



Et si la technologie pouvait enfin simplifier l'intégralité de votre quotidien en toute sécurité ? Et si on vous disait que cette technologie vous la possédez déjà ?

La promesse d'Uniris c'est donner l'accès à toutes les technologies en protégeant son identité d'un simple effleurement du doigt.

L'équipe d'Uniris a mis au point une technologie ultra sécurisée et infalsifiable, qui permet de remplacer n'importe quel mot de passe, clé ou autre support de façon aussi sécurisée que la puce d'une carte bancaire, simplement en lisant l'intérieur des doigts.

Pour fonctionner à l'échelle de l'humanité et sans qu'aucune personne, entreprise ou organisation ne puisse en prendre le contrôle, cette technologie « open source » est basée sur un réseau de nouvelle génération appelé « Blockchain ». Nous avons amélioré la technologie pour qu'elle puisse remplacer n'importe quelle application ou service : ouvrir sa porte de voiture ou de maison, s'identifier ou payer sur Internet sans risque pour ses données ou ses biens, protéger et avoir toujours à disposition son dossier médical... cette technologie fonctionne dès la première utilisation, quel que soit le lieu où l'on se trouve.

Pour fonctionner et récompenser les personnes qui hébergent un serveur du réseau (mineur), une Blockchain s'articule autour d'une cryptomonnaie (UCO dans le cas d'Uniris). Cette monnaie est créée au démarrage du projet pour financer l'ensemble des développements rendant ainsi chaque investisseur de la première heure réel acteur de la construction de ce Nouveau Monde.

Rejoignez-nous en tant qu'investisseur, développeur, ambassadeur et devenez dès aujourd'hui un bâtisseur actif de ce Nouveau Monde.

L'équipe Uniris.

## Sommaire

Page 2 Vue d'ensemble

Page 3 Positionnement et Comparatifs

Page 4 Plus que les Jeux Olympiques 2024, un marché quasiment illimité

Page 5 Le UCO une cryptomonnaie programmée pour croître

Page 6 Distribution, Allocations et Minage

Page 7 Feuille de route

Page 8 L'Équipe

## Annexes Technologiques

Page 9 Résumé de la technologie

Page 10 Une Blockchain à l'échelle de l'humanité

Page 11 Smart-contracts conçus pour améliorer n'importe quel service

Page 12 Identité Décentralisée et Biométrie

Page 13 Gouvernance

Page 14 Brevets cédés à l'open source

Page 15 Exemple d'un transfert de UCO

La Blockchain Uniris propose la première plateforme de services intégrés, capable de répondre à un besoin fondamental : redonner à chacun, le contrôle sur la technologie. Uniris s'inscrit ainsi dans la promesse d'un monde plus sûr, plus inclusif et véritablement décentralisé.

4 ans de recherche et 12 brevets internationaux solides dotent UNIRIS d'attributs technologiques en rupture avec ses précurseurs : changement d'échelle, de vitesse, de fiabilité, reconnaissance biométrique native dans la solution ; le tout cédé à la communauté open source, permettant à chacun de s'approprier, d'interagir et de faire évoluer la technologie.

Désignée pour l'adoption massive, Uniris s'appuie sur un nouveau consensus de validation incassable ARCHE, ultra sécurisé, permettant un nombre illimité de transactions. Uniris embarque la biométrie de façon native, selon une méthode d'identification infalsifiable et accessible à tous. Cette technologie utilise l'incroyable complexité de l'intérieur des doigts qui est unique pour chaque individu ; auquel elle donne les mêmes propriétés que la puce d'une carte bancaire sans avoir besoin de stocker la moindre donnée biométrique..

Notre plateforme blockchain a l'ambition de remplacer l'ensemble des applications actuelles par un écosystème complet et ouvert, permettant de passer de la confiance imposée par les systèmes centralisés (Facebook, Google, Amazon, banques ...), à un système décentralisé où chacun gardera le contrôle de ses données, ses biens et de sa vie privée.

Uniris redonne à l'humanité le contrôle sur la technologie et à chaque individu, la maîtrise de son identité.

## Uniris en Bref ....

Service de transaction surperformant les normes de marché, intimement intégré à la biométrie

**Ergonomie** : une plateforme capable de remplacer toutes les applications

**Scalabilité** : > 1 million transactions/sec

**Instantanéité** : < 5 sec. temps de validation

**Sécurité** : 0,0000001% risque de fraude même avec 90% de noeuds malicieux

**Durabilité** : 3,6 milliards de fois moins de consommation d'énergie que Bitcoin

**0.1% de frais** de transaction moyens

**Yellow Paper** : <https://uniris.io/UYPStfr.pdf>

**Blockchain & Biométrie certifiées** pour le contrôle d'accès aux **Jeux Olympiques**  
Paris 2024

## Une Utilisation Virale

### Des smart-contracts enfin libérés

Modifiables et capables de s'exécuter de façon complètement autonome, capables de s'appuyer sur l'«état du monde» (météo, info ...) ou de gérer un vote à l'échelle de l'humanité. Les smart-contracts les plus évolués et les plus simples à programmer du marché avec la gestion des identités déjà intégrée

### La Blockchain la plus rapide, la plus sûre et la plus économique en énergie

Plus sécurisée qu'une centrale nucléaire et consommant 3,6 milliards de fois moins que le réseau Bitcoin, open source, sans permission et offrant un réseau contrôlé par tous.

### Identité décentralisée universelle garante du respect de la vie privée

Trait d'union neutre entre l'humain et la machine, Uniris fournit la première authentification biométrique inviolable et sans aucun stockage de clé tout en assurant une interopérabilité maximale (FIDO2/W3C).



### Une Cryptomonnaie solide adossée aux smart-contract les plus évolués

Une technologie disposant d'une cryptomonnaie conçue pour s'apprécier dans le temps par un équilibre entre de l'offre et de la demande



### Communautés et Organisations

Uniris remplace les réseaux de médias sociaux, l'organigramme des responsabilités des entreprises (LDAP) ou simplement les délégations directement sur la Blockchain sans fuites ni perte de contrôle



### E-Commerce tout en 1

Site web, gestion des stocks, réservations, paiement, programme de fidélité, livraison « all in 1 » : il n'aura jamais été aussi simple de créer une plate-forme e-commerce



### Smart-City

De l'accès automatique à une chambre d'hôtel ou à une voiture dans la rue sans réserver, au métro sans acheter de billet, une interaction avec notre environnement enfin fluidifiée



### Fintech Programmable

Des prêts communautaires, remboursements automatisés, assurances automatisées et impartiales, jusqu'aux paiements par un simple effleurement de doigt

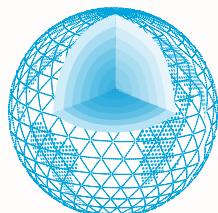


### Santé sécurisée et interopérable

Un dossier médical vraiment sécurisé dont on garde seul le contrôle, disposant d'informations certifiées par des praticiens certifiés - plus besoin de se souvenir de tout ni d'avoir peur des erreurs médicales



# Technologies et Avantages compétitifs



 **UNIRIS**  
Blockchain

## La Blockchain la plus scalable, la plus sûre et la moins consommatrice en énergie grâce au consensus ARCHE

La Blockchain représente pour la première fois dans l'histoire, une technologie capable de fonctionner sans organe central de décision. Un système non seulement impartial, mais aussi transparent et inaliénable. Le Consensus ARCHE créé par Uniris permet à partir d'une élection imprédictible de n'utiliser qu'une infime partie des noeuds (mineurs) pour valider et stocker les transactions (197 pour 100000 noeuds) - de la même façon, par l'intermédiaire de la multidiffusion supervisée chaque noeud saura en permanence où chercher les données par le chemin réseau le plus efficace, permettant ainsi une augmentation linéaire du nombre de transactions/sec en fonction du nombre de noeuds du réseau (~100x). Le tableau ci-dessous présente les principales différences avec les autres Blockchain :

	temps validation	tx/sec	Consommation	sécurité	Priviléges	Sécurité des données	Modèle de transaction	Global	P2P
Bitcoin (POW)	10 min	7	420 000 Wh/txn	51 %	non	partout	UTXO	oui	Gossip
Ethereum 1 (POW)	15 sec	20	36 000 Wh/txn	51 %	non	partout	Compte	oui	Gossip
Ethereum 2 (POS)	15 sec	15000	360 Wh/txn	66 %	oui	fragmenté par groupe de transaction	Compte	oui	Gossip
EOS (dPOS)	0,5 sec	3996	7 Wh/txn	66 %	oui	fragmenté par blockchains	Compte	fragmenté	Gossip
Tezos (dBFT)	1 min	40	-	66 %	oui	partout	UTXO	oui	Gossip
HashGraph (DAG)	5 sec	10	-	66 %	non	fragmenté aléatoirement	UTXO	non	Gossip
Stellar (FBA)	5 sec	1000	-	Quorum	oui	partout	Compte	oui	Gossip
Zilliqa (POW + pBFT)	2 min	2828	-	66 %	non	fragmenté aléatoirement	Compte	oui	Gossip
Hyperledger (BFT / CFT / Kafka)	35 sec	20000	-	66 %	oui	partout	UTXO/Compte	non (privé)	Gossip
Libra (BFT)	10 sec	1000	-	66 %	oui	partout	Compte	oui	Gossip
Harmony (POS + FBFT)	1,36s	10 Millions	-	66 %	oui	frag. aléatoirement sécurisé	Compte	oui	Gossip (UDP QUIC)
<b>UNIRIS (ARCHE)</b>	<b>5 sec.</b>	<b>Illimité</b>	<b>0,00001167 Wh/txn</b>	<b>97,5 %</b>	<b>non</b>	<b>frag. heuristique et geo sécurisé</b>	<b>UTXO</b>	<b>oui</b>	<b>Multicast Supervisé</b>

