

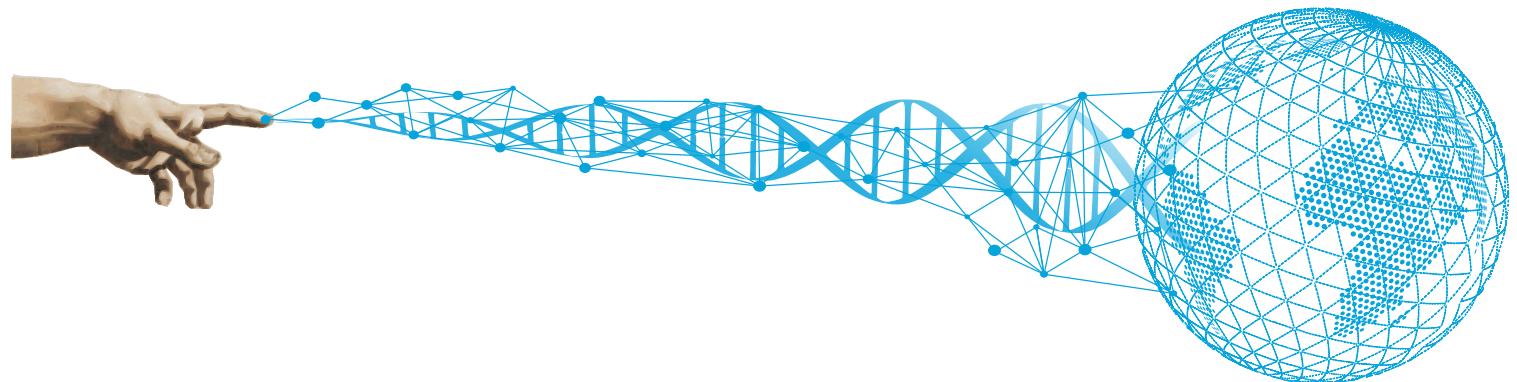


UNIRIS

Белая бумага

Будьте владельцем вашей личности

Декабрь 2019



Что, если технология наконец-то сможет упростить вашу повседневную жизнь, не подвергая риску вашу безопасность? Что, если бы вам сказали, что у вас уже есть эта технология?

Uniris обещает предоставить доступ ко всем технологиям простым прикосновением вашего пальца, защищая вашу личность. Команда Uniris разработала сверх надежную и защищенную от взлома технологию, которая так же безопасна, как и чип банковской карты. Она позволяет заменить любой пароль, ключ или другое устройство аутентификации, просто прочитав его внутри пальца.

Чтобы работать в глобальном человеческом масштабе без контроля или вмешательства любого человека, компании или организации, эта технология "с открытым исходным кодом" основана на новом поколении сеть под названием блокчейн. Для достижения масштабности мы улучшили блокчейн технологии, так что он может заменить любое приложение или сервис: открыть ваш автомобиль или двери дома, идентифицировать себя или платить в Интернете без риска для ваших данных или товаров, всегда иметь вашу медицинскую карту в доступе, но защищенной... Эта технология просто работает с самого первого использования независимо от того, где вы находитесь.

Для функционирования и вознаграждения людей, размещающих сетевой сервер (miner), который проверяет любую транзакцию в блокировке Uniris, блокчейн построен вокруг криптовалюты (UCO в случае с Uniris). Эта валюта создается в начале проекта для финансирования всех девелоперских проектов, что делает каждого инвестора реальным участником строительства Нового Мира с самого первого момента создания.

Присоединяйтесь к нам в качестве инвестора, девелопера, амбассадора и станьте активным строителем будущих глобальных связей.

