

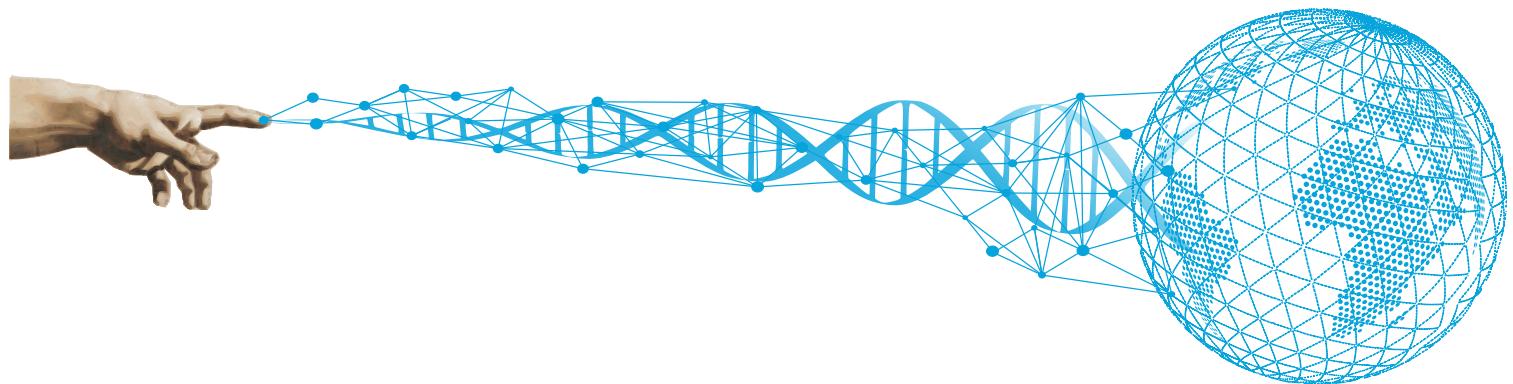


UNIRIS

White Paper

Se el Dueño de tu Identidad

Diciembre 2019



¿Qué pasaría si la tecnología por fin podría simplificar su vida diaria sin arriesgar su seguridad? ¿Qué pasaría si se le dijera que Usted ya tiene esta tecnología?

La promesa de Uniris es proveer el acceso a todas las tecnologías mientras protege su identidad con un simple toque de su dedo. El equipo de Uniris ha desarrollado una tecnología inviolable y de alta seguridad; es tan segura como el chip de la tarjeta bancaria. Ésta le permite reemplazar cualquier contraseña, llave u otro dispositivo de autenticación con una simple lectura de la información de sus dedos.

Esta tecnología de código abierto (“open source”) está basada en una red de nueva generación llamada “Blockchain” (cadena de bloques), con el fin de manejarla a una escala humana global sin el control o la intervención de ninguna persona, compañía u organización. Para lograr la escala y adopción, nosotros mejoramos la tecnología de Blockchain de tal manera que ella pueda reemplazar cualquier aplicación o servicio: abrir su carro o la puerta de su casa, identificarlo a Usted mismo o pagar en línea sin arriesgar sus datos y compras, siempre tener su historial médico accesible pero protegido... La tecnología funciona desde el primer uso a pesar de su ubicación.

Para funcionar y recompensar a las personas que alojan un servidor de red (minero) que verifica cualquier transacción en la Uniris Blockchain, una cadena de bloques se construye alrededor de una criptomonedra (UCO en el caso de Uniris). Esta moneda se crea al comienzo del proyecto para financiar todos los desarrollos, convirtiendo a cada inversor en un verdadero participante en la construcción de este Nuevo Mundo desde el primer momento de inicio.

Únase como un inversionista, desarrollador, embajador, y conviértase en un constructor del futuro de las conexiones globales.

1	UNIRIS Resumen	4
2	Panorama competitivo y las ventajas de Uniris	5
2.1	La Blockchain más escalable, segura y eficiente en energía gracias a ARCH Consensus	5
2.2	Smart-contracts: los robots autónomos de la era digital	6
2.3	Una identidad descentralizada que respeta nuestra privacidad	6
2.4	El fin de las contraseñas y medios innecesarios	6
3	Un mercado casi ilimitado	7
4	Estudios de mercado	8
5	The Uniris Coin - Una criptomoneda programada para crecer	9
5.1	Suministro de control	9
5.2	Crear demanda	9
5.3	Hipótesis sobre el crecimiento de la criptomoneda UCO	10
6	Distribución, asignación y minería	11
6.1	Un modelo que enfatiza el intercambio de valores	11
6.2	Asignación de fondos	11
7	Mineros (nodos) y minería en la red de Uniris	12
8	Hoja de ruta para el futuro	13
9	¡El equipo!	14
10	The UNIRIS Blockchain - designed for global use	16
10.1	Una red verdaderamente descentralizada e ilimitada	16
10.2	Cadenas infinitas de transacciones frente a una cadena de bloques	16
10.3	ARCH Consensus: el consenso absoluto	16
10.4	Sistema de replicación predictivo, optimizado y geo-seguro capaz de auto repararse	16
10.5	Red distribuida (P2P) sin punto de saturación	17
10.6	Beacon Chains	17
10.7	Oracle Chains	17
10.8	Módulo de predicción	17
10.9	Minería, prueba de trabajo y consumo de energía	17
11	Diseñados para mejorar cualquier aplicación	18
12	Identidad descentralizada y biometría : El Grial de la adopción masiva	20
12.1	Identidad descentralizada y biometría	20
12.2	Prueba del origen de la autenticación a través de Prueba de trabajo	21
12.3	Identidad descentralizada e interoperable	21
12.4	Rueda de la privacidad	21
13	Gobernación que integra lo mejor de todos	23
13.1	Gobernación descentralizada dentro y fuera de la cadena	23
13.2	Gobernación planificada por la comunidad	23
13.3	La gobernación de la red Uniris se basa en 8 grupos distintos:	24
14	Innovación : Crea las condiciones para la generalización	25
15	Cuadro grande	26

1 UNIRIS Resumen

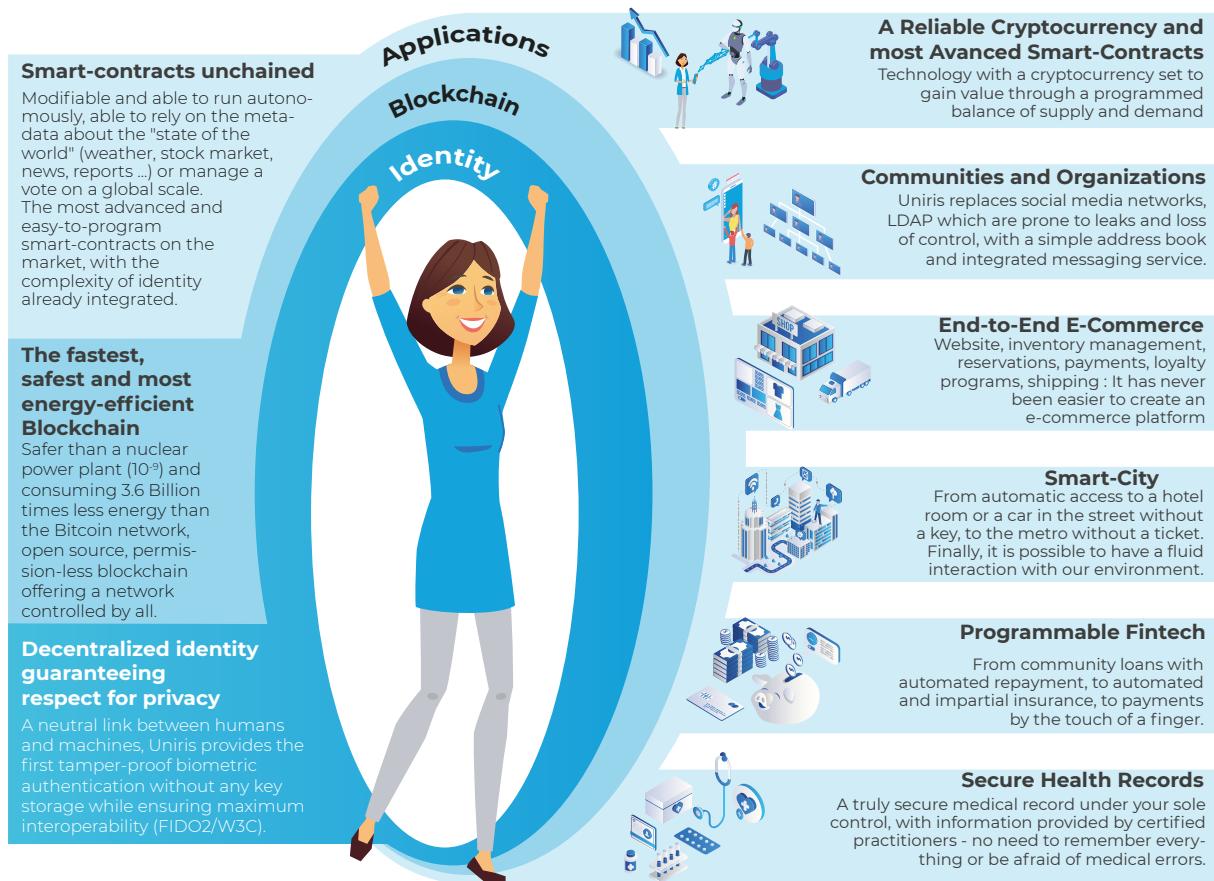
La blockchain de Uniris ofrece la primera plataforma de servicios integrados capaz de satisfacer una necesidad fundamental: devolver a todos el control sobre la tecnología. De esta manera, Uniris es parte de la promesa de un mundo más seguro, más inclusivo y verdaderamente descentralizado.