## Smart-contracts : les robots autonomes de l'ère numérique

Les smart-contracts (contrats intelligents) sont dans l'informatique ce que sont les robots dans la vie réelle : ils exécutent des actions en fonction d'événements. Les smart-contracts Uniris franchissent un saut technologique. Autonomes, ils peuvent se déclencher seuls à partir d'événements internes (dates, transactions) ou de la vie réelle (vérifiés par consensus et croisement d'information : la chaîne Oracle) comme par exemple la météo, le cours de la bourse, les informations. Ils s'adaptent en fonction de leur environnement. Entièrement modifiables, ils sont nativement capables de gérer des opérations – gestion de stocks, paiements, hébergement ... - sans créer de réalité en dehors des transactions confirmées (UTXO).



	type de langage	modifiable	déclenchable	Oracle	Stocks & jetons non financiers	contraintes héritées	Délégation / Multi-Propriétaires
Bitcoin	Interprété	non	externe	externe	non	non	non
Ethereum	compilé (aveugle)	limité	externe	externe	requiert code	non	requiert code
EOS	compilé (aveugle)	limité	externe	externe	requiert code	non	protocole
Tezos	Interprété	non	externe	externe	requiert code	non	requiert code
HashGraph	compilé (aveugle)	limité	externe	externe	requiert code	non	requiert code
Stellar	sans code (tx & multisig)	non	externe	externe	natif	non	multisig
Zilliqa	Interprété / compilé	non	externe	externe	requiert code	non	requiert code
Hyperledger	Interprété / compilé	natif	externe	externe	requiert code	non	requiert code
Libra	compilé (aveugle)	non	externe	externe	requiert code	non	requiert code
Harmony	compilé (aveugle)	non	externe	externe	requiert code	non	requiert code
<b>UNIRIS</b>	<b>Interprété</b>	<b>natif</b>	<b>natif (interne)</b>	<b>interne</b>	<b>natif</b>	<b>oui</b>	<b>native sur chaque transaction</b>

## Une identité décentralisée respectueuse de notre vie privée

L'identité décentralisée évite de confier son identité à un tiers qui pourrait se trouver en conflit d'intérêts et l'exploiter à notre insu, comme Google, Facebook ou son site marchand préféré. Son détenteur en conserve seul le contrôle, elle est stockée sur une multitude de noeuds , ce qui en assure la pérennité et l'intégrité, même si un noeud disparaît. Cette identité décentralisée est ainsi garante du respect de la vie privée et de son interopérabilité avec le reste des applications. Couplée avec les possibilités offertes par les smart-contracts, elle devient un élément central de nos interactions avec le monde : Accès aux grandes manifestations publiques (JO, concerts ...), aux transports, aux hôtels, à nos messages, sans jamais avoir à dévoiler les détails de notre identité.



## La fin des mots de passe et des supports inutiles

Imbriquée à la blockchain, la technologie biométrique apportée par Uniris permet à n'importe qui de s'identifier sans peine, sans stocker aucune donnée biométrique. Il s'agit d'un contrôle d'accès infalsifiable et sans divulgation. Comment ça marche ?

Les données biométriques de l'intérieur d'un de nos doigts vont générer plusieurs clés cryptographiques qui ne seront jamais dévoilées, et à partir desquelles notre identité numérique sera chiffrée. Seule la personne capable de régénérer une de ces clés pourra déchiffrer son identité numérique et ainsi prouver son identité. Au-delà de l'élégance technologique capable de généraliser la biométrie sans risque pour nos vies privées, cette méthode permet de résoudre le problème majeur des Blockchain qui est l'adoption massive.

	stockage des données biométriques	RGPD	Sensible aux attaques logicielles	Méthode d'identification	Biométrie falsifiable	Apprentissage morphologique	Échelle d'identification
Biométrie Smartphone (iOS, Android ...)	oui local	local	oui	seuil	oui	non	100 000
Biométrie industrielle/Défense (Idemia, Fujitsu ...)	oui (serveurs)	local	oui	seuil	oui	non	100 000
<b>Biométrie UNIRIS</b>	<b>non</b>	<b>Global</b>	<b>non</b>	<b>crypto-biométrie</b>	<b>non</b>	<b>oui</b>	<b>Humanité</b>

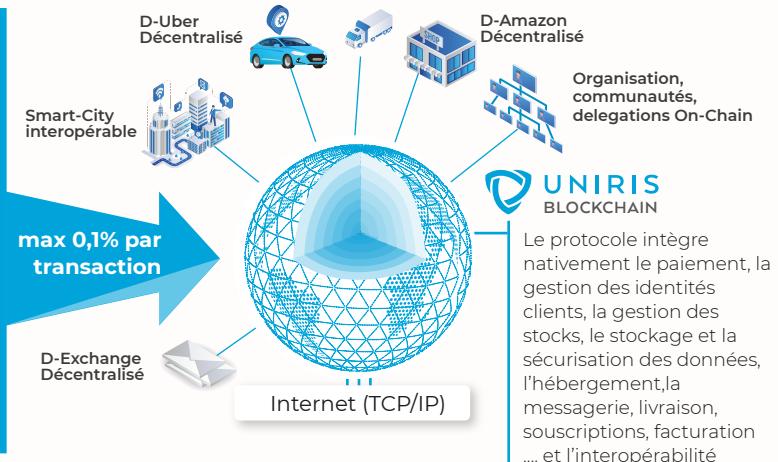
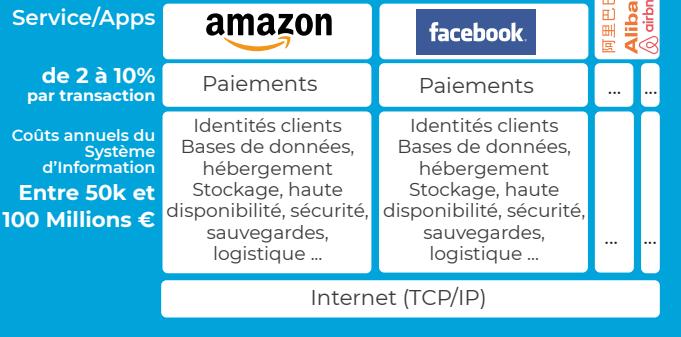


# Un marché quasiment illimité

## La rivière choisit toujours le chemin le plus efficace

La révolution de la confiance va libérer une nouvelle génération de services

### Méthode traditionnelle (en silo)



Dans le modèle pré-historique du web (il n'en est qu'aux toutes origines encore), chaque nouveau service recrée à chaque fois ses briques de fonctionnement élémentaires : portail, identification des clients, bases de données clients, gestion des services, hébergement, stockage, sauvegardes, paiements. Amazon, Facebook, Google et les autres ne partagent rien, avec pour principales conséquences :

- Une consommation de serveurs informatiques abyssale
- Une forêt de logins / mots de passe effarante pour les utilisateurs
- Des risques de fraude, voire de cyberattaque qui font trembler la planète

Le modèle de la Blockchain + Identité Décentralisée permet enfin de rationaliser cette spirale infernale en intégrant directement toutes les couches nécessaires à la création de nouveaux services.

Nécessité de bien moindres capacités informatiques grâce à l'intégration en amont :

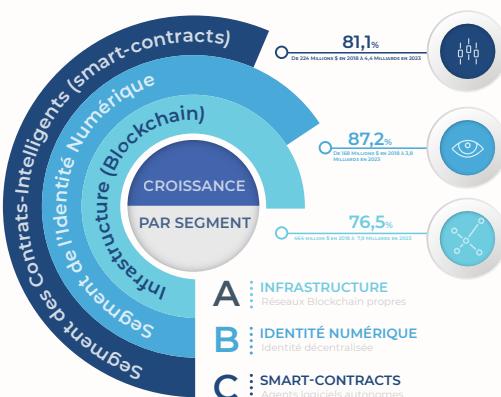
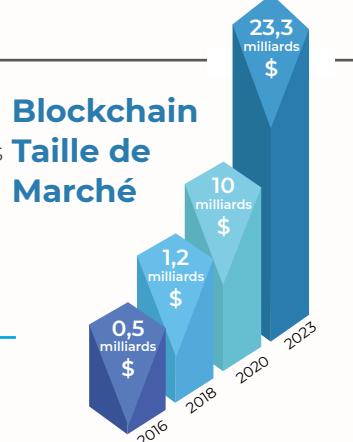
- Identité unique et universelle, activable par le seul détenteur, quel que soit son lieu physique ou virtuel de visite
- Effacement des tiers au profit de la blockchain pour assurer la pérennité du système
- Impact économique et financier majeur sur le coût de chaque nouveau service.

### Études de marché

#### Un marché mondialisé avec une croissance de 80,2% entre 2018 et 2023

Le marché de la Blockchain est estimé en hypothèse conservative à 23 milliards de dollars d'ici à 2023 contre 1,2 milliard en 2018 avec un taux de croissance annuel impressionnant de 80,2% entre 2018 et 2023.

Cette statistique incrémentale ne prend pas en compte le possible remplacement des plates-formes de service et d'application actuelles, hypothèse pourtant crédible.