1	Uniris. Краткий обзор	5
2	Конкурентная среда и преимущества Uniris	6
2.1	Самый масштабируемый, безопасный и энергосберегающий блокчейн, благодаря консенсусу ARCH.	6
2.2	Умные контракты: автономные роботы цифровой эры	7
2.3	Децентрализованная идентичность, уважающая нашу личную жизнь	7
2.4	Конец паролям и ненужным носителям	7
3	Практически неограниченный рынок	9
4	Исследование рынка	10
5	The Uniris Coin - криптовалюта, запрограммированная а рост	11
5.1	Баланс предложения	11
5.2	Баланс спроса	11
5.3	Гипотеза развития криптовалюты UCO	12
6	Раздача токенов и распределение средств	13
6.1	Модель, способствующая разделению ценностей	13
6.2	Распределение средств	13
7	Майнеры и майнинг в сети Uniris	14
8	План развития	15
9	Команда	16
10	Блокчейн Uniris - разработан для глобального использования	18
10.1	По-настоящему децентрализованная и безгранична сеть	18
10.2	Бесконечные цепочки транзакций против цепочки блоков	18
10.3	Консенсус ARCHE: абсолютный консенсус	18
10.4	Прогнозируемая, оптимизированная, гео-безопасная система репликации	18
10.5	Вмешаемая распределенная сеть (P2P)	19
10.6	Цепочки разметок(Beacon Chains)	19
10.7	Цепочки Oracle	19
10.8	Модуль прогнозирования	19
10.9	Майнинг, доказательство работы & потребление энергии	19
11	Умные контракты, созданные для того, чтобы улучшить любое приложение или услугу	20
11.1	Пример смарт-контракта для рыночной площадки	21
12	Децентрализованная идентификация и биометрия : Грааль массового принятия.	22
12.1	Децентрализованная идентичность и биометрия	22
12.2	Доказательство происхождения аутентификации с помощью доказательства работы	23
12.3	Децентрализованная и интероперабельная идентичность	23
12.4	Колесо конфиденциальности	23
13	Управление, которое включает лучшее из каждого	25
13.1	Управление, которое включает лучшее из каждого	25
13.2	Планируемое управление сообществом	25
13.3	Управление на основе 8 различных групп	26

14 Открытая инновация: создание условий для обобщения	27
15 Общая картина	28

1 Uniris. Краткий обзор

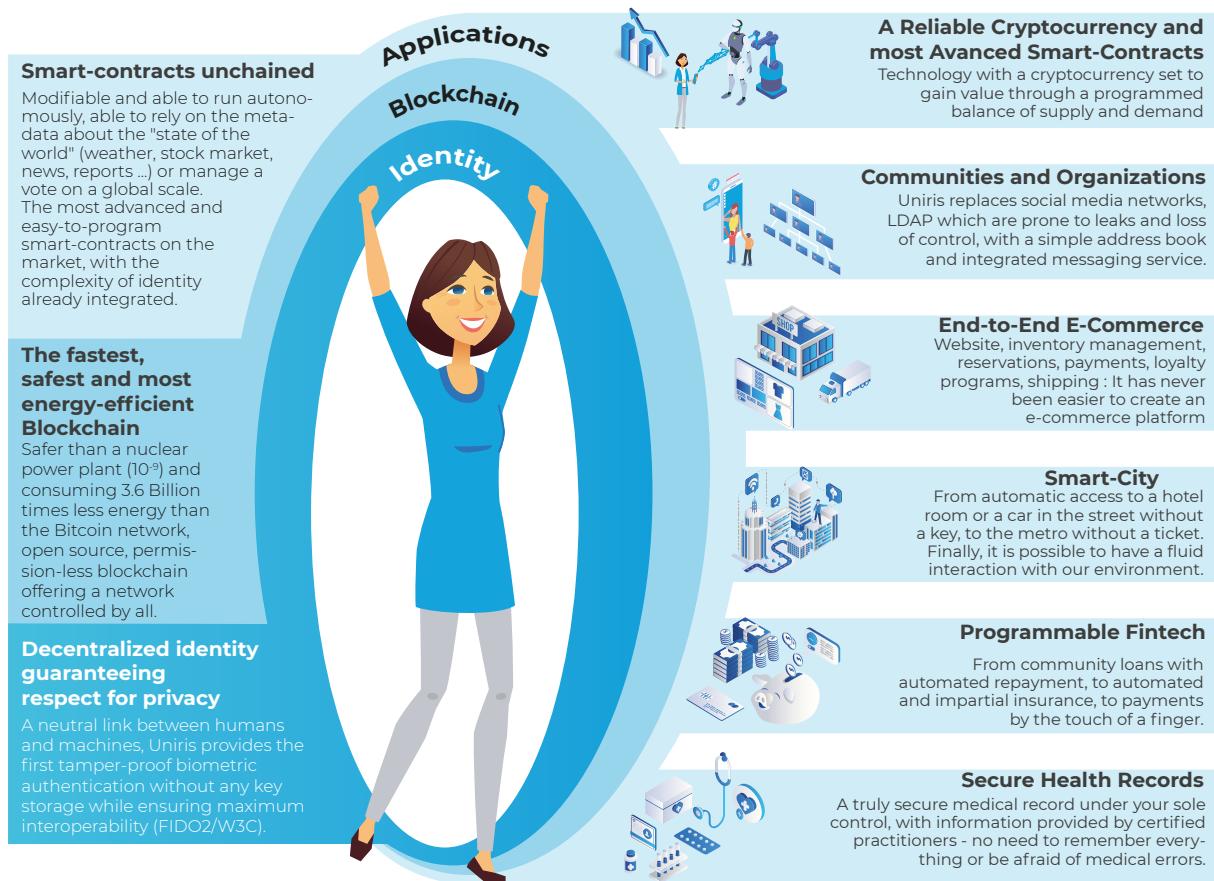
Блокчейн Uniris предлагает первую интегрированную сервисную платформу, способную удовлетворить фундаментальную потребность: возвращая каждому контроль над технологией. Таким образом, Uniris дает обещание более безопасного, инклюзивного и по-настоящему децентрализованного мира.