4 años de investigación y 12 patentes internacionales sólidas dotan a Uniris con los atributos tecnológicos que los predecesores han carecido—escalabilidad, velocidad, fiabilidad, y simplicidad de identificación nativa biométrica. Estas patentes se ofrecerían a la comunidad de open source para fomentar la participación, y, por consiguiente, acelerar la tecnología.

Diseñada para la adopción masiva, Uniris está basada en una forma nueva de consenso de validación irrompible (ARCH en inglés). Es ultra seguro, y permite un número ilimitado de transacciones. Uniris incorpora la biometría de forma nativa, utilizando un método de identificación inviolable y accesible a todos. Esta tecnología utiliza la increíble complejidad del interior del dedo, la que es única para cada individuo, sin necesidad de guardar ningún dato biométrico.

Nuestra criptomoneda UCO es la columna vertebral de la red que alimenta estas transacciones y da beneficios económicos a los contribuidores, desarrollando un ecosistema construido para las personas y por las personas. Nuestra plataforma de blockchain tiene como objetivo reemplazar y mejorar todas las aplicaciones actuales con un ecosistema completo y abierto, lo que permite a las personas moverse de la confianza impuesta por sistemas centralizados (Facebook, Google, Amazon, bancos ...) para un sistema descentralizado donde todos retendrán el control de sus datos, propiedad y privacidad.

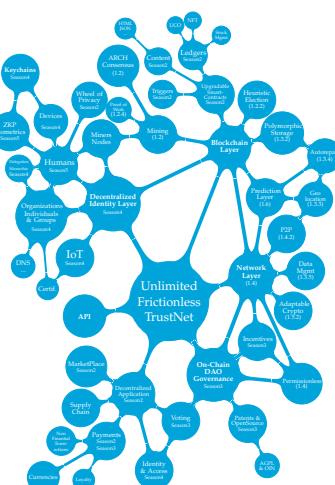
Uniris le devuelva a la humanidad el control sobre la tecnología, y a cada individuo el control sobre su identidad.



2 Panorama competitivo y las ventajas de Uniris

2.1 La Blockchain más escalable, segura y eficiente en energía gracias a ARCH Consensus

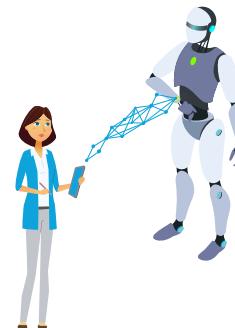
Por primera vez en la historia, Blockchain representa una tecnología que puede funcionar sin un organismo central de toma de decisiones. Un sistema que no solo es imparcial sino también transparente e inalienable. La nueva forma de ARCH Consensus, creada por Uniris, se basa en una elección impredecible de un pequeño subconjunto de nodos (minero) para validar y almacenar transacciones (197 por 100,000 nodos). La red utiliza la multidifusión supervisada para que cada nodo siempre sepa dónde buscar datos a través de la ruta de red más eficiente, lo que permite un aumento lineal en el número de transacciones / seg en función del número de nodos de red (100x). La siguiente tabla presenta las principales diferencias con las otras 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 (FBP)	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

2.2 Smart-contracts: los robots autónomos de la era digital

Los Smart-contracts son en la informática lo que los robots son en la vida real: realizan acciones de acuerdo con los eventos. Los contratos inteligentes de Uniris dan un salto tecnológico hacia adelante. Son autónomos y pueden activarse a partir de eventos internos (fecha, transacciones) o de la vida real (el canal de Oracle: verificado por consenso y referencias cruzadas de información) como el clima, el precio de las acciones, las noticias. Se adaptan a su entorno. Totalmente modificables, pueden gestionar de forma nativa operaciones como gestión de existencias, pagos, alojamiento web... sin crear realidad fuera de las transacciones confirmadas (UTXO).



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

2.3 Una identidad descentralizada que respeta nuestra privacidad

La identidad descentralizada evita la necesidad de confiar la identidad de uno a un tercero, que podría encontrarse en un conflicto de intereses y explotar nuestra identidad sin nuestro conocimiento, como Google, Facebook o nuestro sitio comercial favorito. La persona retiene el control exclusivo de su identidad, que se almacena en una multitud de nodos asegurando su durabilidad e integridad. Esta identidad descentralizada garantiza así el respeto a la privacidad y su interoperabilidad con el resto de las aplicaciones. Junto con las posibilidades que ofrecen los contratos inteligentes, se convierte en un elemento central de nuestras interacciones con el mundo: acceso a los principales eventos públicos (Juegos Olímpicos, conciertos, etc.)

2.4 El fin de las contraseñas y medios innecesarios



Integrada en la blockchain, la tecnología biométrica proporcionada por Uniris permite a cualquier persona identificarse sin dificultad y sin almacenar datos biométricos. Este es un control de acceso a prueba de falsificaciones y sin divulgación. ¿Cómo funciona? Los datos biométricos del interior de uno de nuestros dedos generarán varias claves criptográficas que nunca se revelarán y que utilizarán nuestra identidad digital. Solo la persona capaz de regenerar una de estas claves podrá descifrar su identidad digital y, por lo tanto, probar su identidad. Más allá de la elegancia tecnológica, capaz de generalizar la biometría sin riesgo para nuestra vida privada, este método permite resolver el principal problema de las blockchain, que es la adopción masiva.

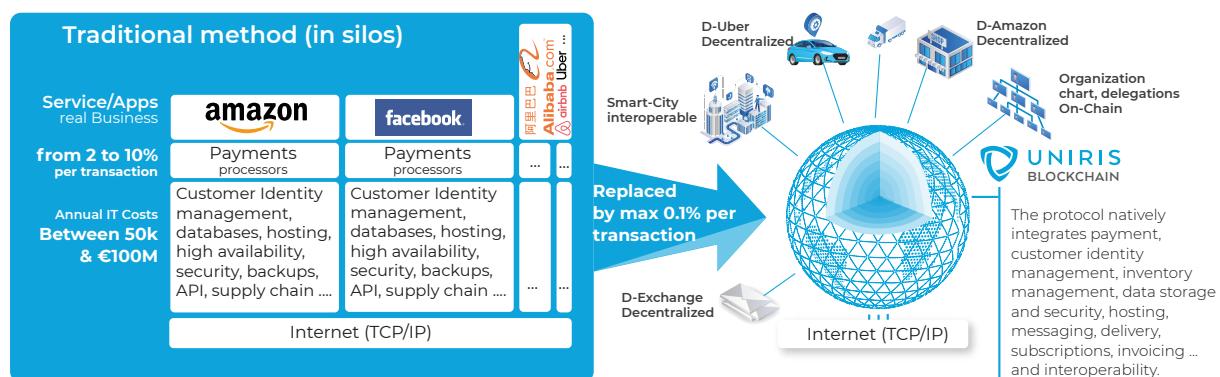
	Biometrics data stored	GDPR	Software vulnerabilities	Identification method	Falsifiable Biometrics	Learning morphological evolution	Identification Scale
Biometrics on Smartphone (iOS, Android ...)	Yes (local)	Local	Yes	threshold	Yes	No	100 000
Industrial/Defence Biometrics (Idemia, Fujitsu ...)	Yes (Servers)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

3 Un mercado casi ilimitado

"Un río siempre elige la ruta más eficiente"

En el modelo prehistórico de la web (aún prevaleciente desde el origen), cada nuevo servicio recrea sus bloques operativos elementales: portal, identificación de clientes, bases de datos de clientes, gestión de servicios, alojamiento, almacenamiento, copias de seguridad, pagos. Amazon, Facebook, Google y otros no comparten nada, lo que lleva a:

- un consumo espantoso de la potencia computacional
- una gran cantidad de nombres de usuario/contraseñas que terminan siendo anotadas por todos lados revelándose.
- riesgos de fraude o ciberataque que pueden sacudir el planeta



El modelo de la Blockchain + Identidad descentralizada finalmente racionaliza este modelo operativo integrando directamente todas las capas necesarias para la creación de nuevos servicios :

- Mucho menos necesidad de habilidades computacionales gracias a la integración "upstream"
- Identidad única y universal, activada solamente por el propietario, a pesar de su ubicación física o virtual de visita
- Deletion of third parties in favor of the Blockchain to ensure the sustainability of the system.
- Eliminación de terceras partes a favor de Blockchain para asegurar la sostenibilidad del sistema.