#### Croissance et taille de marché par segment

Les 3 segments de marché considérés comme les plus porteurs d'ici à 2023 sont l'identité numérique, les smart-contracts et les infrastructures (Blockchain) - segments sur lesquels Uniris dispose des technologies les plus abouties.

#### Une croissance sur tous les continents

##### Amérique du Nord

Parts de marché : 40,7%

Croissance 2023 : 72,1%

##### Amérique Latine

Parts de marché : 3,8%

Croissance 2023 : 83,1%

##### Europe Russie

Parts de marché : 30,2%

Croissance 2023 : 82,1%

##### Asie Pacifique

Parts de marché : 18%

Croissance 2023 : 90,3%

##### Afrique Moyen-Orient

Parts de marché : 7,4%

Croissance 2023 : 84,5%

Une équipe particulièrement bien positionnée sur les marchés Europe et Asie Pacifique

# Le Uniris Coin (UCO)

## Une cryptomonnaie programmée pour croître



La nouvelle économie des jetons de cryptomonnaie est basée sur le principe particulièrement sain et universel de l'offre et de la demande de la même façon qu'une matière première telle que l'or ou le diamant. Une cryptomonnaie crée de la valeur sur une plateforme Open Source indépendamment de la société créatrice. Notre stratégie vise d'abord à créer les conditions technologiques pour que les « mineurs » qui accordent leur confiance à notre plateforme créent le plus de valeur possible. Par ailleurs, nous veillons au bon équilibre de l'offre et de la demande.

### ÉQUILIBRE DE L'OFFRE

Limiter l'offre : 10 milliards de UCO et pas un de plus. Si quelqu'un investit dans l'or et que quelqu'un d'autre découvre comment en fabriquer à moindres coûts alors le cours de l'or va chuter, car il y aura alors plus d'offre que de demande. La Blockchain Uniris interdit la création de nouveaux UCO car toute transaction est basée sur l'existence d'une transaction précédente non dépensée (UTXO).

Limiter la distribution : Pour éviter l'effet d'une arrivée massive de UCO sur les marchés d'échange qui pourraient faire baisser le cours par une augmentation subite de l'offre, Uniris met en place un mécanisme de lock-up. À l'exception des UCO achetés en ventes privée (pour partie) et publique, tous les autres UCO sont libérables par tiers sur une période de deux à cinq ans, par exemple, à partir de l'arrivée de nouvelles applications sur le réseau augmentant dans le même temps la demande.

Déflation programmée : au fur et à mesure, la Blockchain Uniris va détruire automatiquement une partie des UCO issus des frais de transaction, créant ainsi un mécanisme de déflation programmée permettant d'augmenter la valeur de chaque UCO (partie grise de la courbe).

### ÉQUILIBRE DE LA DEMANDE

Le deuxième principe est de créer la rareté de la ressource par la demande. Au-delà des dispositifs biométriques qui ne seront disponibles à l'achat qu'en UCO, l'enjeu est de créer une adoption massive de la solution. Notre stratégie s'articule autour de 3 axes (décris en détail sur la Feuille de route ci-après) :

Être la plateforme de référence pour la production de smart-contracts et l'Identité Numérique : Grâce aux fonctionnalités inédites et longtemps attendues des smart-contracts (autonomes, modifiables, Oracle intégré, scalables ...) et intégrant enfin une Identité décentralisée utilisable par n'importe qui - La plate-forme Uniris propulse l'univers des smart-contracts au-delà du monde de la cryptomonnaie.

Démultiplier l'usage en offrant la plateforme la plus simple et la plus évoluée pour la création de services À l'image d'un AppStore qui permet de démultiplier le nombre de services sur le réseau, l'objectif d'Uniris n'est pas de déployer les différentes verticales applicatives, mais de créer l'écosystème qui permet de faciliter et d'accompagner l'arrivée de toutes ces applications. Le réseau apportera ainsi, fonctionnalité après fonctionnalité, toutes les briques nécessaires au remplacement des applications existantes (Feuille de route)

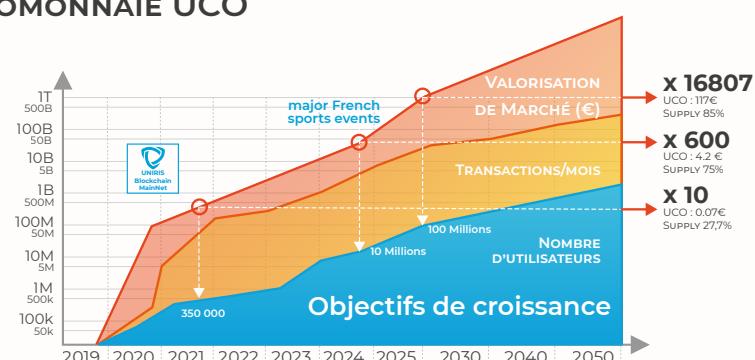
Le Monde au bout des doigts : L'objectif final du projet est de généraliser à l'échelle de la population mondiale l'identification biométrique (ou dérivés) à partir d'un réseau 100% ouvert et transparent capable enfin de prouver la confiance. De l'ouverture des portes de votre maison ou voiture, en passant par l'ensemble des mécanismes d'échanges (financier, communications) jusqu'aux votes.

### HYPOTHÈSES DE CROISSANCE DE LA CRYPTOMONNAIE UCO

La méthode actuelle la plus adaptée pour évaluer la valeur d'une Blockchain est basée sur la loi de Metcalfe qui met en relation la valeur du réseau et le nombre d'utilisateurs. Beaucoup de recherches ont été faites sur le sujet de l'évaluation des cryptomonnaies à l'aide de la loi de Metcalfe. Différentes variations ont été utilisées pour décrire le prix du Bitcoin et en utilisant les corrélations de Pearson sur la période entre 2010 et 2018, il a été constaté que la valeur du réseau est de l'ordre de :

$$\text{valeur d'une blockchain} \sim n^{1.5}$$

(n représentant le nombre d'utilisateurs)



Cette loi permet ainsi d'obtenir une approximation de la valeur d'un réseau en fonction du nombre d'utilisateurs. Par exemple, en considérant un événement tel que les Jeux Olympiques Paris 2024, regroupant à lui seul 8 millions de personnes et sachant que le nombre maximum de UCO échangeables sur le marché sur cette période sera de 75% (7,5 milliards de UCO) on obtient alors :

$$(10 millions)^{1.5} = 31,6 \text{ milliards } € \text{ soit une valorisation par UCO disponible de } 31,6 \text{ milliards } / 7,5 \text{ milliards } \sim 4,2 \text{ } € / \text{UCO}$$



# Répartition, Allocations des UCO

## Un modèle privilégiant le partage de valeur

**10 Milliards UCO**

Nombre total maximum de UCO

**0,007 €/UCO**

Prix initial ICO/IEO

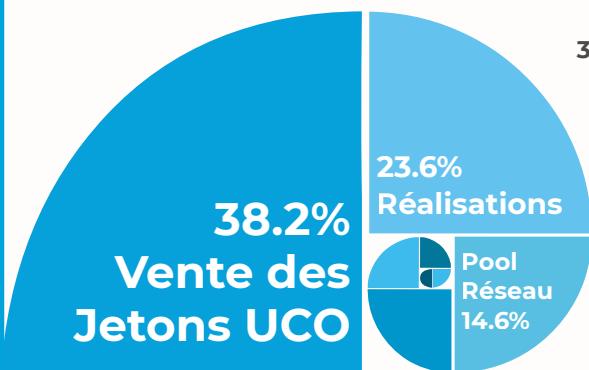
**25,1 Millions €**

Capitalisation de marché initiale

**UCO**

Uniris Coin : Jetons de cryptomonnaie

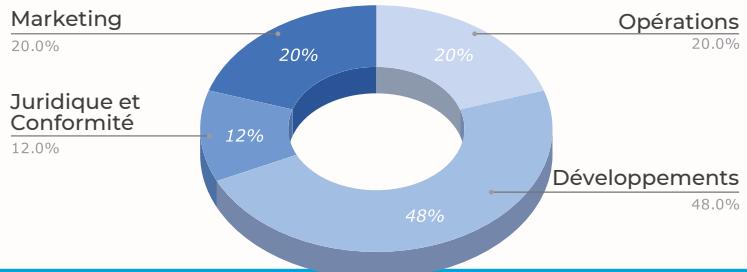
### Répartition des UCO



- 38.2%** Financement Vente de jetons UCO
- 23.6%** Réalisations
- 14.6%** Réserve réseau
- 9%** Améliorations
- 5.6%** Équipe
- 3.4%** Pf Echange
- 3.4%** Marketing
- 2.2%** Fondation

### Allocation des fonds

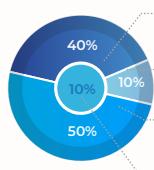
Les ventes privée et publique ont pour but de collecter des fonds pour développer le réseau et les innovations publiées dans les livres jaunes. Le schéma ci-contre représente la répartition fonctionnelle des fonds collectés.



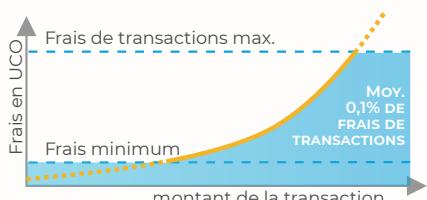
### Des Mineurs reconnus et justement récompensés



Plus besoin de bottes et de casque de chantier ! Le minage et la preuve de travail sur le réseau Uniris ne sont plus basés sur la puissance de calcul et l'énergie électrique dépensée, mais sur une vérification cryptographique permettant de valider et de sécuriser l'origine d'une transaction (dispositifs biométriques, smartphones, clés hardware ou software ...). Conséquence directe du consensus ARCHE, seuls 295 mineurs sont nécessaires pour offrir la puissance de calcul du réseau Bitcoin qui compte ~ 100 000 mineurs.