4 года исследований и 12 международных патентов дают Uniris технологические атрибуты, которых не хватало предшественникам - Масштабируемость, скорость, надежность и простота нативного биометрического распознавания. Эти патенты будут выданы сообществу с открытым исходным кодом в целях поощрения участия и, следовательно, ускорение темпов инновационной деятельности.

Предназначенный для массового принятия, Uniris опирается на новую форму нерушимой консенсус валидации (ARCH), который является сверхнадежным и допускает неограниченное число сделок. Uniris внедряет биометрию по собственному усмотрению, используя метод идентификации, защищенный от взлома и доступный ко всему. Эта технология использует невероятную сложность внутренней части пальца, которая уникальна для каждого человека, без необходимости хранения каких-либо биометрических данных.

Наша криптовалюта, UCO, является основой сети, питающей эти операции и монетизирует вкладчиков в развитие экосистемы, построенной людьми для людей. Наша блокчейн платформа нацелена на замену и совершенствование всех существующих приложений с всеобъемлющей и открытой экосистемой, позволяющей людям выйти из-под контроля централизованных систем (Facebook, Google, Amazon, Banks...) на децентрализованную систему, где каждый будет сохранять контроль над своими данными, собственностью и конфиденциальностью. Uniris возвращает человечеству контроль над технологиями, а каждому человеку - контроль над своей идентичностью.

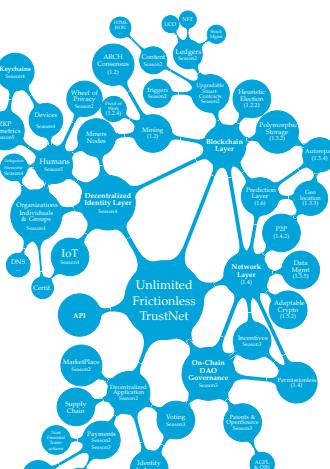
Uniris возвращает человечеству контроль над технологиями и контроль каждого человека над своей личностью.



2 Конкурентная среда и преимущества Uniris

2.1 Самый масштабируемый, безопасный и энергосберегающий блокчейн, благодаря консенсусу ARCH.

