but also to force each update according to a specific governance (voting quorum, veto right...).



Incentives

Financing of the work associated with updates, new features, and contributions is an essential element. The network has a reserve of one-third of the tokens (with progressive distribution constraints) for this purpose.

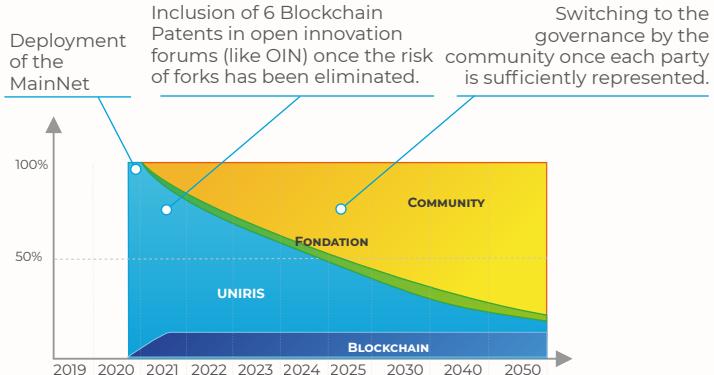
The Governance of the Uniris network is based on 8 distinct



UNIRIS
BLOCKCHAIN

Users	Anyone with the ability to prove their uniqueness (via biometric devices or other processes).
Miners	Owners of the mining nodes which constitute the network itself.
Applications & Services	Application providers with a weightage based on the generated usage.
Foundation	Their role is to lead the community and to organize governance.
Technical Council	Composed of the "core developers" with a weightage based on the importance of their code contribution.
Uniris	As the creator of the network.
Ethics Council	Whose members will be proposed/elected by the community and who will have a veto right overall technical features that would impact the privacy of users.
Blockchain	The Blockchain itself, specifically through its ability to test a full-scale functionality before deploying it on the network. For example, the maximum size of transactions is not linked to a point of view, rather it can be directly tested to determine the actual impact on the network with respect to the need considered.

Planned Governance by the Community





Open Innovation

Create the conditions for generalization

OPEN GOVERNANCE
OPEN INNOVATION
OPEN SOURCE
NETWORK

 UNIRIS
BLOCKCHAIN



Uniris, a Humanitarian and Community Project

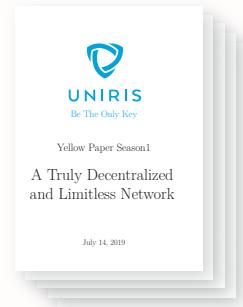
Once the risk of a fork is removed, all the patents will be transferred to the heritage of the open source technologies, this heritage should likely be transferred to the OIN (Open Invention Network) or equivalent. The entire source code will be AGPL licensed.

A voluntary strong pedagogical approach, giving everyone the opportunity to understand the UNIRIS technology

Between scientific publications and popular articles, the underlying technology will be described in detail in 5 Yellow Papers.

The first part, already published, describes the functioning of the network (Consensus ARCH, Supervised Multicasting (p2p) and all the mechanisms that have led to an unlimited network) :
<https://uniris.io/UNIRIS-Yellow-Paper.pdf>

The following sections will be discussed in the future: application programming, open governance, the building blocks of the functioning of the decentralized identity, and finally, the biometric devices and their derivatives.