- Noeuds de cross-validation**  
Noeuds élus pour vérifier les calculs du noeud coordinateur
- Noeud coordinateur**  
Nœud en charge de coordonner la validation de la transaction
- Noeuds de stockage**  
Nœuds à partir desquels les précédentes transactions ont été téléchargées
- Charges du réseau**  
Modules des chaînes Oracle, de balisage ou de prédiction, incitations géographiques et Token Burn (destruction d'une partie des UCO). Le montant est prélevé sur les frais de minage au moment de la récupération des fonds des mineurs évitant ainsi tout point de contention sur la validation des transactions.



Les frais sont calculés en fonction des coûts réels du réseau (taille, complexité ...). Les frais maximum et minimum sont définis par l'intermédiaire de la chaîne Oracle qui est capable d'ajuster ces deux limites en fonction des coûts de l'électricité ou de la valeur de marché de la cryptomonnaie UCO - permettant ainsi de pérenniser le modèle financier aussi bien pour les mineurs que pour les utilisateurs.

Le nombre de jetons UCO, la valeur initiale du UCO ainsi que la capitalisation de marché sont initialisés en fonction des moyens nécessaires à la mise en oeuvre du réseau l'écosystème en fonction des hypothèses de croissance et des priorités du projet. Sur l'ICO Uniris (Initial Coin Offering : Offre initiale de jetons), deux acteurs ont été privilégiés :

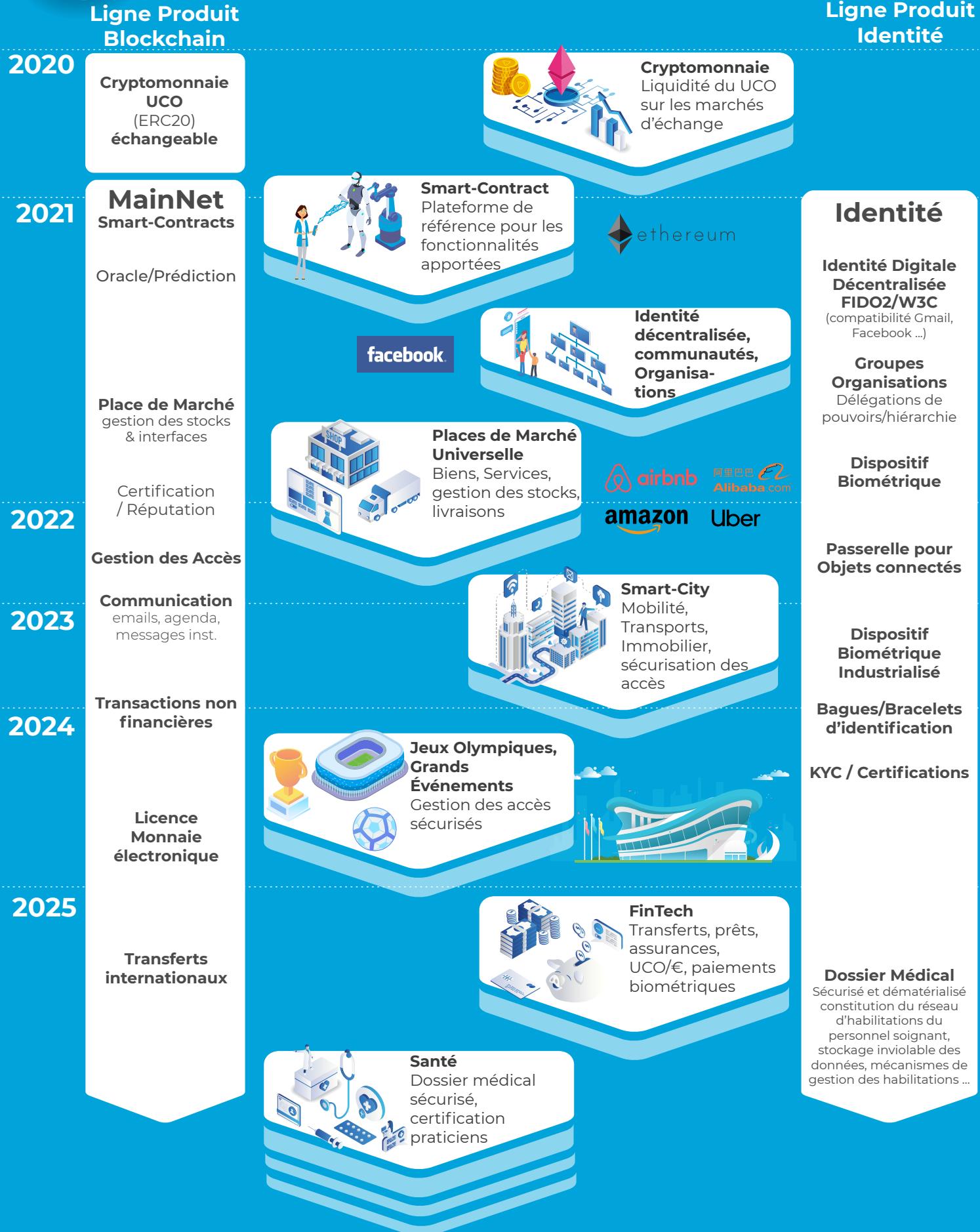
- **les investisseurs précoces** : la quasi-exclusivité des jetons disponibles les deux premières années seront ceux issus de l'ICO.
- **Les contributeurs mobilisés jusqu'à la livraison de l'écosystème** (10% des tokens à la livraison du code et 90% après le déploiement effectif et fonctionnel des fonctionnalités.

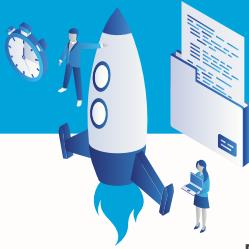
À l'exception des jetons vendus, les autres jetons Uniris (UCO) seront délivrables à hauteur de 20-33%/an sur une période de 2 à 5 ans. Les 14,6% de la réserve réseau seront utilisés pour garantir une incitation financière favorable aux mineurs en attendant la période d'auto-financement. Enfin, les 9% alloués aux Améliorations seront utilisés pour développer de nouveaux cas d'utilisation, mais ne pourront être vendus que lorsque la valeur unitaire d'un UCO sera supérieure à 100x la valeur initiale (soit 0,7€/UCO).



# Feuille de route

Le réseau Uniris, la brique essentielle et le catalyseur pour la création d'un Nouveau Monde de Services à confiance prouvée, interopérables, accessibles et contrôlés par tous.





# L'Équipe !

Créée en 2017, à l'issue des 2 premières années de recherche fondamentale, par Sébastien, Nilesh et Christophe, la société UNIRIS SAS est détenue pour partie par l'**École Polytechnique (Paris Saclay)**, financé par **BPI France** et des Investisseurs de la **smart-city** à hauteur d'un million d'euros. À l'issue de l'ICO (vente publique de la cryptomonnaie UCO) une entité sera créée sous forme d'association pour organiser la communauté autour d'événements pour, d'ici à 2025, laisser la Blockchain Publique voler de ses propres ailes.

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

Ces derniers mois nous ont permis de développer une partie des modules de la Blockchain ainsi qu'un prototype du dispositif biométrique ce qui nous a permis d'être certifiés par le Comité Stratégique de Filière Industries de Sécurité dans le cadre du contrôle d'accès pour l'ensemble des événements sportifs internationaux jusqu'en 2025 !

Notre équipe est un mélange unique de personnalités complémentaires, soudées et expérimentées provenant d'entreprises comme Thales, Mastercard, Barclays, Orange, Mozilla, Google, PwC et de chercheurs de l'École Polytechnique/ CNRS. Nous nous connaissons pour la plupart bien avant la création du projet, professionnellement ou personnellement, ce qui nous a permis de gagner un temps considérable dans la mise en place de chacune des briques de la solution.

## Executive Team



**Sébastien CEO & Co-Founder**

Précédemment responsable de 2 des plus grands projets Orange : Identité (100M d'utilisateurs) et Mobile Banking en Afrique (CA de 10M à 4 milliards €) - Expert en Cyber-sécurité Thales - Conférencier Blockchain (depuis 2013)



**Nilesh COO & Co-Founder**

ex-CTO PAYBACK, Responsable du Développement Logiciel et Support pour les Plateformes de Paiement MasterCard, Chef Opérateur des Paiements Numériques Barclays.



**Christophe CSO & Co-Founder**

Ex-Forces Spéciales - Responsable sécurité Technip (Niger), consultant sureté RGPD.