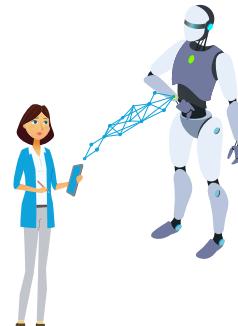
Впервые в истории, блокчейн представляет технологию, которая может работать без центрального органа, принимающего решения. Система, которая не только беспристрастна, но и прозрачна и неотчуждаема. Новая форма консенсуса ARCH, созданная Uniris, основана на непредсказуемом выборе небольшого подмножества узлов (майнеров) для подтверждения и сохранения транзакций (197 из 100 000 узлов). В сети используется контролируемая многоадресная передача, поэтому что каждый узел всегда будет знать, где искать данные по наиболее эффективной сети. Путь, позволяющий линейно увеличивать число транзакций/сек в функции количества сетевых узлов (100x). В таблице ниже представлены основные различия с другими блокчейнами:



	Validation Time	txns/sec	Consumption/txn	Security	Privileges	Data Security (replication algo)	Transactions Ref.	Global	P2P Layer
Bitcoin (POW)	10 min	7	420 000 Wh/txn	51 %	no	Everywhere	UTXO	yes	Gossip
Ethereum 1 (POW)	15 sec	20	36 000 Wh/txn	51 %	no	Everywhere	Account	yes	Gossip
Ethereum 2 (POS)	15 sec	15000	360 Wh/txn	66 %	yes	Sharding by transactions groups	Account	yes	Gossip
EOS (dPOS)	0.5 sec	3996	7 Wh/txn	66 %	yes	Sharding by Blockchain	Account	Split per Blockchain	Gossip
Tezos (dBFT)	1 min	40	-	66 %	yes	Everywhere	UTXO	yes	Gossip
HashGraph (DAG)	5 sec	10	-	66 %	no	Random Sharding	UTXO	no	Gossip
Stellar (FBA)	5 sec	1000	-	Quorum	yes	Everywhere	Account	yes	Gossip
Zilliqa (POW + pBFT)	2 min	2828	-	66 %	no	Random Sharding	Account	yes	Gossip
Hyperledger (BFT / CFT / Kafka)	35 sec	20000	-	66 %	yes	Everywhere	UTXO/Account	no (private)	Gossip
Libra (BFT)	10 sec	1000	-	66 %	yes	Everywhere	Account	yes	Gossip
Harmony (POS + FBFT)	136s	10 Millions	-	66 %	yes	Random Secured Sharding	Account	yes	Gossip (UDP QUIC)
UNIRIS (ARCH)	5 sec.	Unlimited	0.0000167 Wh/txn	97.5 %	no	Geo-Secured Heuristic Sharding	UTXO	yes	Supervised Multicast

2.2 Умные контракты: автономные роботы цифровой эры

Умные контракты (интеллектуальные контракты)- это роботы в реальной жизни, только в мире информатики-они выполняют действия, в соответствии с событиями. Умные контракты Uniris делают технологический рывок вперед. Они автономны и могут быть инициированы внутренними событиями (дата, сделки) или реальной жизнью (канал "Оракл": проверено на основе консенсуса и перекрестных ссылок на информацию) такие, как погода, цены акций, новости. Они приспосабливаются к окружающей среде. Полностью модифицируемые, они естественным образом способны управлять такими операциями, как управление складами, платежами, веб-хостингом ... без создания реальности за пределами подтвержденных транзакций (UTXO).



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

2.3 Децентрализованная идентичность, уважающая нашу личную жизнь

Децентрализованная идентичность избавляет от необходимости доверять свою идентичность третьей стороне, которая может оказаться в конфликте интересов и эксплуатировать нашу идентичность без нашего ведома, таких как Google, Facebook или наш любимый торговый сайт. Человек сохраняет единоличный контроль над его личностью, которая хранится на множестве узлов, обеспечивая его долговечностью и целостностью. Таким образом, децентрализованная идентичность гарантирует уважение личной жизни и ее интероперабельностью с остальными приложениями. В сочетании с возможностями, предоставляемых умными контрактами, она становится центральным элементом нашего взаимодействия с миром: Доступ к большим публичным мероприятиям (Олимпийские игры, концерты и т.д.), транспорт, гостиницы, наши сообщения, без какого-либо раскрытия деталей нашей личности.