List of Patents

- FR3049089 (A1) **Method of transaction validation relating to Transactions Chains through a decentralized network**
US2019044735 Transaction validation relating to one or more transactions chains in a unitary and asynchronous way by the elimination of all the limitations of Blockchain technology. The process allows enhanced security and confidentiality, in particular by integrating the constraints in terms of geolocation and number of the messages validation.
WO2017162931
- FR3049101 (A1) **Process management of smart-contracts through transactions chains**
Digital identities - exchange of value - delegations management, authorizations and revocations - electronic votes management - delivery of goods/supply chain - organizations - health data management - reputation management and certification.
- FR1907901 **Atomic validation of transaction chains through a decentralized network**
Consensus ARCH (Atomic Rotating Commitment Heuristic Election), optimized and geo-secure replication process - self-repair network and data - Prediction Module and Supervised Multicast Network Layer (P2P Protocol)
- FR3049088 (A1) **Method associated with the Digital identity management of an individual, a connected object, an organization, a service through a decentralized network**
Identification-authentication-registration of unique or multiple digital identities for an individual or an object on an external device - exchange of values without disclosure - condition management - management of members, owners, multi-signatures, reputation, certification and recertification of a digital identity - management of mutable external identifiers through digital identity.
- FR3049087 (A1) **Method of securing transactions through knowledge and through cross-capabilities across a decentralized network**
Cryptographic process to cross-reference the knowledge and capabilities of the devices so as to prohibit any unauthorized operation, renew and permanently forfeit all cryptographic keys of all devices, remove correlation elements of time, value, and actors involved (privacy wheel), initialize cryptographic keys for a decentralized network without using an external device to the system, minimize the exposure of public keys related to private keys of the device, to reset a device and revoke a user.
- FR3049086 (A1) **Method of Biometric Authentication without disclosure through a decentralized network**
A method of not having to reveal all or part of the biometric measurements of an individual - integrating the compensations of the biometric measurements and lifelong morphological adaptability of an individual - never having to store any biometric data or any biometric measurement or a cryptographic key relating to an individual - making it possible to record several fingers of the same individual without disclosure and allowing operations without a network and without an individual having never used any device before.
- FR3049090 (A1) **Biometric adaptive authentication device using ultrasound, photographs in visible light of contrast and infrared, without disclosure through a decentralized network**
CN108780501 A Biometric authentication device without any disclosure obtained from ultrasounds and photograph of the venous network of the finger, of the lateral fingerprint of the finger and configured to take a photograph of the infrared intrinsic emission of the finger, to check the heart rate and perform an analysis, Multireferential spectrometry of the finger.
CN109074478
US2019089539
WO2017162930
- FR3049121 (A1) Mechanical and electrical coupling device to connect to a computer periphery without damaging the host system.
- FR3049093 (A1) Device for the reproducible positioning of at least one finger of an individual while taking the biometric measurements
- FR3049085 (A1) Communication device for communicating with other devices and enabling nearby transactions and creating a mesh network
- FR3049091 (A1) Device for Biometric ultrasonic testing and vital signs verification
- FR3049092 (A1) Device for biometric authentication and reliability of measurements by visible and infrared light photography, spectrometry, and differential analysis

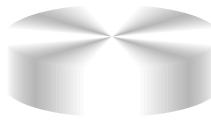


Big Picture

An example of cryptocurrency transfer

Decentralized KeyChains

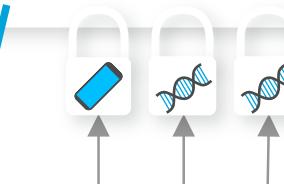
Contains the user's private keys and the pointers keys (other digit pointers, smart-card, IoT ...)



Human, Organization, Group, IoT Keychains

Alice's Keychain

Country ID key1, key2
Wallet UCO key1 ...
smart-contracts key1,
Bitcoin, Ethereum Key1 ...
Carl Key1 ...



Encrypted with
Alice's Public Keys

Alice recovers her keys on
her decentralized biometric
Keychain, generates the
transaction and transmits it
to a «Welcome Node»



@Alice #2
10 UCO to @Michelle

Heuristic Rotating
Coordinator Node
generates PoW
& transaction stamp

Alice

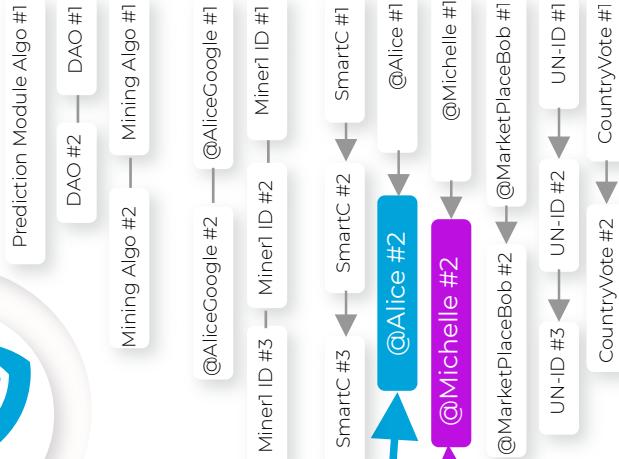


Coordinator & Cross-validation
Nodes recover full @Alice chain,
unspent outputs ... by requesting
each associated Storage Pool

Smart-contracts & Identities

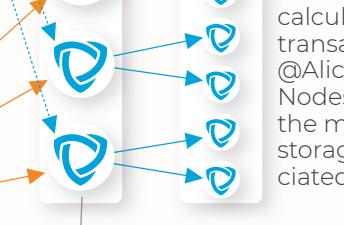
Contains all Public Data
(smart-contract chains, Decentralized Identity chains for Nodes,
Organizations, Groups, IoT, Individuals, etc.)

Network Identities Smart-contracts & Ledgers



Heuristic Rotating Coordinator Node

generates PoW & transaction stamp



Heuristic Rotating Cross
Validation Nodes
cross validate the Coordinator
stamp & PoW



Michelle