**Samuel Architecte Blockchain**

Architecte Logiciel et développeur Ethereum (Identité, ICO ...) Michelin/Viseo/Deloitte



**Akshay R&D Maths**

École Polytechnique - Chercheur en mathématiques associés à la Blockchain et la Biométrie



**Virginie Community Manager**

Responsable de Gestion de Contenus Web et Communautés pour le Groupe Gueudet - Edition



**Victor CBizDevo**

Coordinateur/BizDev CryptoMondays & Chain Accelerator - MIT BlockChain Biz Innov&Apps

## Conseillers des boards technologiques, stratégiques et communication



**Bernadette**

Directrice de recherche CNRS/ École polytechnique, spécialiste des systèmes distribués - Prix de l'Académie des Sciences



**Anne**

Administratrice Orange, holding Peugeot, Pernod-Ricard et Imprimerie Nationale - ex Directrice Exécutive Innovation Cisco - Fondatrice Mantis



**Gilles**

Evangéliste Open Source & Blockchain - Expert en cryptographie quantique (ID Quantique / WiPro)



**Peter**

Ex-CMO de Mozilla, Google - Construction de la communauté Open Source



**Camille & Valentin**

(Othello) Experts en Sciences comportementales & communication - Préparation Media



**Baptiste**

Économie & partenariats Mata Capital tokenisation des opérations d'investissement immobilier

Un grand merci à tous ceux qui nous ont accompagnés depuis le début de l'aventure : toute l'équipe des programmes HEC Challenge+, l'accélérateur de l'École Polytechnique X-UP, le Founders Program de StationF, le GICAT, le CEPS, Cap Gemini, nos investisseurs sans qui tout cela n'aurait pas été possible : Stéphane, Frédéric, la BPI et tous nos investisseurs de la vente privée. Un grand merci également et toutes les personnes, ambassadeurs, conseillers qui ont permis d'affiner aussi bien la dimension technologique qu'humaine du projet.

## Partenaires

Les partenariats Uniris sont axés sur l'innovation et la croissance communautaire. Les instituts de recherche nous donnent accès aux technologies de pointe et à la validation de nos innovations.



**STATION F**

**GICAT**



# La Révolution Technologique sous-jacente



## Économie conçue pour croître

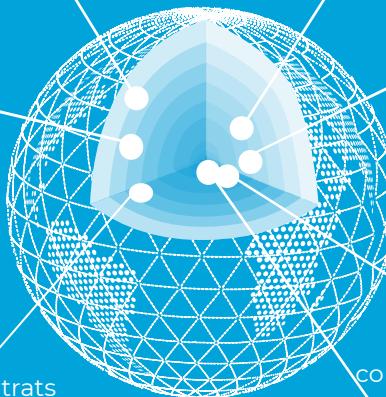
La cryptomonnaie pré-minée est conçue pour une utilisation à grande échelle et donc une adoption massive. Le modèle économique prévoit une destruction de monnaie automatisée permettant mécaniquement de favoriser les premiers investisseurs par une déflation programmée.

## Adaptée pour toutes les Apps

Notre écosystème est conçu pour améliorer toutes les applications actuelles (sites marchands, votes, accès aux Jeux Olympiques et même l'hébergement de sites Web) par des contrats intelligents modifiables, autonomes, autodéclenchables et disposant d'une fiabilité à toute épreuve.

## Gouvernance Durable

Grâce aux identités décentralisées et aux contrats intelligents, une gouvernance enfin équilibrée va pouvoir être assurée par toutes les parties (Utilisateurs, Mineurs, Investisseurs, développeurs et fournisseurs d'applications). Le code source et les 12 brevets sont détenus par la communauté pour fournir l'équilibre parfait entre le cercle vertueux de l'Open Source et la protection contre les bifurcations (forks) permettant au réseau de croître et de survivre pendant des siècles.



## Identité Décentralisée

Le lien manquant entre les humains et les nouvelles technologies, Uniris fournit la première authentification biométrique inviolable et sans aucun stockage de clé tout en assurant les dernières normes d'authentification W3C.

## Données Géo-Sécurisées

Le réseau Uniris peut survivre à n'importe quelle catastrophe grâce à ses algorithmes de réplication heuristique, ses coordonnées géographiques et réseaux, ses chaînes de balises, ses oracles et son module de prédition.

## Consensus Incassable

Le consensus ARCHE (Heuristic Rotating Atomic Commitment) augmente considérablement la sécurité et la confiance du réseau (critères de sûreté de l'aéronautique)

## Réseau P2P illimité

Réseau sans permission et sans mineurs privilégiés basé sur un nouveau protocole P2P "Multidiffusion Supervisée" éliminant tous les points de contentions goulots d'étranglement du réseau.

# La Blockchain UNIRIS

## Taillée pour une utilisation planétaire



### Un Réseau réellement décentralisé et sans limites

Compte tenu des contraintes matérielles et physiques universelles, des milliards de transactions ne peuvent pas être intégrées dans une seule chaîne de bloc. De la même façon, quelle que soit la méthode de consensus, il est impossible d'assurer un consensus sur des milliards de transactions en interrogeant tous les noeuds du réseau. Enfin, compte tenu du fonctionnement des réseaux distribués (P2P) il n'est pas possible de garantir la fraîcheur (consistance) d'une donnée sur un réseau asynchrone, sauf comme dans le cas du réseau Bitcoin en ralentissant significativement le réseau par l'intermédiaire du calcul du nonce d'un bloc dans la preuve-de-travail. Uniris a résolu ces problèmes, de la façon suivante :

**Infinité de Chaînes de transactions vs. une chaîne de blocs** au lieu de blocs de transactions chaînées, chaque bloc est réduit en sa version atomique, c'est-à-dire que chaque bloc ne contient qu'une seule transaction, chaque transaction dispose de sa propre chaîne.

**Consensus ARCHE : le consensus absolu** est une nouvelle génération de Consensus « Atomic Rotating Commitment Heuristic (ARCH ou ARCHE) » en français « Validation Atomique obtenue par élection heuristique tournante » - en décomposant chacune des notions :

**Validation Atomique** (Atomic Commitment) est la forme de Consensus « absolue » qui implique 100% de réponses concordantes et positives ou le refus de la validation de la transaction.

**Heuristique** est l'ensemble des algorithmes, des logiciels et des paramètres qui gèrent l'intégralité du réseau permettant par exemple au réseau d'élire de façon décentralisée et coordonnée les noeuds en charge de la validation et du stockage des chaînes de transactions.

**Rotating** le réseau étant entièrement distribué (aucun rôle central ou privilégié), les noeuds élus pour chaque opération changent en permanence de sorte qu'aucun noeud ne peut prédire avant l'arrivée de la transaction quels noeuds seront élus.

**Système de Réplication Prédictif, Optimisé, Geo-sécurisé capable de s'auto-réparer** au lieu de synchroniser les transactions de façon désorganisée sur l'ensemble du réseau, chaque chaîne de transactions sera stockée de façon reproducible et ordonnée sur un ensemble de noeuds - ainsi chaque noeud, de façon autonome, connaîtra l'ensemble des noeuds hébergeant une transaction donnée et pourra ainsi soulager le réseau en interrogeant uniquement les noeuds « élus » les plus proches. L'élection des noeuds stockage intègre la position géographique permettant d'assurer une sécurité des données même en cas de désastre sur une ou plusieurs zones géographiques.

**Réseau Distribué (P2P) sans point de saturation** Basé sur la Multidiffusion Supervisée, le réseau de pair-à-pair utilise un mécanisme d'auto-découverte basé sur les connexions entrantes et le mécanisme des chaînes de transaction du réseau pour maintenir une vision qualifiable et de confiance en générant un minimum de nouvelles transactions.

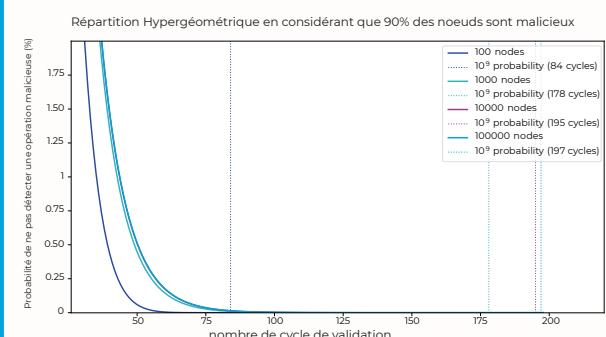
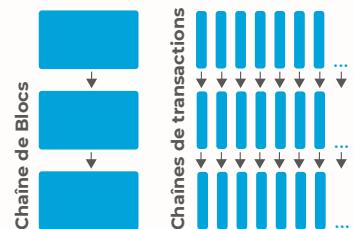
**Chaînes de balisage (Beacons Chains)** Aucun noeud n'ayant la capacité physique de connaître l'état de chaque transaction dans un réseau illimité, le réseau Uniris utilise un jeu de chaînes de transactions spécifiques contenant chacune un sous-ensemble des adresses des dernières transactions pour une date donnée, permettant, par exemple, à n'importe quel noeud de se resynchroniser automatiquement en cas de déconnexion.

**Chaînes Oracle** Les chaînes Oracle "État du Monde" sont mises à jour par Consensus à chaque mise à jour d'une information (par exemple à la diffusion d'un nouveau bulletin météorologique, informations, bourse ...)

**Module de Prédiction** Pour permettre à un réseau décentralisé de survivre à des siècles, il doit pouvoir s'adapter aux menaces et réagir en conséquence. Pour cela le réseau Uniris dispose d'un module de prédiction capable de faire le lien entre une perturbation du réseau (ex. indisponibilité des noeuds sur une zone géographique) et un événement (ex. Orage sur cette zone via Oracle)

**Minage, Preuve de travail & Consommation d'énergie** L'élection des noeuds et la synchronisation du réseau étant assuré par les Algorythme Heuristiques, la preuve de travail est utilisée pour vérifier que les noeuds à l'origine de la validation et que le dispositif à l'origine de la transaction sont bien autorisés (p.ex dispositif biométrique) permettant ainsi de compléter l'authentification par son contexte (p.ex. vote électronique nécessitant l'identité réelle d'un votant). L'élection aléatoire des noeuds n'étant plus liée à la dépense d'énergie, la consommation du réseau est ainsi divisée par 3,6 milliards par rapport au réseau Bitcoin.