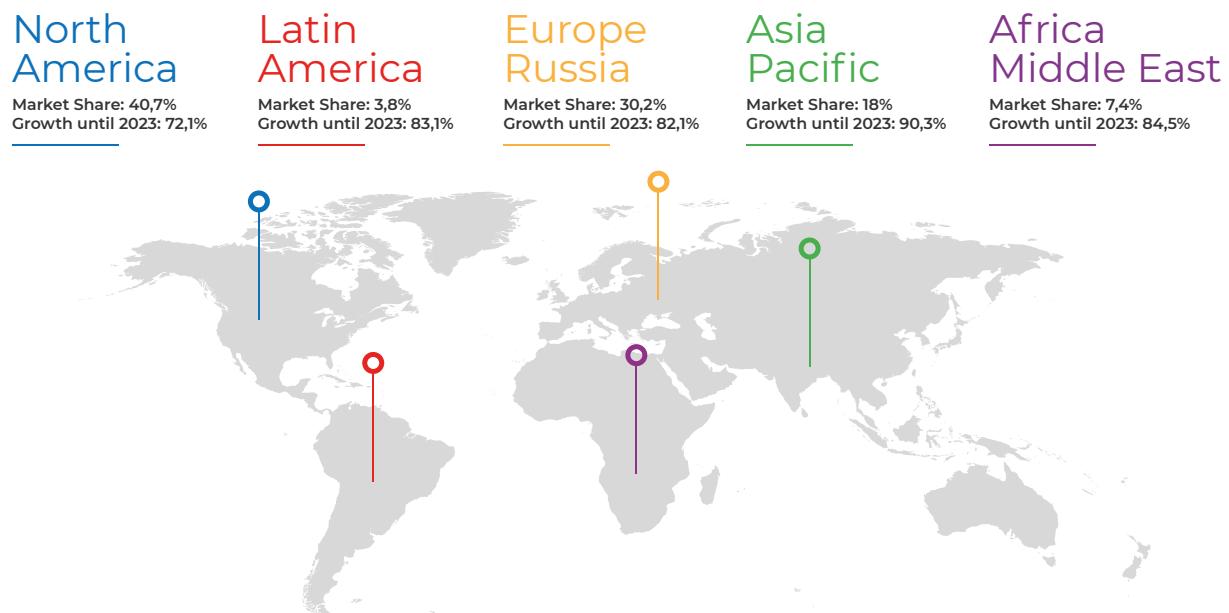
4 Estudios de mercado

Un mercado globalizado con un crecimiento de 80,2% entre 2018 y 2023

El mercado Blockchain se estima conservadoramente en 23 mil millones de dólares para 2023 comparado con 1,2 mil millones de dólares en 2018 con una impresionante tasa de crecimiento anual de 80,2% entre 2018 y 2023.

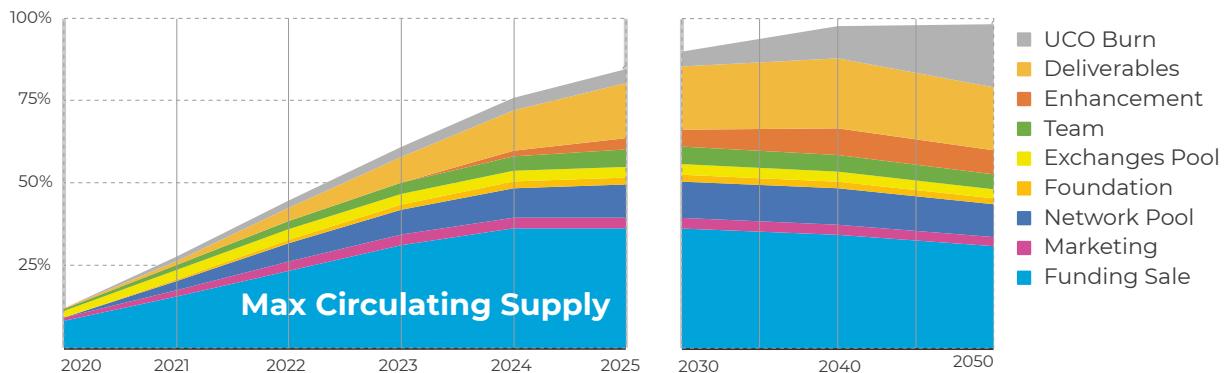


Los 3 segmentos del mercado considerados como los más prometedores para 2023 son identidad digital, Smart-contracts e infraestructuras (Blockchain); son segmentos en los cuales Uniris posee las tecnologías más avanzadas.



5 The Uniris Coin - Una criptomoneda programada para crecer

La nueva economía de los tokens de criptomonedas está basada en el principio sólido y universal de oferta y demanda similar a los productos básicos como el oro o los diamantes. Una criptomoneda crea valor en una plataforma open-source que sobrevivirá independientemente de la compañía que la creó. Nuestra estrategia principal es crear las condiciones tecnológicas para que los "mineros" que confían en nuestra plataforma creen y capturen el mayor valor posible. Además, aseguramos el equilibrio adecuado de oferta y demanda.



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

5.1 Suministro de control

Límite la oferta 10 mil millones de UCO y no uno más. Si alguien invierte en oro mientras otra persona descubre cómo hacerlo a un costo menor, entonces el precio del oro caerá, porque habrá más oferta que demanda. Uniris Blockchain prohíbe la creación de nuevos UCO porque cualquier transacción se basa en la existencia de una transacción no gastada anteriormente (UTXO).

Límite de distribución para evitar el efecto de una afluencia masiva de UCO en los mercados de cambio que podría reducir el precio debido al aumento repentino de la oferta, Uniris está implementando un mecanismo de bloqueo. Con la excepción de los UCO comprados durante la venta privada (parcialmente) y pública, todos los demás UCO están bloqueados y conferidos durante un período de dos a cinco años. Durante este tiempo, la llegada de nuevas aplicaciones a la red conduciría a un aumento de la demanda, compensando el posible aumento de la oferta.

Deflación programada Uniris Blockchain destruirá automáticamente una parte de los UCO resultantes de los costos de transacción, creando así un mecanismo de deflación programado para aumentar el valor de cada UCO (parte gris de la curva).

5.2 Crear demanda

El segundo principio es crear escasez del recurso a través de la demanda. Más allá de los dispositivos biométricos que solo estarán disponibles en UCO, el desafío es crear una adopción masiva de la solución (necesidad de comprar UCO para alcanzar una necesidad real). Nuestra estrategia se basa en 3 ejes (descritos en detalle en la Hoja de ruta más adelante):

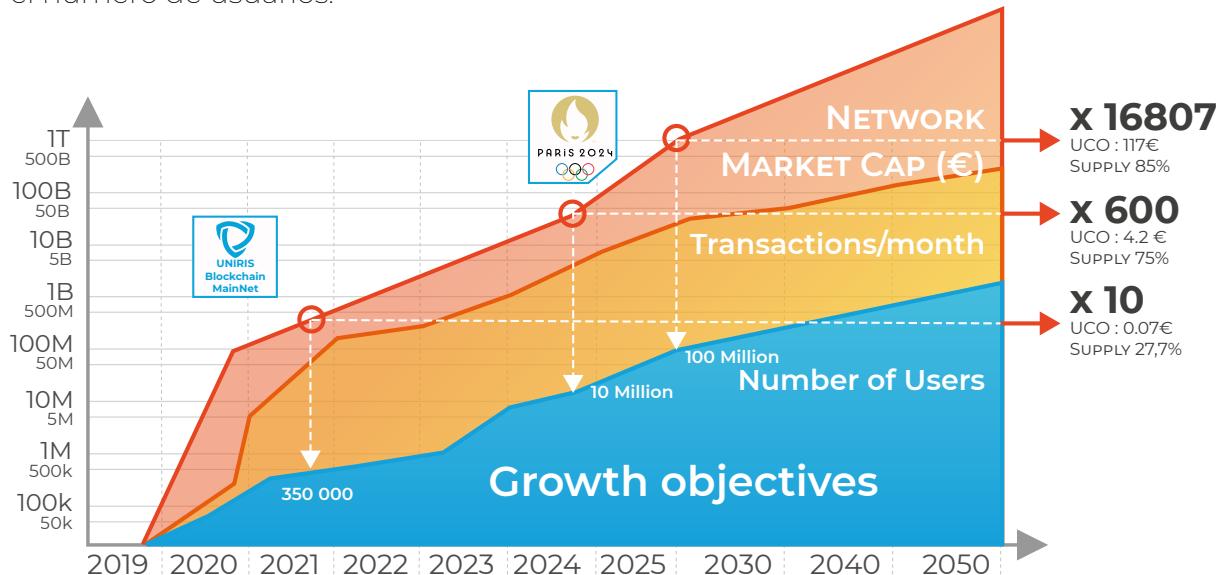
Ser la plataforma de referencia para la producción de smart-contracts Gracias a las características sin precedentes y tan esperadas de los smart-contracts (autónomos, modificables, Oracle integrado, escalables...) y finalmente integrando una Identidad descentralizada que cualquiera puede usar, la plataforma Uniris impulsa el mundo de los smart-contracts más allá del mundo de la criptomoneda.

Aumentar el uso ofreciendo la plataforma más simple y avanzada Como App-Store que le permite multiplicar la cantidad de aplicaciones y servicios en la red, el objetivo de Uniris no es desarrollar e implementar todas las diferentes aplicaciones, sino crear un ecosistema que facilita, financia y apoya la llegada de todas estas aplicaciones. Por lo tanto, la red proporcionará funcionalidades que son los bloques de construcción necesarios para reemplazar las aplicaciones existentes (ver Hoja de ruta).

El mundo al alcance de sus dedos El objetivo final del proyecto es generalizar la identificación biométrica (o derivados) a escala global, de una red 100% abierta y transparente que finalmente pueda demostrar confianza. Desde abrir las puertas de su casa o su carro hasta votaciones – todo a través de los mecanismos de intercambio.

5.3 Hipótesis sobre el crecimiento de la criptomoneda UCO

El método actual más apropiado para evaluar el valor de una Blockchain (Capitalización de mercado) se basa en la ley de Metcalfe que relaciona el valor de la red con el número de usuarios.