2.4 Конец паролям и ненужным носителям



Встроенная в блокчейн биометрическая технология, предоставляемая Uniris, позволяет любому человеку идентифицировать себя без затруднений и без хранения биометрических данных. Это доступ контролль, который защищен от подделок и не раскрывается. Как он работает? Биометрические данные внутри одного из наших пальцев генерируют несколько криптографических ключей, которые никогда не будут раскрыты и с помощью которых наша цифровая идентичность будет зашифрована. Только сам человек может регенерировать один из этих ключей, и он же сможет расшифровать свою цифровую идентичность и, тем самым, доказать свою личность. Помимо технологической элегантности, способной обобщить биометрические данные без риска для нашей личной жизни, этот метод позволяет решить основную проблему блокчейна- массовое принятие.

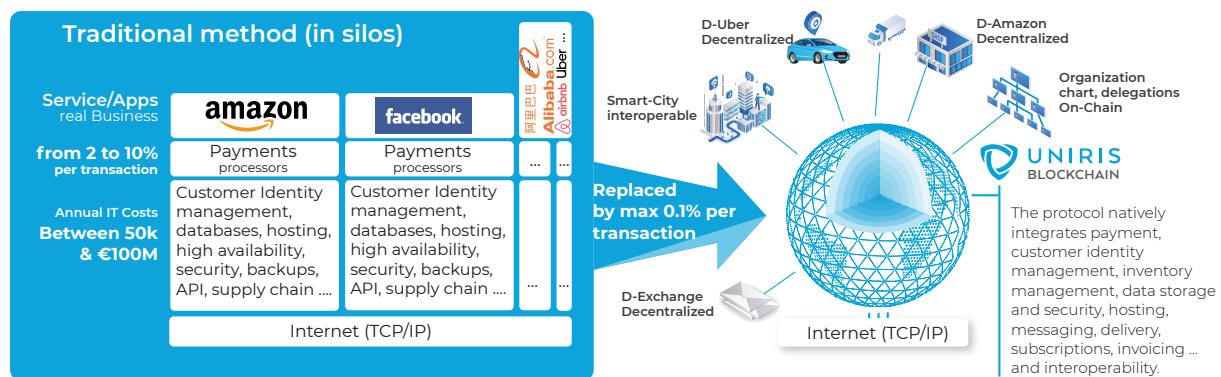
Biometrics data stored	GDPR	Software vulnerabilities	Identification method	Falsifiable Biometrics	Learning morphological evolution	Identification Scale
Biometrics on Smartphone (iOS, Android ...)	Yes (local)	Local	Yes threshold	Yes	No	100.000
Industrial/Defence Biometrics (Idemia, Fujitsu ...)	Yes (Servers)	Local	Yes threshold	Yes	No	100.000
UNIRIS Biometrics	No	Global	No	crypto-biometrics	No	Humanity

3 Практически неограниченный рынок

“Река всегда выбирает наиболее эффективный путь”

В доисторической модели веб (все еще преобладающей с момента возникновения), каждый новый сервис каждый раз воссоздает свои элементарные операционные блоки: портал, клиентная идентификация, базы данных клиентов, управление услугами, хостинг, хранение, резервное копирование, платежи. Amazon, Facebook, Google и другие не делятся ничем, что приводит к:

- Огромное потребление компьютерных серверов
- Дремучий лес логинов и паролей для пользователей
- Риски мошенничества или даже кибератак, сотрясающих мир