Chacun de ces aspects est expliqué en détail dans le Yellow Paper : <https://uniris.io/Yellow-Paper-FR.pdf>



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

Le réseau Uniris s'appuie sur les propriétés des lois de répartition hypergéométrique qui à partir d'une élection imprévisible et d'un consensus formel permet d'obtenir avec certitude (99,9999999%) la même réponse en interrogeant 197 noeuds qu'en interrogeant 100000. En d'autres termes, cette loi mathématique permet d'obtenir un consensus formel global à partir d'une infime partie des noeuds - cette propriété entre ainsi dans la notion Heuristique largement utilisée sur l'ensemble du réseau. Le risque sur la disponibilité associée est assuré par une gestion stricte des noeuds perturbateurs qui après investigation sur l'origine du désaccord bannira tout noeud perturbateur.





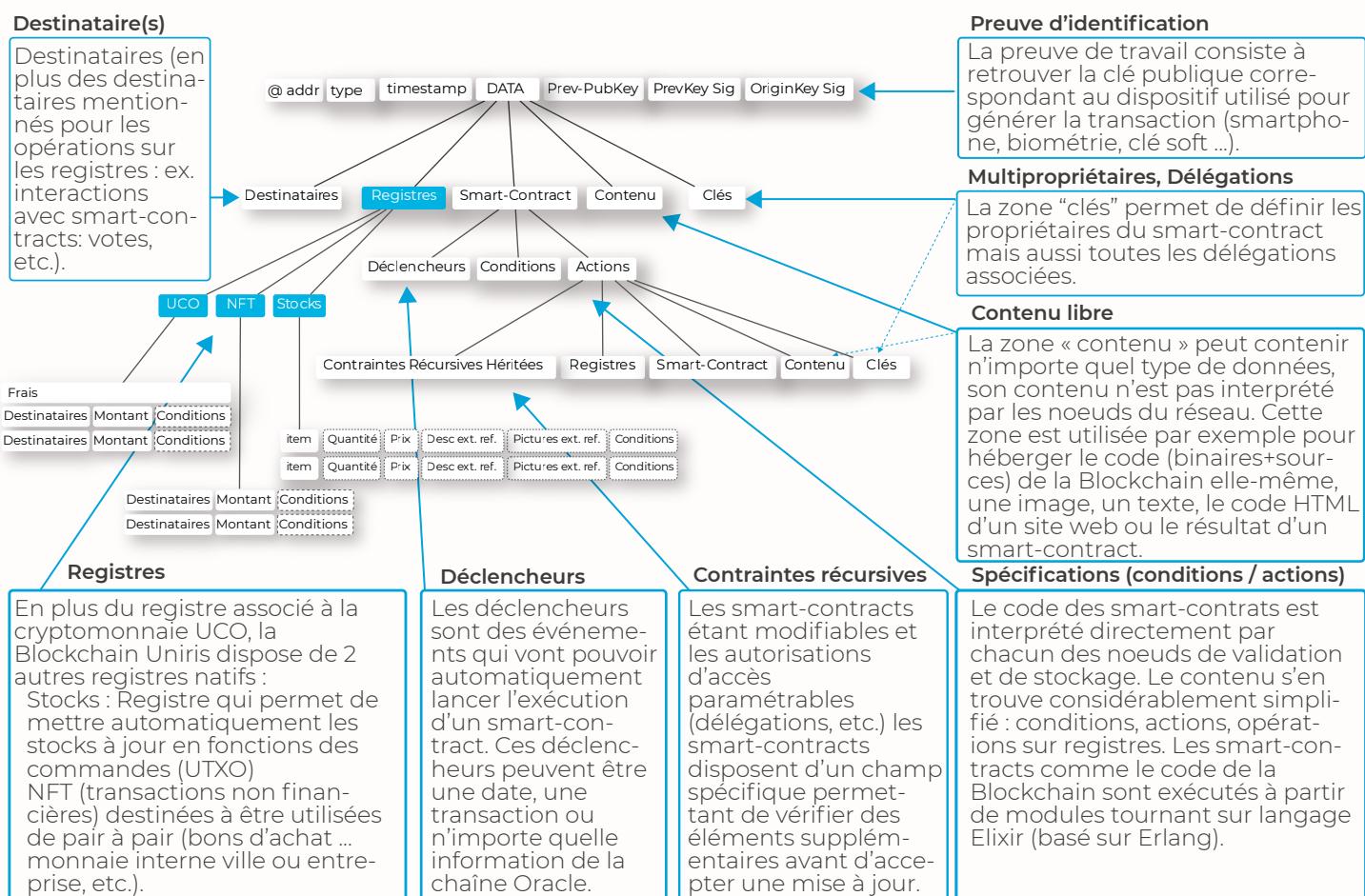
# Smart-Contracts

Conçus pour améliorer n'importe quel service

D'abord créée par le réseau Bitcoin pour la mise à jour d'un registre partagé, puis renforcée par la possibilité d'effectuer des actions programmées grâce à des contrats intelligents et jusqu'à la capacité d'exploiter des systèmes complets, la technologie Blockchain ne cesse de se réinventer. Contrairement aux smart-contracts compilés sur Ethereum, les smart-contract sur le réseau Uniris sont directement interprétés par les mineurs. Chaque transaction ou smart-contract étant stocké sur un groupe de noeuds spécifique (élection tournante heuristique ARCHE) ils peuvent alors prendre en charge de façon synchrone un ensemble de nouvelles fonctionnalités : par exemple connaître l'état du stock, le nombre de votes et les transactions à destination de ce même smart-contract (toute transaction à destination d'un smart-contract est notifiée et stockée sur le groupe de noeuds associé) ou encore déclencher automatiquement une action à l'arrivée d'un événement (date, météo, etc.) permettant ainsi de supporter n'importe quel cas d'utilisation réelle.

Pour assurer une sécurité et une irrévocabilité des smart-contracts, ceux-ci sont entièrement basés sur le modèle UTXO (sortie de transaction non dépensée) qui peut être dépensée/utilisée comme une entrée dans une nouvelle transaction. En d'autres termes les smart-contract ne sont pas dépendants de l'état d'une base de données interne, mais uniquement des transactions déjà validées.

Qu'il s'agisse d'un simple transfert, d'une règle d'accès à un bâtiment, d'une boutique en ligne, de l'hébergement d'un site web, d'un vote à l'échelle d'un pays ou même l'ensemble du code utilisé sur le réseau lui-même, n'importe quelle transaction respecte le schéma suivant :