Se han realizado muchas investigaciones sobre el tema de la valoración de criptomonedas utilizando la ley de Metcalfe. Se usaron diferentes variaciones para describir el precio de Bitcoin y, utilizando las correlaciones de Pearson durante el período entre 2010 y 2018, se descubrió que el valor de la red es del orden de:

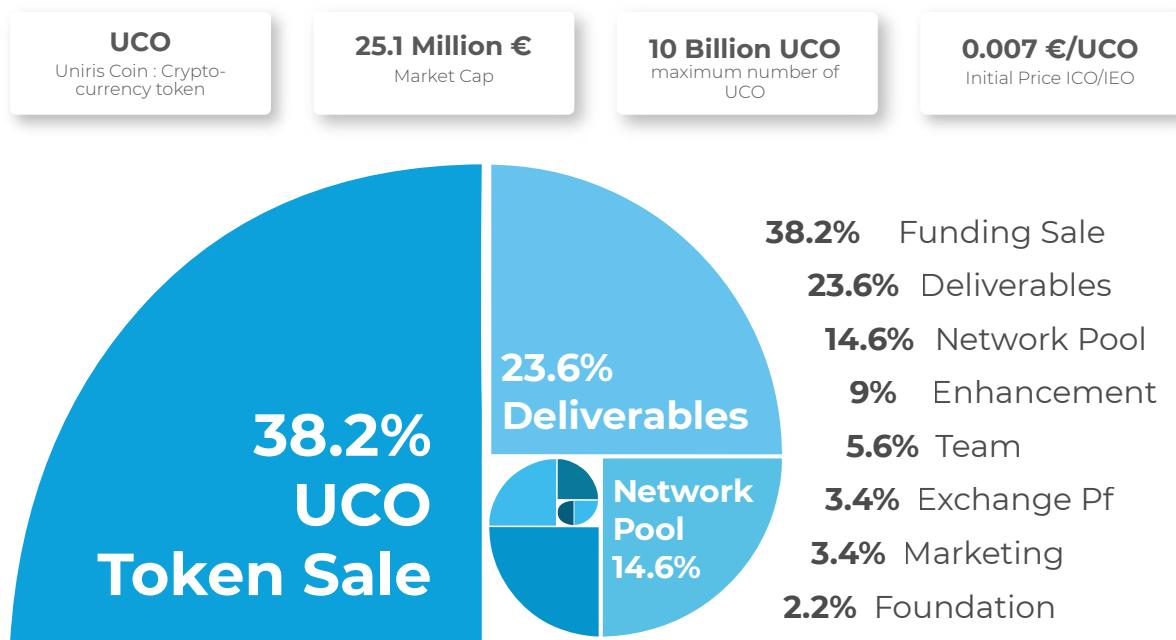
$$\text{valor de blockchain} \approx (\text{cantidad de usuarios})^{1.5} \quad (1)$$

Por lo tanto, esta ley permite obtener una aproximación del valor de una red de acuerdo con el número de usuarios. Por ejemplo, considerando un evento como los Juegos Olímpicos de París 2024, que solo reúne a 8 millones de personas, y sabiendo que el número máximo de UCO intercambiables en el mercado durante este período será del 75% (7,5 mil millones de UCO), nosotros por consiguiente obtenemos:

$$(10 \text{ millones})^{1.5} = 31.6 \text{ mil millones euros}, \text{ esto una valuación por disponible UCO de } 31.6 \text{ mil millones euros} / 7,5 \text{ mil millones UCO} \approx 4.2 \text{ euros/UCO}$$

6 Distribución, asignación y minería

6.1 Un modelo que enfatiza el intercambio de valores



El número de tokens UCO, el valor inicial del UCO y la capitalización de mercado se inicializan de acuerdo con los medios necesarios para la implementación del ecosistema, así como las hipótesis de crecimiento y las prioridades del proyecto. En ICO (Initial Coin Offering: Oferta Inicial de monedas) de Uniris, dos actores han sido privilegiados:

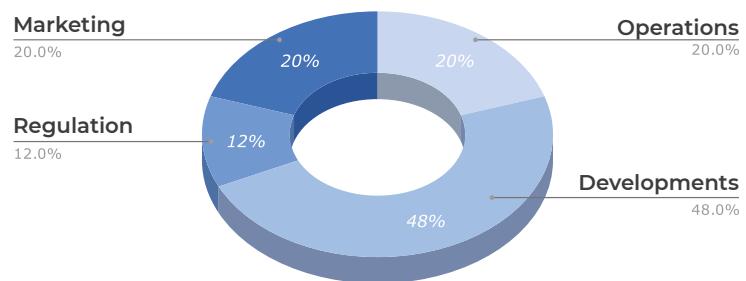
Primeros Inversionistas la casi exclusividad de los tokens disponibles durante los primeros dos años serán los del ICO.

Los contribuidores movilizados hasta la entrega del ecosistema (10% de los tokens en la entrega del código y 90% después de la implementación efectiva y funcional del código).

Con la excepción de los tokens vendidos, los otros tokens Uniris (UCO) estarán bloqueados y se liberarán al 20–33% por año durante un período de 2 a 5 años. El 14.6% de la reserva de la red se utilizará para garantizar un incentivo financiero favorable para los mineros en espera del período de autofinanciamiento. Por último, el 9% asignado a las mejoras se utilizará para desarrollar nuevos casos de uso, pero solo se podrá vender cuando el valor de UCO es 100x mayor que su valor inicial (esto es, 0,7 €/UCO).

6.2 Asignación de fondos

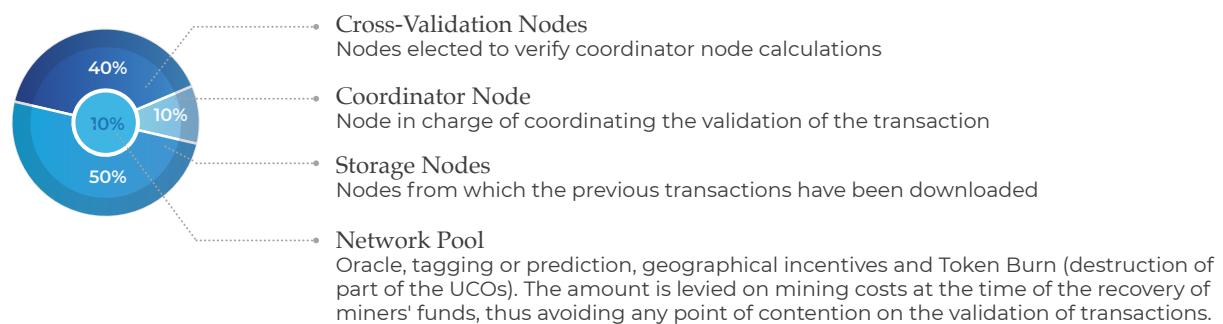
El propósito de las ventas privadas y públicas es recaudar fondos para desarrollar la red y las innovaciones, publicadas en el yellow paper (el libro amarillo). El diagrama opuesto muestra la distribución funcional de los fondos recaudados.



7 Mineros (nodos) y minería en la red de Uniris

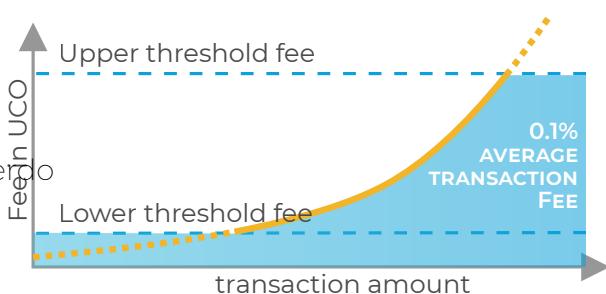
¡No hay necesidad de botas y casco de construcción!

La minería y la prueba de trabajo en la red Uniris ya no se basan en la potencia informática y la energía eléctrica gastada, sino en una verificación criptográfica para validar y asegurar el origen de una transacción (dispositivos biométricos, smartphones, las claves de hardware o software...). Como resultado directo de Consensus ARCH, solo se necesitan 295 mineros para ofrecer el mismo rendimiento que la red Bitcoin, que tiene 100,000 mineros.



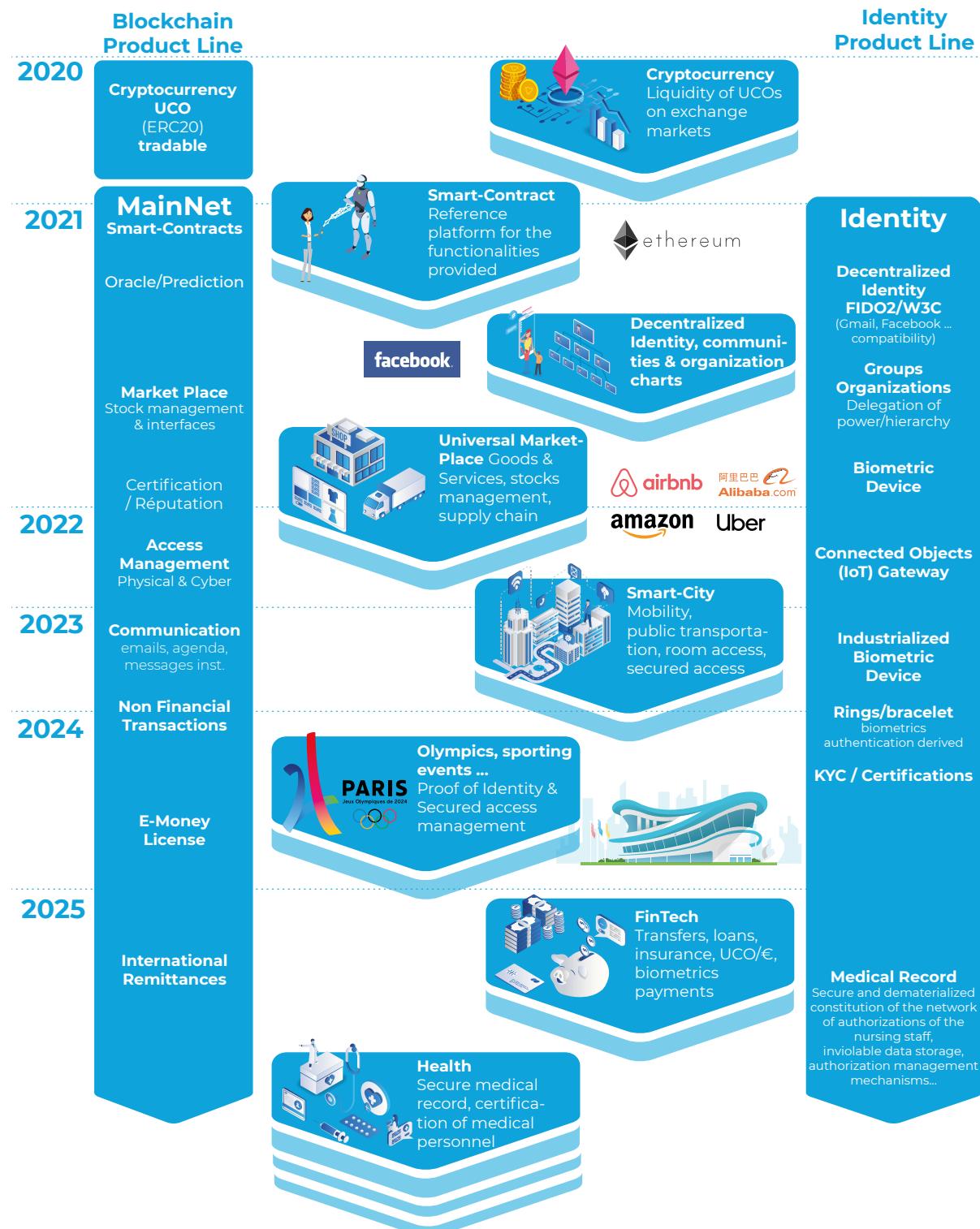
Esto permitirá que cualquier persona sea propietaria de un nodo de almacenamiento y reciba la remuneración asociada, pero solo los mineros elegidos por la propia red pueden convertirse en mineros de validación. Esta elección, transparente a través de un smart-contract, tiene como objetivo maximizar la distribución geográfica de los mineros, pero también garantiza un nivel de ingresos suficiente para todos los mineros elegidos (evitando así el riesgo de que las granjas mineras pongan en peligro la solidez de las redes descentralizadas). Los primeros mineros serán elegidos prioritariamente entre los inversores primerizos que han permitido financiar el desarrollo de la red.