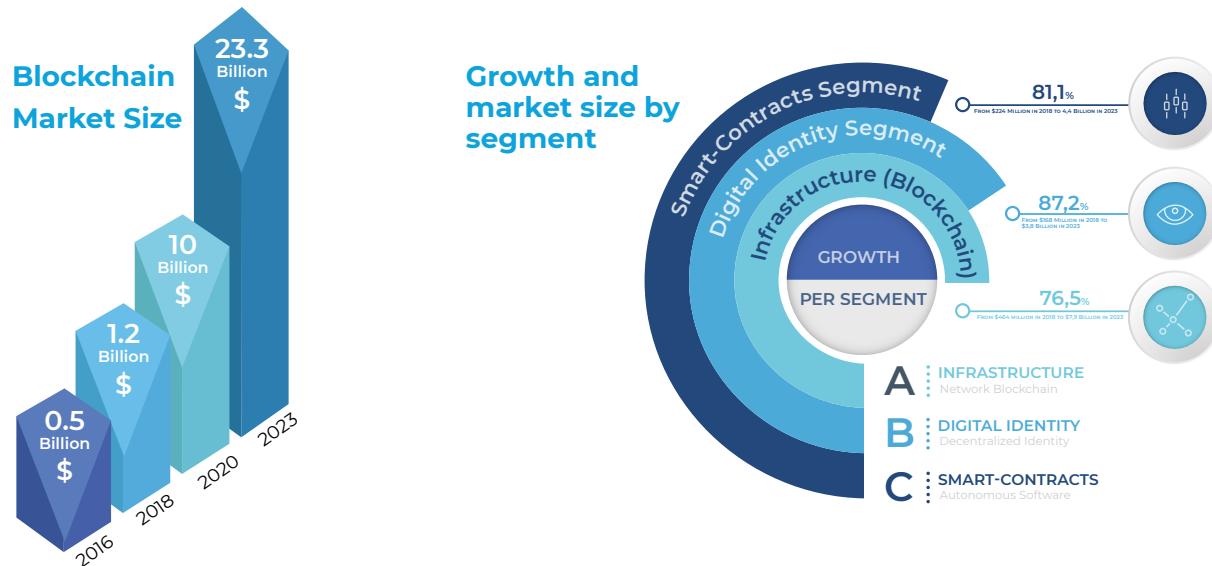
Модель "блокчейн+ децентрализованная идентичность наконец-то рационализирует эту операционную модель путем непосредственной интеграции всех слоев, необходимых для создания новых услуг :

- Требуется меньший ИТ-потенциал за счет заранее запланированной интеграции
- Уникальная и универсальная идентичность, активируемая только владельцем, независимо от его физического или виртуального местонахождения
- Удаление третьих лиц в пользу блокчейна для обеспечения устойчивости системы
- Основные экономические и финансовые последствия для стоимости каждой новой услуги.