## Exemple smart-contract pour une place de marché

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

@Alicel : ...
```

Dans le modèle UTXO, les seules références sont les transactions validées, par exemple, pour un site marchand, l'état du stock n'est pas modifié dans le contrat intelligent lui-même, mais est reconstitué à partir des transactions validées. L'expérience d'un utilisateur ou d'un commerçant est absolument identique, mais chaque état est irréfutable et sans ambiguïté.



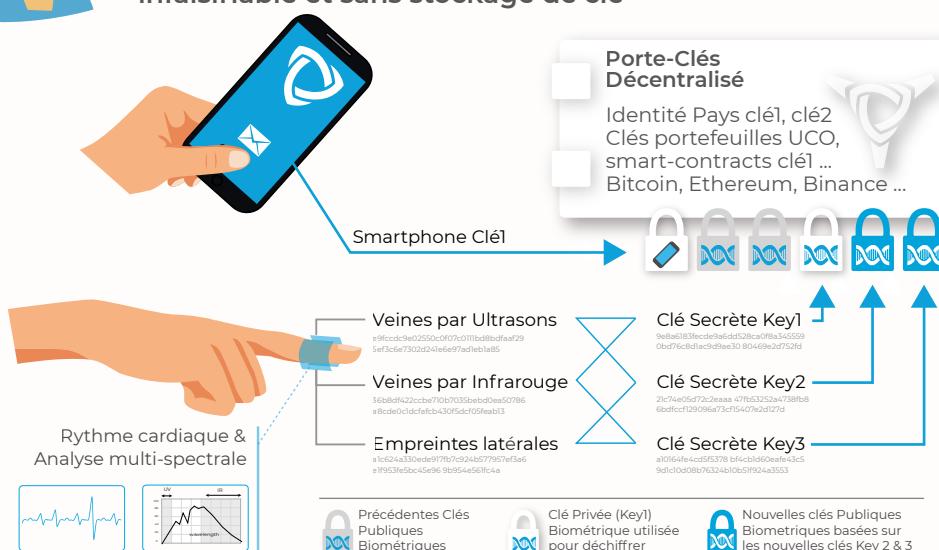
```
{
  "address": "@MyShop2",
  "type": 3,
  "timestamp": 1557131179,
  "DATA": {
    "Ledger": {
      "UCO": [{}],
      "STOCK": [
        {
          "category": "t-shirt",
          "description": "t-shirt eco 200g",
          "price policies": [{"threshold": 10, "policy": "10%"}],
          "vouchers 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": "tws", "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"
  }
}
```



# Identité Décentralisée et Biométrie

## Le Graal de l'adoption massive

Une authentification biométrique de nouvelle génération infalsifiable et sans stockage de clé



### Une authentification qui ne peut pas être utilisée à notre insu

Contrairement aux empreintes, à l'iris, au visage qui peuvent être aisément reproduits et falsifiés à partir d'une photo sur Facebook ou dans la rue - il est impossible de reconstituer l'intérieur doigt - le dispositif vérifie les signes vitaux lors de chaque authentification pour s'assurer que le doigt n'a pas été coupé et que la personne est bien consciente et consentante avant toute validation de transaction.

### Sans stockage de clés

Toutes les identifications biométriques actuelles reposent sur le même principe : • capture de la donnée biométrique et stockage de la donnée de reconnaissance • comparaison de la mesure avec le motif • si la concordance dépasse un certain seuil alors la personne est identifiée (soft)

L'identification par le dispositif biométrique Uniris n'est plus basée sur un seuil de reconnaissance et n'a donc plus besoin d'être stockée pour être comparée. Comme représenté sur la figure ci-contre, les clés privées ou secrètes cryptographiques sont générées à la volée (puis supprimées) ce qui permet à l'utilisateur de récupérer et de déchiffrer son "porte-clé" décentralisé. La tolérance sur l'identification est assurée par le mécanisme d'apprentissage décrit ci-dessus. Enfin l'authentification n'est plus logicielle, mais cryptographique rendant ainsi toute tentative d'attaque logicielle inutile.

### Preuve de l'origine de l'authentification via Preuve-de-travail

L'identification sur le réseau Uniris n'est pas limitée aux dispositifs biométriques et comme représenté dans la figure ci-dessus chaque méthode d'accès (smartphone, clé USB, clé logicielle ...) disposera de sa propre méthode de certification (cf. Yellow Paper Saison1).

La méthode d'identification étant associée à la transaction (cf. schema smart-contract : "OriginKey Sig") et à la preuve de travail elle va ainsi permettre de modular la sécurité associée à n'importe quel smart-contract ou portefeuille - par exemple :

- une transaction de moins de 1000 UCO pourra être réalisée à partir d'un smartphone spécifique et à partir d'un dispositif biométrique au-delà.
- L'entrée dans un bâtiment sensible pourra être effectuée par NFC pendant les heures de bureau et par biométrie au-delà ....

Plus personne ne pourra voler vos clés, vous pourrez les supprimer, mais vous ne pourrez plus les oublier ou les perdre.

- Authentification Inviolable
- Aucun stockage de clés (RGPD)
- Surveillance des signes vitaux
- Apprentissage des évolutions morphologiques
- Conçu pour la population mondiale

### Une authentification de la population mondiale indépendante du dispositif

Contrairement à une identification biométrique sur un smartphone qui ne va fonctionner que sur un seul smartphone - l'authentification Uniris fonctionne pour n'importe quelle personne et sur n'importe quel dispositif. Aucune clé n'étant stockée, elle est alors compatible les réglementations les plus strictes de protection des données (RGPD, CNIL ...) faisant entrer la biométrie dans l'usage à grande échelle.

### Apprentissage automatique tout au long de la vie

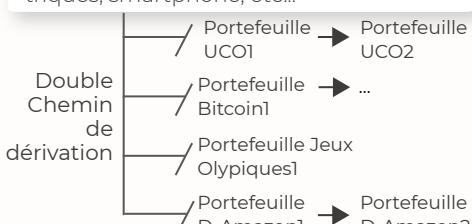
Comme représenté sur la figure ci-dessus, les clés sont générées deux à deux à partir des mesures biométriques. Si une des mesures est différente (coupure, brûlure, etc.) alors une seule clé sera concordante et pourra valider l'authentification et les deux nouvelles clés seront ajoutées pour chiffrer (via clés publiques associées) le porte-clés décentralisé, permettant ainsi d'apprendre les nouvelles mesures biométriques d'une personne sans jamais avoir à en stocker les clés.



### Identité Décentralisée et Interopérable

#### Porte-Cles Décentralisé

Seed (graine) générée aléatoirement et chiffrée avec une clé AES elle-même chiffrée avec les clés publiques biométriques, smartphone, etc...



Techniquement l'identité décentralisée d'une personne ou d'un objet connecté est constituée d'un Seed (clé racine) générée aléatoirement à partir de laquelle sera générée l'ensemble des clés en fonction d'un chemin de dérivation - ainsi pour tout accès à un service ou application une clé sera calculée à la volée à partir d'une clé issue du seed et de la première clé publique associée à un service ou une application - permettant ainsi de créer une infinité d'identités sans même avoir à en stocker les clés - l'ensemble des fonctionnalités associées à cette identité décentralisée seront détaillées dans le Yellow Paper Saison4: Carnets d'adresses automatisés, email, FIDO2

### Roue de la vie privée

Les transactions étant publiques, le réseau dispose d'un mécanisme appelé "Roue de la vie privée" permettant de supprimer les corrélations entre l'émetteur, le destinataire, l'heure et le montant des transactions - Ce mécanisme est notamment utilisé dans le cadre des votes électroniques et permet sans remettre en cause la cohérence des registres à chacun de garder le contrôle de sa vie privée.





# Gouvernance (DAO)

Une Gouvernance qui intègre le meilleur de chacun

## Gouvernance décentralisée On-Chain et Off-Chain

Une DAO (Decentralized Autonomous Organization) est une organisation décentralisée dont les règles de gouvernance sont automatisées et inscrites de façon immuable et transparente dans une blockchain.

La gouvernance est probablement le plus grand défi que les Blockchain doivent relever. Le réseau Bitcoin dispose aujourd'hui du réseau disposant de la gouvernance décentralisée la plus aboutie avec l'expression désormais célèbre «code is law» (Le code est la loi) néanmoins cette gouvernance ne repose que sur un seul type d'acteur «le propriétaire du mineur» ou par extension au plus gros groupe de mineurs - c'est en effet le code installé par la plus grande puissance de calcul et donc les fermes de minage professionnelles qui gouvernent de fait le réseau.



Bien que cette gouvernance soit décentralisée, elle occulte toute une partie de l'écosystème à commencer par les utilisateurs eux-mêmes, les fournisseurs d'applications, les contributeurs techniques et même la Blockchain elle-même contrainte par le code installé sur la plus grande puissance de calcul.

Pour que le réseau puisse survivre dans le temps et s'adapter aux évolutions de la société, la gouvernance de la Blockchain Uniris repose sur plusieurs fondamentaux techniques et fonctionnels :

### Identité décentralisée & preuve d'Identité



Prérequis indispensable à une gouvernance intégrant l'humain : la capacité de l'écosystème à identifier une personne comme unique et à l'intégrer dans un groupe d'acteurs spécifiques.

### Code «On-Chain»



Le code utilisé par les noeuds est hébergé par la Blockchain elle-même, le réseau est ainsi certain que l'ensemble des noeuds appliqueront immédiatement les mises à jour décidées (via modules hot-reload d'Elixir et à partir des informations stockées dans la zone «contenu des smart-contracts») - La Blockchain Uniris est également dotée de la capacité à tester en grandeur réelle l'impact de nouvelles fonctionnalités.

### Smart-Contract modifiables



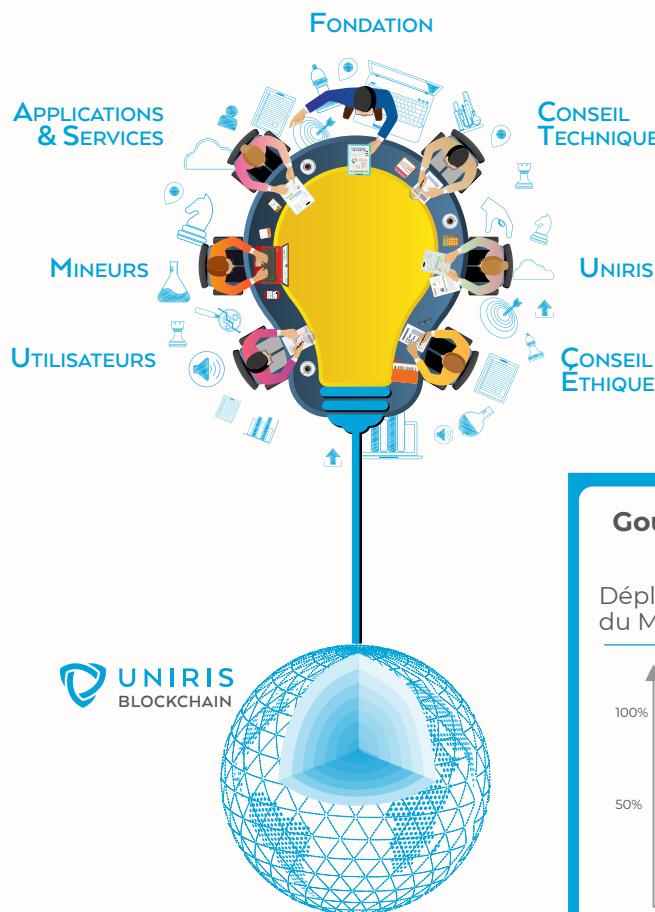