Las tarifas se calculan de acuerdo con los costos reales de la red (tamaño, complejidad...). Las tarifas máximas y mínimas se definen a través de la cadena Oracle, que puede ajustar estos dos límites de acuerdo con los costos de electricidad o el valor de mercado de la criptomonedra UCO. De este modo, es posible perpetuar el modelo financiero tanto para los mineros como para los usuarios.



8 Hoja de ruta para el futuro

La red Uniris, el elemento esencial y el catalizador para la creación de un Nuevo Mundo de Servicios con probada confianza, interoperabilidad, accesibilidad y control por parte de todos.



9 ¡El equipo!

Creada en 2017, después de 2 años de investigación fundamental por Aina, Christophe, Nilesh y Sébastien, UNIRIS SAS es parcialmente propiedad de École Polytechnique (Paris Saclay), financiada por BPI France e inversores de Smart-city hasta un millón de euros. Al final de ICO (venta pública de criptomonedas UCO) se creará una entidad como asociación para organizar la comunidad y para 2025, dejará que el Blockchain público vuele por sus propias alas.

En los últimos meses, hemos desarrollado algunos de los módulos del Blockchain, así como un prototipo del dispositivo biométrico, lo que nos ha permitido **obtener la certificación del Comité Estratégico del Sector de Industrias de Seguridad** para proporcionar el control de acceso durante los juegos Olímpicos de verano de París 2024.

Nuestro equipo es una combinación única de personalidades complementarias, cohesivas y con experiencia de compañías como Thales, Mastercard, Barclays, Orange, Mozilla, Google, PwC e investigadores de la École Polytechnique, CNRS. La mayoría de nosotros nos conocemos mucho antes de la creación del proyecto, profesionalmente o personalmente, lo que nos ha permitido ahorrar una cantidad considerable de tiempo en la implementación de cada uno de los componentes de la solución.

Equipo ejecutivo

 in Sébastien CEO Previously responsible for 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 ex-CTO PAYBACK, Head of Software Development and Support for MasterCard Payment Processing Platforms, Head of Barclays Digital Payments Technology
 in Christophe CSO Ex-Special Forces - Technip Security Manager (Niger), RGPD safety consultant	 in Samuel Blockchain Architect Software Architect and Developer Ethereum (Identity, ICO ...) Michelin/Viseo/Deloitte
 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

Asesores de juntas tecnológicas, estratégicas y de comunicación

 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, Mantis	 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) Experts in Behavioral Sciences & Communication - Media Preparation	 in Baptiste Mata Capital tokenization of real estate investment transactions - Economy & Partnerships

Muchas gracias a todos los que nos han acompañado desde el comienzo de esta aventura: todo el equipo del programa HEC Challenge +, el acelerador de la École Polytechnique X-UP, el Programa de Fundadores StationF, GICAT, CEPS, Cap Gemini; nuestros inversores sin quienes esto no hubiera sido posible: Stéphane, el BPI y todos nuestros inversores de la venta privada. Un gran agradecimiento también a todas las personas, embajadores y asesores que hicieron posible refinar las dimensiones tecnológicas y humanas de este proyecto.

Socios

Las asociaciones de Uniris se centran en la innovación y el crecimiento de la comunidad. Los institutos de investigación nos dan acceso a tecnologías avanzadas y la ayuda en la validación de nuestras innovaciones.



10 The UNIRIS Blockchain - designed for global use

10.1 Una red verdaderamente descentralizada e ilimitada

Dadas las restricciones universales, tanto materiales como físicas, miles de millones de transacciones no pueden integrarse en una sola rama de bloques encadenados. Del mismo modo, independientemente del método de consenso, no es posible garantizar un consenso universal sobre miles de millones de transacciones sondeando todos los nodos de la red. Finalmente, el funcionamiento de las redes distribuidas actuales (P2P) es tal que no es posible garantizar la frescura (consistencia) de los datos en una red asíncrona, a menos que la red se ralentice excesivamente por el cálculo del "nonce" (número que solo puede usarse una vez) del bloque (PoW; proof-of-work en inglés: prueba de trabajo), como es el caso de la red Bitcoin.

10.2 Cadenas infinitas de transacciones frente a una cadena de bloques

en lugar de bloques de transacciones encadenados, cada bloque se reduce a su forma atómica, es decir, cada bloque contiene una transacción y cada transacción se encadenará en su propia cadena.

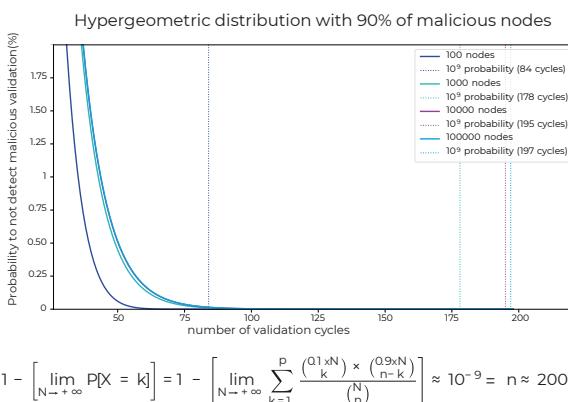
10.3 ARCH Consensus: el consenso absoluto

ARCH o "Atomic Rotating Commitment Heuristic" por sus siglas en inglés (Compromiso de Rotación Atómica Heurística) es una nueva generación de Consenso. A continuación, hay una explicación detallada de cada concepto de ARCH:

El compromiso atómico es la forma de consenso "absoluto" que implica respuestas 100% concordantes y positivas o el rechazo de la validación de la transacción.

La heurística es el conjunto de algoritmos, software y parámetros que gestionan toda la red, permitiendo que la red elija, de forma descentralizada y coordinada, los nodos encargados de validar y almacenar las cadenas de transacciones.

Rotando la red se distribuye completamente (sin función central o privilegiada), y los nodos elegidos para cada operación cambian constantemente para que ningún nodo pueda predecir qué nodo se elegirá hasta que llegue la transacción.



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 a strict management of the disruptive nodes, which are banished after investigation of the origin of the disagreement.

10.4 Sistema de replicación predictivo, optimizado y geo-seguro capaz de auto repararse

en lugar de sincronizar transacciones de manera desorganizada en toda la red, cada cadena de transacciones se almacenará de forma reproducible y ordenada en un con-

junto de nodos, por lo tanto, cada nodo, independientemente, conocerá todos los nodos que alojan una transacción determinada y, por lo tanto, podrá liberar la red al interrogar solo a los nodos "elegidos" más cercanos. La elección de los nodos de almacenamiento también incluye la posición geográfica para garantizar la seguridad de los datos, incluso en caso de desastre en una o más áreas geográficas.

10.5 Red distribuida (P2P) sin punto de saturación

basada en la multidifusión supervisada, la red P2P utiliza un mecanismo de autodescubrimiento basado en conexiones entrantes y el mecanismo de la cadena de transacciones de red para mantener una visión calificada y confiable mientras genera un mínimo de nuevas transacciones en la red.

10.6 Beacon Chains

dado que ningún nodo tiene la capacidad física de conocer el estado de cada transacción en una red ilimitada, la red Uniris utiliza un conjunto de cadenas de transacciones específicas, cada una de las cuales contiene un subconjunto de las direcciones de las últimas transacciones para una fecha determinada, lo que permite cualquier nodo sincronizarse de nuevo automáticamente en caso de desconexión.

10.7 Oracle Chains

Las cadenas Oracle ("Estado del mundo") se actualizan por Consensus cada vez que se actualiza la información (por ejemplo, cuando se emite un nuevo informe meteorológico, noticias ...).