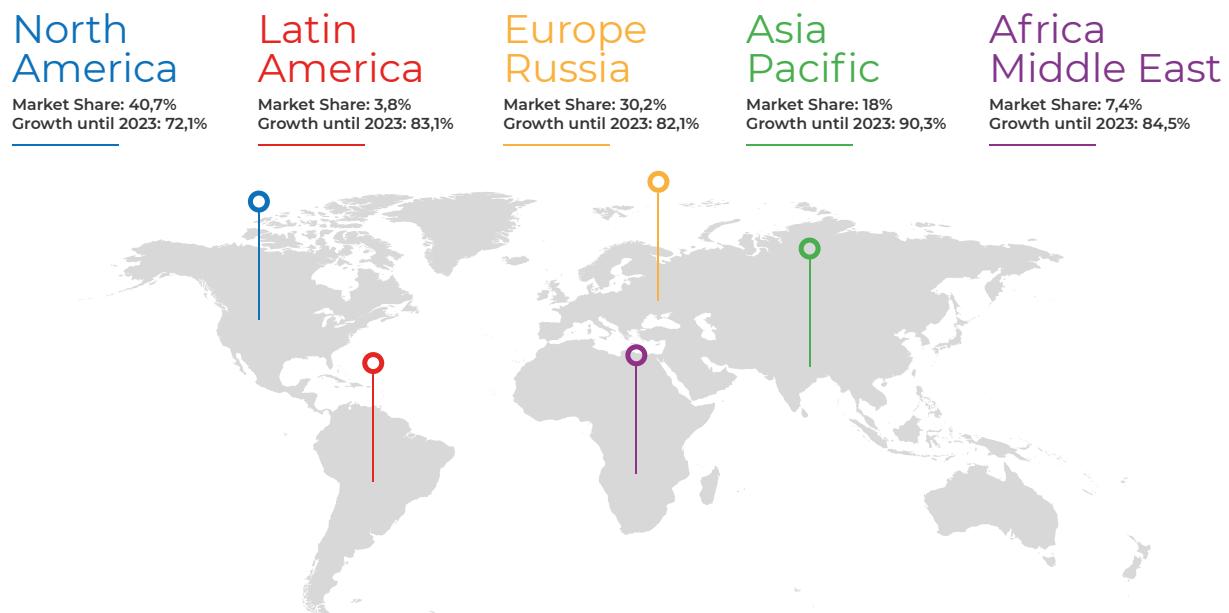
4 Исследование рынка

Мировой рынок с ростом на 80,2% в период с 2018 по 2023 гг.

Рынок блокчейна консервативно оценивается в 23 млрд. долларов США к 2023 году по сравнению с 1,2 млрд. долларов США в 2018 году с впечатляющими годовыми темпами роста в 80,2% между 2018 и 2023. Эта инкрементальная статистика не учитывает возможную замену текущих услуг и платформ приложений, что является правдоподобной гипотезой.

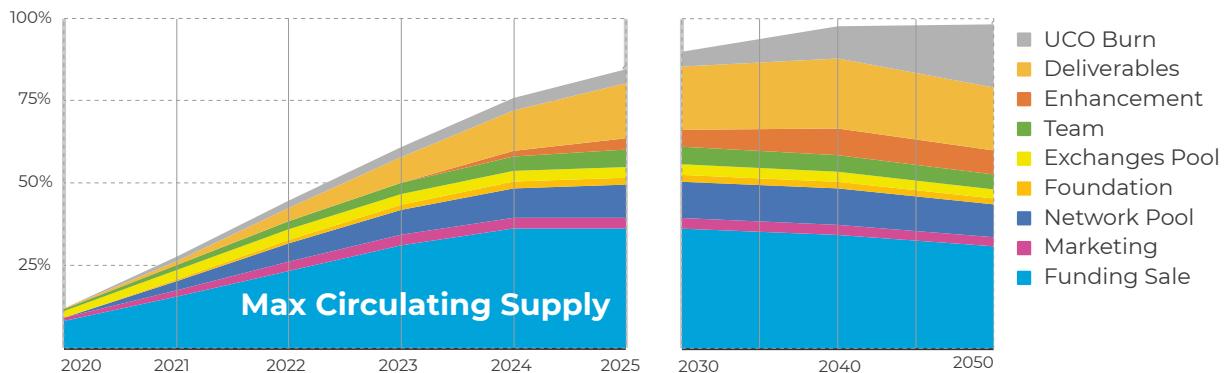


3 сегмента рынка считаются наиболее перспективным к 2023 году являются идентичность цифровые, интеллектуальные контракты и инфраструктура (Blockchain) - сегменты, в которых Uniris использует самые передовые технологии



5 The Uniris Coin - криптовалюта, запрограммированная а рост

Новая экономика криптовалют основана на особо здравом и универсальном принципе спроса и предложения, как и сырья, такого как золото или бриллианты. Криптовалюта создает ценность на платформе с открытым исходным кодом независимо от компании, которая его создала. Наша стратегия направлена, прежде всего, на создание технологических условий для "майнеров которые доверяют нашей платформе, чтобы создать как можно большую ценность. Кроме того, мы обеспечиваем правильный баланс между спросом и предложением.



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

5.1 Баланс предложения

Ограничено предложение: 10 млрд. UCO и не более. Если кто-то инвестирует в золото, а кто-то другой узнает, как сделать его дешевле, то цена на золото упадет, потому что будет больше предложения, чем спроса. Блокчейн Uniris запрещает создание новых UCO, поскольку каждая транзакция основана на существовании предыдущей неизрасходованной транзакции (UTXO).