Chaque smart-contract est stocké sous forme de chaîne de transactions spécifique permettant au réseau de versionner (git ...) l'ensemble des mises à jour, mais aussi de contraindre chaque mise à jour selon une gouvernance spécifique (quorum de votes, droit de veto ...).

### Dotation monétaire



Maillon essentiel pour financer le travail associé aux mises à jour, aux nouvelles fonctionnalités et aux contributions le réseau dispose d'une réserve d'un tiers des tokens (avec des contraintes de distribution progressive).

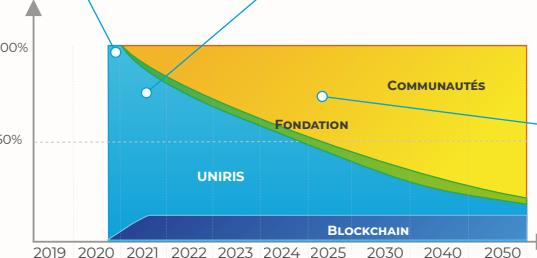
## La gouvernance sur le réseau Uniris s'articule sur 8 groupes distincts :



## Gouvernance par la communauté programmée

### Déploiement du MainNet

Don des brevets à l'OIN (Open Invention Network) une fois le risque de Fork écarté



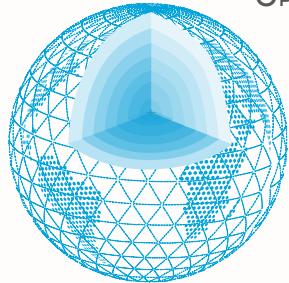
Basculement de la gouvernance vers la communauté une fois chaque partie suffisamment représentée



# Open Innovation

## Créer les conditions d'une généralisation

OPEN GOVERNANCE  
OPEN INNOVATION  
OPEN SOURCE  
NETWORK



UNIRIS  
BLOCKCHAIN

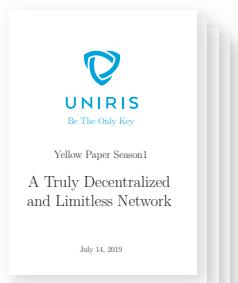
### Uniris, un projet à vocation humanitaire et communautaire

Une fois le risque de fork écarté, l'ensemble des Brevets seront cédés au patrimoine des technologies Open Source, ce patrimoine devrait être très probablement cédé à l'OIN (Open Invention Network), l'ensemble du code source étant en licence AGPL 3.0.

### Une démarche affirmée de pédagogie volontaire, donnant la possibilité à chacun de comprendre la technologie

À mi-chemin entre la publication scientifique et les articles de vulgarisation, la technologie sous-jacente sera décrite en détail dans 5 papiers jaunes (Yellow Paper). Le premier volet, déjà publié, décrit le fonctionnement du réseau (Consensus ARCHE, Multidiffusion Supervisée (p2p) et l'ensemble des mécanismes qui ont permis d'aboutir à un réseau illimité) :  
<https://uniris.io/Yellow-Paper-FR.pdf>

Les volets suivants aborderont successivement : la Programation des applications, la gouvernance ouverte, les briques de fonctionnement de l'identité décentralisée pour finir sur les dispositifs biométriques et leurs dérivés.



### Liste des Brevets

- FR3049089 (A1) **Procédé de validation des transactions relatif à une chaîne de transactions à travers un réseau décentralisé** validations de transactions relatives à une ou plusieurs chaînes de transactions de façon unitaire et asynchrone permettant de supprimer les limites de la technologie blockchain. Le procédé permettant une sécurité et une confidentialité renforcées notamment par l'intégration des contraintes en nombre et en géolocalisation des validations des messages.  
US2019044735  
WO2017162931
- FR3049101 (A1) **Procédé gestion des smart-contracts à travers des chaînes de transactions** Identités digitales - échange de valeurs - gestion des délégations, habilitations et révocations - gestion de votes électroniques - livraison de marchandises - organisations - gestion des données santé - gestion de la réputation et de la certification.
- FR1907901 **Procédé de validation atomique de chaines de transactions à travers un réseau décentralisé** Consensus ARCHE (Validation atomique par élection heuristique tournante), procédé de réplication optimisé et géo-sécurisé - auto réparation du réseau et des données - module de prédiction et la couche réseau Multidiffusion Supervisée (protocole P2P)
- FR3049088 (A1) **Procédé gestion des identités digitales associées à un individu, un objet connecté, une organisation, un service à travers un réseau décentralisé** Identification-authentification-enregistrement d'une identité digitale unique ou non pour un individu ou un objet sur un dispositif externe - échange de valeurs sans divulgation - gestion de conditions - gestion des membres, propriétaires, multisignatures, réputation, certification et réinitialisation relative à une identité digitale - gestion des identifiants externes mutables à travers une identité digitale.
- FR3049087 (A1) **Procédé de sécurisation des transactions par l'intermédiaire de connaissance et de capacités croisées à travers un réseau décentralisé** Procédé cryptographique permettant de croiser les connaissances et les capacités des dispositifs de sorte à interdire toute opération non permise, de renouveler et de déchoir en permanence l'ensemble des clés cryptographiques de l'ensemble des dispositifs, de supprimer les éléments de corrélation temporelle, de valeur, et des acteurs mis en jeux (roue de la vie privée) d'initialiser les clés cryptographiques relatives à un réseau décentralisé sans utiliser de dispositif externe au système, de minimiser l'exposition des clés publiques relatives aux clés privées des dispositifs, de réinitialiser un dispositif et révoquer un utilisateur.
- FR3049086 (A1) **Procédé d'authentification biométrique sans divulgation à travers un réseau décentralisé** un procédé permettant de ne jamais avoir à dévoiler tout ou partie des mesures biométriques d'un individu - intégrant les compensations des mesures biométriques et une adaptabilité tout au long de la vie d'un individu - permettant de ne jamais avoir à stocker une quelconque donnée sur au moins une mesure biométrique ou une clé cryptographique relative à au moins un individu - permettant d'enregistrer plusieurs doigts d'un même individu sans divulgation et permettant de réaliser des opérations sans réseau et sans qu'un individu n'ait jamais utilisé aucun dispositif auparavant.
- FR3049090 (A1) **Dispositif d'authentification biométrique adaptatif par échographie, photographies en lumière visible de contraste et infrarouge, sans divulgation à travers un réseau décentralisé** dispositif d'authentification biométrique sans divulgation à partir d'échographies et photographie du réseau veineux du doigt, de l'empreinte digitale latérale du doigt et configuré pour réaliser une photographie de l'émission intrinsèque infrarouge du doigt, pour vérifier le rythme cardiaque et réaliser une analyse spectrométrie multiférentielle du doigt.
- FR3049121 (A1) **Dispositif de couplage mécanique et électrique permettant de relier un périphérique informatique sans endommager le système hôte**
- FR3049093 (A1) **Dispositif de positionnement reproductible d'au moins un doigt d'un individu lors de la prise de mesures biométriques**
- FR3049085 (A1) **Dispositif de communication permettant de communiquer avec d'autres dispositifs et permettant les transactions à proximité et la création d'un réseau maillé autonome mesh**
- FR3049091 (A1) **Dispositif d'authentification biométrique par échographie ultrasonique et vérification des signes vitaux**
- FR3049092 (A1) **Dispositif d'authentification biométrique et de fiabilisation des mesures par photographie en lumière visible et infrarouge, spectrométrie et analyse différentielles**

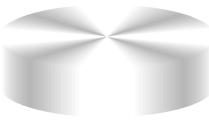


# Vue Globale

## Exemple de transfert de crypto-monnaie

### Porte-clés décentralisés

Contient les clés et les points d'accès des utilisateurs (autres doigts, cartes sécurisées, Objets connectés ...)



Porte-clés Humains, Organisations, Groupes, IoT

### Porte-Clés d'Alice

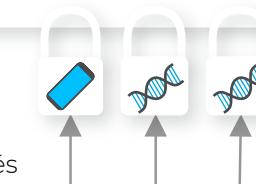
Pays ID clé1, clé2

UCO clé1, clé2

Smart-Contract1 clé1

Clé BitCoin

Clé voiture ...



Chiffré avec les clés publiques d'Alice



Alice récupère ses clés sur son porte-clés décentralisé, génère la transaction de paiement et la transmet à n'importe quel noeud du réseau



@Alice #2  
10 UCO to @Michelle

Noeud Coordinateur  
Heuristique Tournant  
génère la preuve de travail et  
l'estampille de validation

Alice



le Coordinateur et les Contre-Validateurs récupèrent la chaîne d'@Alice, les sorties non dépensées (UTXO) ... en interrogeant les pools de stockage associés

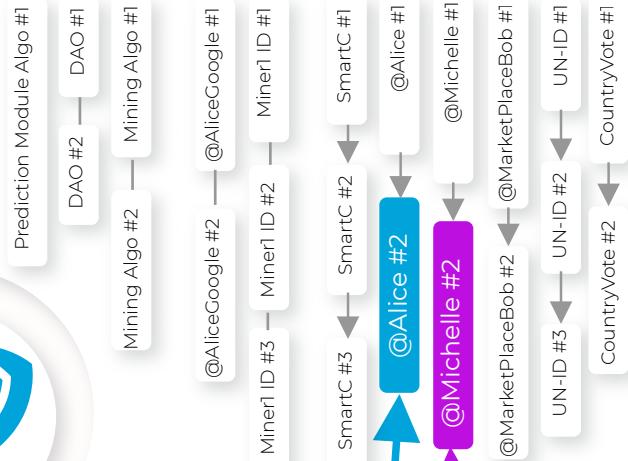
### Smart-contracts & Identités

Contient toutes les données et transactions publiques (chaînes de smart-contracts, des identités décentralisées des noeuds, groupes, organisations, IoT, Individus, etc. ...)

Réseau

Identités

Smart-contracts & Registres



Le pool de Stockage  
Heuristique tournant  
calculé à partir des adresses  
des transactions associées :  
@Alice#2, @Michelle#2,  
noeuds impliqués dans la  
validation et le stockage de  
la transaction

Michelle

Noeuds de Contre-Validation  
Tournants

contre valident l'estampille de  
validation et la preuve de travail