10.8 Módulo de predicción

para permitir que una red descentralizada sobreviva décadas o incluso siglos, debe poder adaptarse a las amenazas y reaccionar como corresponde. Para este propósito, la red Uniris tiene un módulo de predicción capaz de vincular una perturbación de la red (por ejemplo, falta de disponibilidad de nodos en un área geográfica) a un evento (por ejemplo, tormenta en esa área a través de Oracle).

10.9 Minería, prueba de trabajo y consumo de energía

la elección de los nodos, la sincronización de la red asegurada por los algoritmos heurísticos y la prueba de trabajo se utiliza para verificar que los nodos que causan la validación y el dispositivo que causa la transacción están autorizados (por ejemplo, dispositivo biométrico) permitiendo que la autenticación se completará por su contexto (por ejemplo, la votación electrónica que requiere la identidad real de un votante). Dado que la elección aleatoria de nodos ya no está vinculada al gasto de energía, el consumo de energía de la red se reduce en 3,6 mil millones de veces en comparación con la red de Bitcoin.

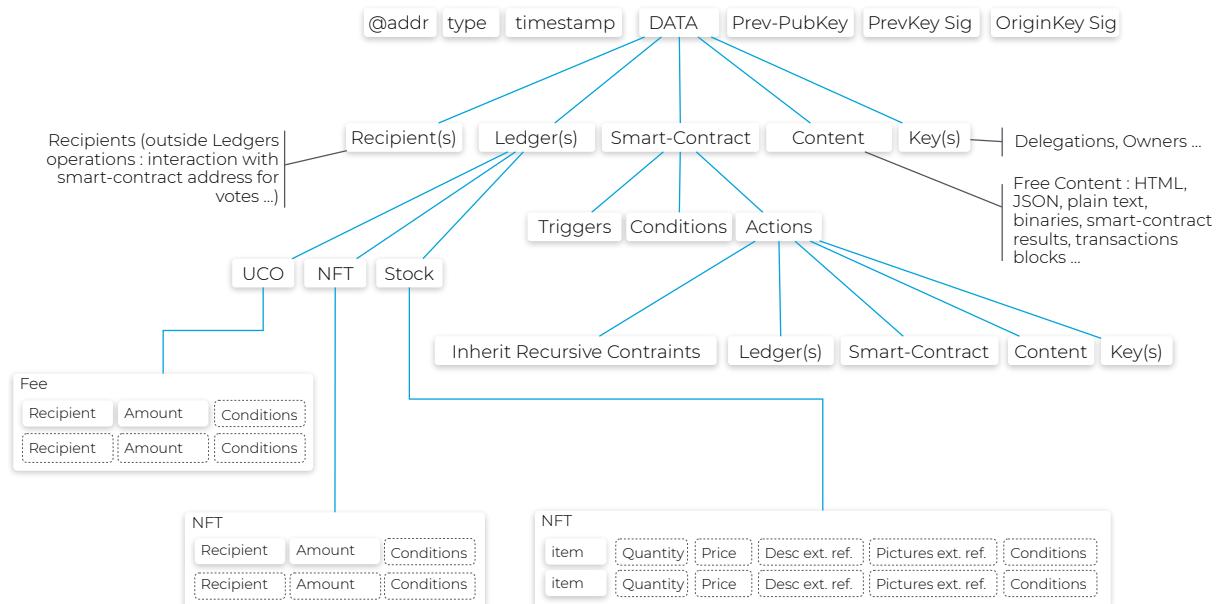
Note: Todos esos elementos se explican de manera detallada dentro del [Yellow Paper \(Libro amarillo\)](#)

11 Diseñados para mejorar cualquier aplicación

Primero creado por la red Bitcoin para actualizar un libro mayor compartido, luego mejorado por la posibilidad de realizar acciones programadas a través de smart-contracts hasta la capacidad de operar completamente los sistemas, la tecnología Blockchain continúa reinventándose. A diferencia de los smart-contracts compilados en Ethereum, los smart-contracts en la red Uniris son directamente interpretados y validados atómicamente por los mineros. Cada transacción o smart-contract se almacena en un grupo específico de nodos (elección heurística rotativa: ARCH) que luego puede cargar sincrónicamente un conjunto de nuevas características: por ejemplo, para conocer el estado del stock, el número de votos y las transacciones en el mismo smart-contract (cualquier transacción a un smart-contract se notifica y almacena en el grupo de nodos) o activar automáticamente una acción a la llegada de un evento (fecha, clima, etc.), lo que respalda cualquier caso de uso real.

Para garantizar la seguridad y la irrevocabilidad de los smart-contracts, estos se basan completamente en el modelo UTXO (liberación de la transacción no gastada) que puede gastarse/usarse como una entrada en una nueva transacción. En otras palabras, los smart-contracts no dependen del estado de una base de datos interna, sino solo de las transacciones ya validadas.

Ya sea que se trate de una simple transferencia, una regla de acceso a un edificio, una tienda en línea, un sitio web, un voto en todo el país o incluso todo el código utilizado en la red, cualquier transacción sigue el siguiente patrón:



Destinatario(s) Destinatarios (además de los destinatarios mencionados para las operaciones en registros, por ejemplo, interacciones con smart-contracts, votos, etc.)

Libros mayores(s) Además del libro mayor asociado con la criptomoneda UCO, la Uniris Blockchain tiene otros 2

registros nativos: [Stocks:] Libro mayor que permite actualizar automáticamente el stock de acuerdo con los pedidos (UTXO). [NFT] (transacciones no financieras) destinadas al uso peer-to-peer (órdenes de compra... tokens internos de una ciudad o empresa, etc.)

Desencadenantes(s) Los desenca-

denantes son eventos que iniciarán automáticamente la ejecución de un smart-contract. Estos desencadenantes pueden ser una fecha, una transacción o cualquier información en la cadena de Oracle.

Restricciones recursivas Dado que los smart-contracts pueden modificarse y las autorizaciones de acceso pueden configurarse (delegaciones, etc.), los smart-contracts tienen un campo específico para verificar elementos adicionales antes de aceptar una actualización.

Prueba de identificación (OriginKey Sig)
La prueba de trabajo consiste en encontrar la clave pública correspondiente al dispositivo utilizado para generar la transacción (smartphone, datos biométricos, softkey, etc.).

Propietarios múltiples, delegaciones

La zona "clave" le permite definir los propi-

etarios del smart-contract y también todas las delegaciones asociadas.

Contenido libre El área de "contenido" puede contener cualquier tipo de datos, su contenido no es interpretado por los nodos de la red. Esta área se utiliza, por ejemplo, para alojar el código (binarios + fuentes) de Blockchain, una imagen, un texto, el código HTML de un sitio web o el resultado de un smart-contract.

Especificaciones (condiciones / acciones)

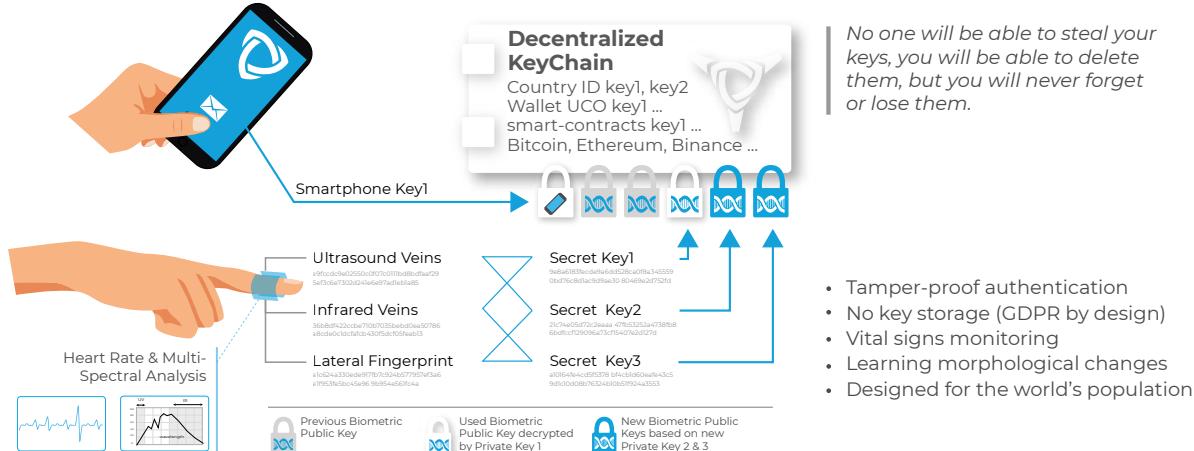
El código de contrato smart-contract es interpretado directamente por cada uno de los nodos de validación y almacenamiento. El contenido se simplifica considerablemente: condiciones, acciones, operaciones, registros. Los Smart-contracts, como el código Blockchain, se ejecutan desde módulos que se ejecutan en el lenguaje Elixir (basado en Erlang).

Ejemplo de un smart-contract para un mercado En el modelo UTXO, las únicas referencias son las transacciones validadas, por ejemplo, para un sitio comercial el estado del stock no cambia en el smart-contract en sí, sino que se reconstruye a partir de las transacciones validadas. La experiencia de un usuario o un comerciante es absolutamente idéntica ya que cada estado es irrefutável e inequívoco.



12 Identidad descentralizada y biometría : El Grial de la adopción masiva

12.1 Identidad descentralizada y biometría



Una autenticación que no puede ser utilizada sin nuestro conocimiento A diferencia de las huellas digitales, los iris, las caras que se pueden reproducir y falsificar fácilmente de una foto en Facebook o en la calle, es imposible reconstruir el interior de un dedo. El dispositivo verifica los signos vitales durante cada autenticación para garantizar que el dedo no se haya cortado y que la persona esté totalmente consciente y que pueda consentir, antes de cualquier validación de transacción.

Sin almacenamiento de claves Toda la identificación biométrica actual se basa en el mismo principio: principio:

- captura de datos biométricos y almacenamiento de esos datos de reconocimiento (patrón)
- comparación de la medida con el patrón
- si la coincidencia supera un cierto umbral, se identifica a la persona (software)

La identificación por el dispositivo biométrico de Uniris ya no se basa en un umbral de reconocimiento y, por lo tanto, ya no necesita almacenarse para comparar. Como se muestra en la siguiente figura, las claves criptográficas privadas se generan sobre la marcha (y luego se eliminan), lo que permite al usuario recuperar y descifrar su "llavero" descentralizado. La tolerancia en la identificación está garantizada por el mecanismo de aprendizaje descrito anteriormente. Finalmente, la autenticación ya no es software, sino criptográfica, haciendo inútil cualquier intento de ataque de software.

Una autenticación de la población mundial independiente del sistema A diferencia de la identificación biométrica en un smartphone que solo funcionará en un solo smartphone, la autenticación Uniris funciona para cualquier persona y en cualquier dispositivo. Como no se almacenan claves, es compatible con las normas de protección de datos más estrictas (RGPD, CNIL, etc.), lo que hace que los datos biométricos estén disponibles para su uso a gran escala.

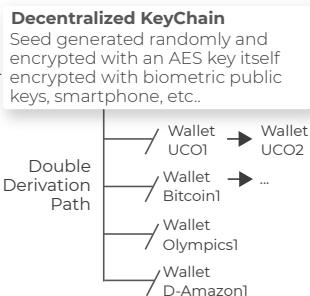
Aprendizaje automático permanente Como se muestra en la figura anterior, las claves se generan en pares a partir de las mediciones biométricas. Si una de las mediciones es diferente (un corte, una quemadura, etc.), solo una clave coincidirá y podrá validar la autenticación, mientras que las dos nuevas claves se agregarán para cifrar (a través de claves públicas asociadas) el anillo de claves descentralizado, aprendiendo así las nuevas mediciones biométricas de la persona sin tener que guardar las llaves.

12.2 Prueba del origen de la autenticación a través de Prueba de trabajo

La identificación en la red de Uniris no se limita a dispositivos biométricos y, como se muestra en la figura anterior, cada método de acceso (smartphone, llave USB, clave de software, etc.) tendrá su propio método de certificación (consulte [Yellow Paper Season 1](#)). El método de identificación que se asocia con la transacción (ver esquema de smart-contract: "OriginKey Sig") y la prueba de trabajo, permitirá el ajuste de la seguridad requerida con cualquier smart-contract o cartera, por ejemplo: Se puede realizar una transacción de menos de 1000 UCO desde un smartphone específico, pero más allá de ese valor solo desde un dispositivo biométrico. La entrada a un edificio sensible puede ser realizada por NFC (Near-field communication en inglés: comunicación de campo cercano) durante el horario de oficina y los datos biométricos fuera de ese horario.

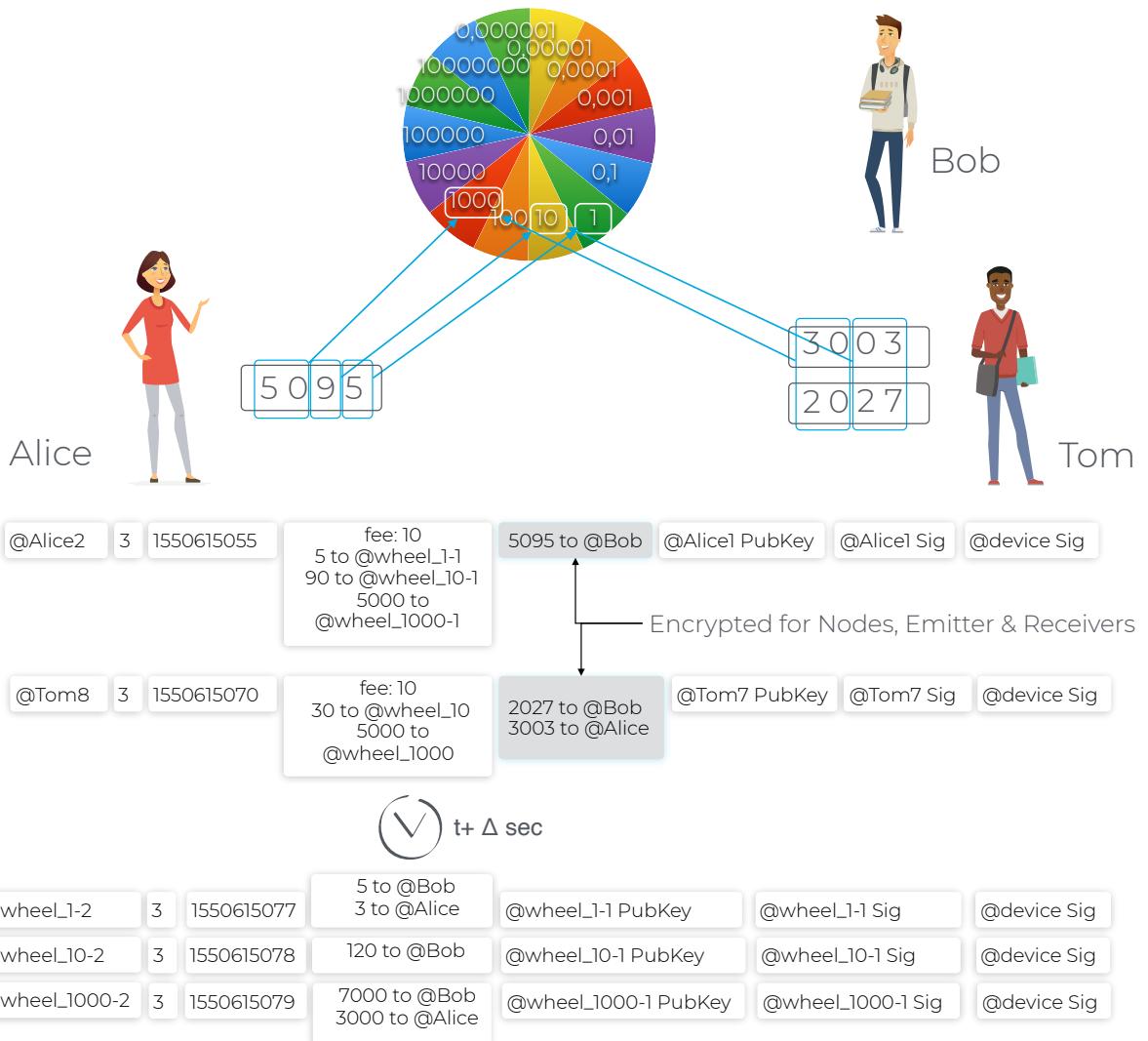
12.3 Identidad descentralizada e interoperable

Técnicamente, la identidad descentralizada de una persona o un objeto conectado se compone de la clave raíz generada aleatoriamente a partir de la cual es posible generar todas las claves de acuerdo con una ruta de derivación. Por lo tanto, para cualquier acceso a un servicio o una aplicación, se calculará una clave sobre la marcha desde la seed (clave raíz) y la primera clave pública asociada con un servicio o una aplicación, permitiendo así crear un número infinito de identidades sin necesidad de tener que almacenar claves relacionadas. Todas las características asociadas con esta identidad descentralizada se detallarán en el Yellow Paper Season 4: libretas de direcciones automatizadas, correo electrónico, FIDO2. .



12.4 Rueda de la privacidad

Como todas las transacciones son públicas, la red tiene un mecanismo llamado "Rueda de la privacidad" para eliminar las correlaciones entre el remitente, el destinatario, el tiempo y el monto de la transacción. Este mecanismo se usa en particular para la votación electrónica y permite que todos mantengan su voto privado sin comprometer la consistencia de los registros de votación.



13 Gobernación que integra lo mejor de todos

13.1 Gobernación descentralizada dentro y fuera de la cadena

Una DAO (Decentralized Autonomous Organization en inglés: Organización Autónoma Descentralizada) es una organización descentralizada cuyas reglas de gobierno son automatizadas, inmutables y están incrustadas de forma transparente en una cadena de bloques.

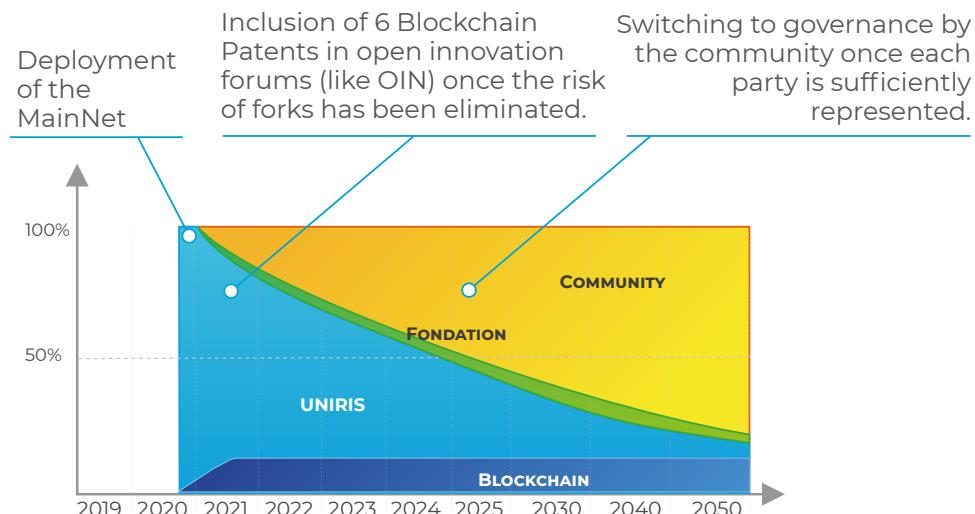
La gobernanza es probablemente el mayor desafío que enfrentan las Blockchains. La red de Bitcoin ahora tiene el gobierno descentralizado más avanzado con la famosa expresión "código es ley", sin embargo, este gobierno se basa en un solo tipo de actor: "el propietario del minero" o, por extensión, el grupo más grande de mineros. De hecho, es el código impuesto por la mayor potencia informática y, por lo tanto, las granjas mineras profesionales que gobiernan efectivamente la red Bitcoin.

Aunque esta gobernanza está descentralizada, ignora una gran parte del ecosistema, comenzando por los propios usuarios, los proveedores de aplicaciones, los contribuyentes técnicos e incluso la propia Blockchain limitada por el código instalado en la potencia informática más alta.

Para que la red sobreviva con el tiempo y se adapte a los cambios en la sociedad, la gobernanza de Uniris Blockchain se basa en varios fundamentos técnicos y funcionales:

 Decentralized Identity & Proof of Identity 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.	 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...).
 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.	 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.

13.2 Gobernación planificada por la comunidad



13.3 La gobernanza de la red Uniris se basa en 8 grupos distintos:

Usuarios Cualquier persona con la capacidad de demostrar su singularidad (a través de dispositivos biométricos u otros procesos)..

Mineros Propietarios de los nodos mineros que constituyen la red misma.

Aplicaciones Y Servicios Proveedores de aplicaciones con un peso basado en el uso generado.

Fundación Su papel es liderar a la comunidad y organizar la gobernanza.

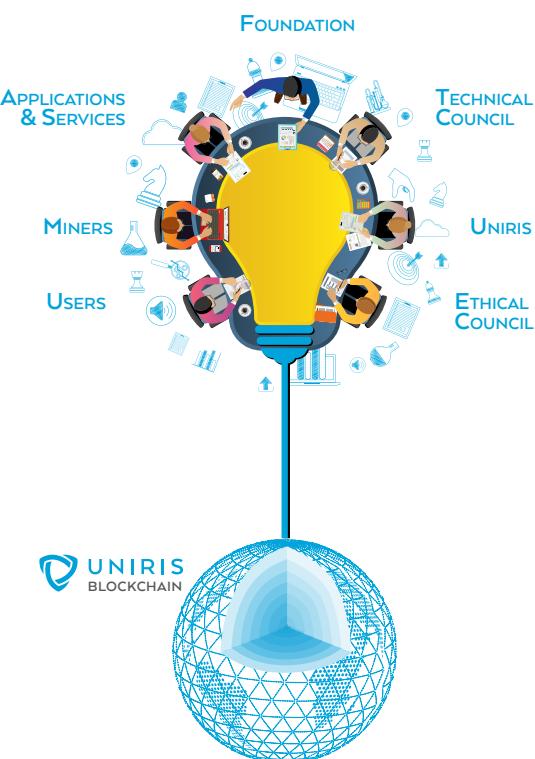
Consejo Técnico Compuesto por los "desarrolladores principales" con un peso basado en la importancia de su contribución de código.

Uniris Como la creadora de la red.

Consejo Ético Cuyos miembros serán propuestos / elegidos por la comunidad y quienes tendrán derecho de veto sobre todas las características técnicas que afectarían la privacidad de los usuarios.

Blockchain Blockchain en sí, en particular, a través de su capacidad de probar una funcionalidad a gran escala antes de implementarla en la red. Por ejemplo, el

tamaño máximo de las transacciones no está vinculado a un punto de vista, sino que se puede probar directamente para determinar el impacto real en la red con respecto a la necesidad considerada.



14 Innovación : Crea las condiciones para la generalización

Uniris, un proyecto humanitario y comunitario

Una vez que se elimine el riesgo de bifurcación, todas las patentes se transferirán al patrimonio de las tecnologías de open source, lo más probable es que este patrimonio se asigne a la OIN. Todo el código fuente tendrá licencia AGPL.

Un fuerte enfoque pedagógico voluntario, que brinda a toda la oportunidad de comprender la tecnología.

Entre publicaciones científicas y artículos populares, la tecnología subyacente se describirá en detalle en 5 Yellow Papers (libros amarillos).

La primera parte, ya publicada, describe el funcionamiento de la red (ARCH Consensus, Supervised Multicasting (p2p) y todos los mecanismos que han resultado en una red ilimitada) : <https://uniris.io/UNIRIS-Yellow-Paper.pdf>

Las siguientes secciones serán discutidas en el futuro: programación de aplicaciones, gobierno abierto, los componentes básicos del funcionamiento de la identidad descentralizada y, finalmente, los dispositivos biométricos y sus derivados.

Lista de patentes

FR3049089 (A1) US2019044735 WO2017162931	Method of transaction validation relating to Transactions Chains through a decentralized network Transaction validation relating to one or more transactions chains in a unitary and asynchronous way by the elimination all the limitations of the Blockchain technology. The process allows enhanced security and confidentiality, in particular by integrating the constraints in terms of geolocation and number of validations of the messages.
FR3049101 (A1)	Process management of smart-contracts through transactions chains Digital identities - exchange of value - management of delegations, authorizations and revocations - management of electronic votes - 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 a unique or multiple digital identity 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 a 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, to renew and permanently forfeit all cryptographic keys of all devices, remove correlation elements time, values, and actors involved (privacy wheel) to initialize cryptographic keys for a decentralized network without using external device to the system, to minimize the exposure of public keys related to device private keys, 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) CN108780501 CN109074478 US2019089539 WO2017162930	Biometric adaptive authentication device using ultrasound, photographs in visible light of contrast and infrared, without disclosure through a decentralized network Biometric authentication device without disclosure obtained from ultrasounds and photograph of the venous network of the finger, the lateral fingerprint of the finger, 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.
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

15 Cuadro grande

Un ejemplo de transferencia de criptomonedas

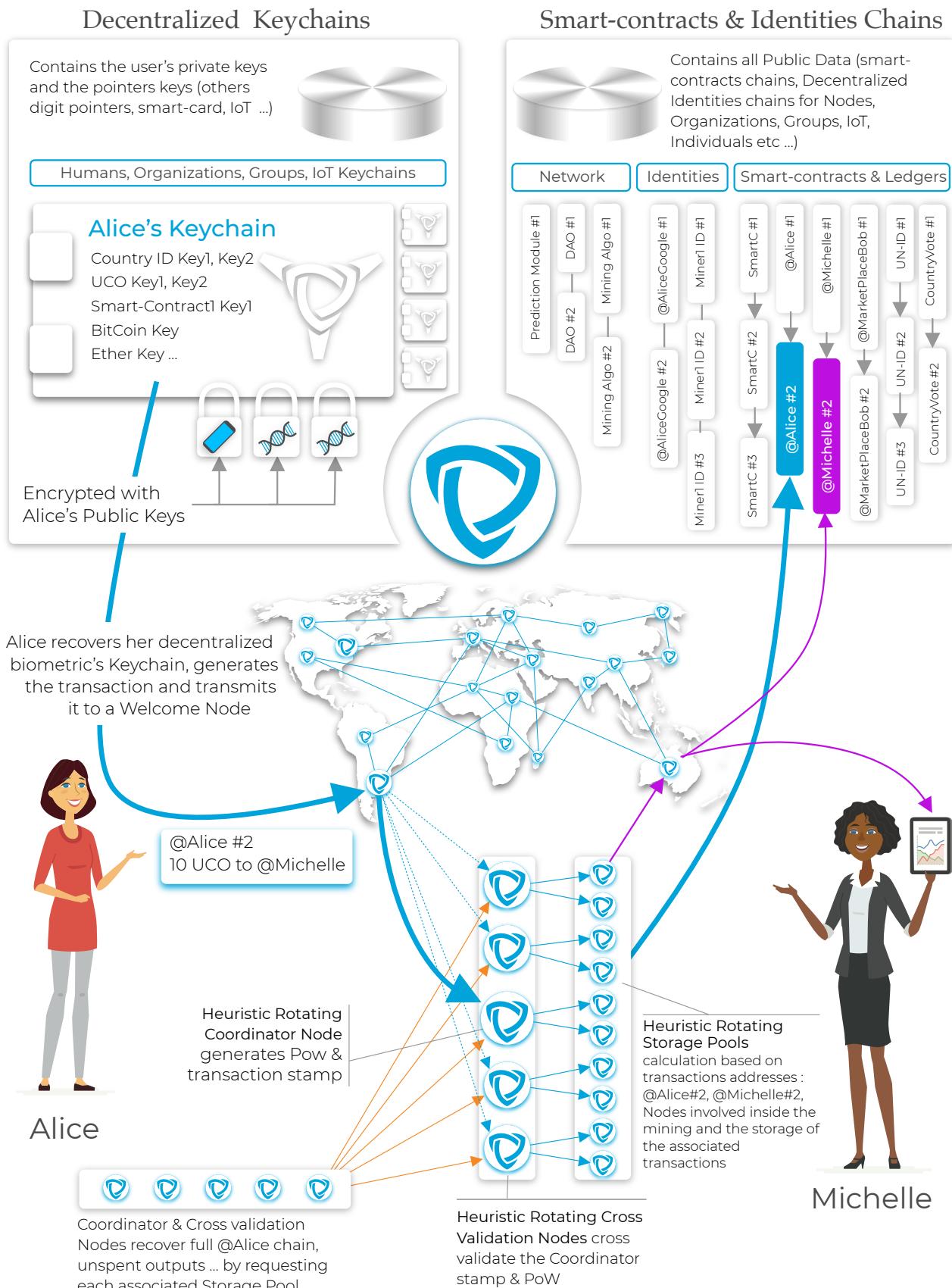


Figure 1: Uniris Chain Overall Functioning