Ограничено распространение: Чтобы избежать эффекта массового наплыва UCO на биржевые рынки, который может привести к снижению цены за счет внезапного увеличения предложения, Uniris устанавливает механизм блокировки. За исключением UCO, приобретенных в рамках частных (частично) и публичных продаж, все остальные UCO в течение двух-пяти лет могут быть выпущены частично, например, с появлением новых приложений в сети, увеличивающимся спросом в то же время. Запрограммированная дефляция с течением времени блокчейн Uniris автоматически уничтожает часть UCO, возникающую в результате транзакционных издержек, создавая таким образом запрограммированный механизм дефляции, который увеличивает стоимость каждого UCO (серая часть кривой).

5.2 Баланс спроса

Второй принцип заключается в создании дефицита ресурсов через спрос. Помимо биометрических устройств, которые будут доступны только для приобретения в UCO, задачей является массовое внедрение решения. Наша стратегия вращается вокруг 3 осей (подробно описанных в плане развития ниже):

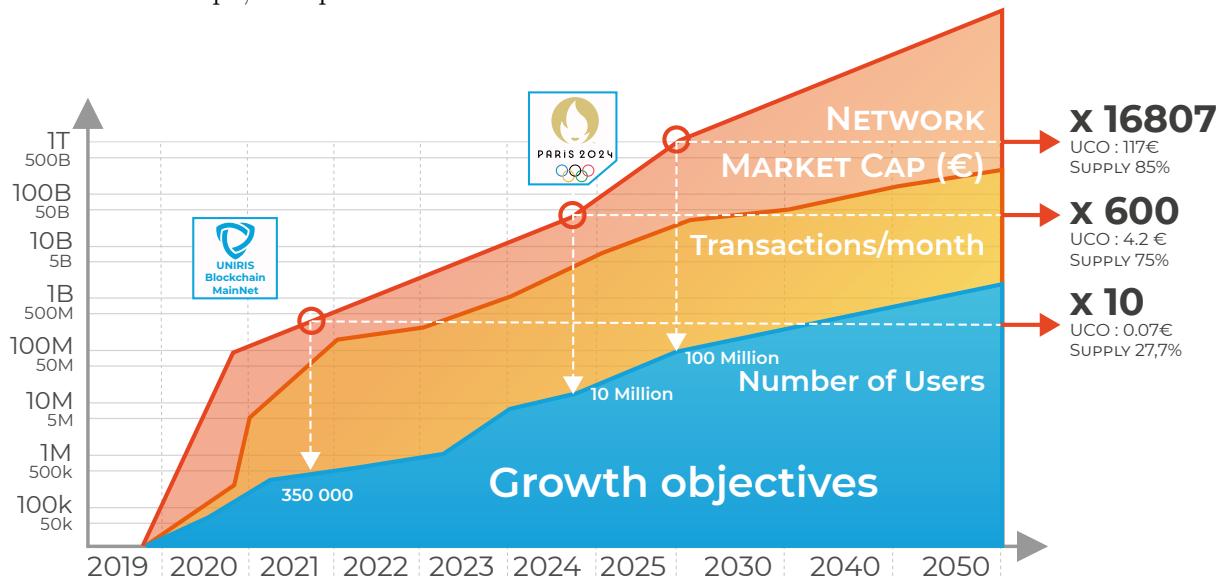
Быть референтной платформой для производства интеллектуальных контрактов и цифровых контрактов (автономный, модифицируемый, интегрированный Oracle, масштабируемый ...) и, наконец, интеграция децентрализованной идентичности, ис-

пользуемую любым человеком - платформа Uniris продвигает мир интеллектуальных контрактов за пределы мира криптовалюты.

Распространить использование, предлагая самую простую и продвинутую платформу для конечной целью проекта является обобщение биометрической идентификации (или производных) в глобальном масштабе населения с использованием 100% открытой и прозрачной сети, которая, наконец, способна доказать доверие. От открытия дверей вашего дома или автомобиля, через все механизмы обмена (финансовые, коммуникационные) до голосования.

5.3 Гипотеза развития криптовалюты UCO

В настоящее время наиболее подходящий метод оценки стоимости блокчейна основан на законе Меткалфа, который соотносит стоимость сети с количеством пользователей.



Было проведено много исследований на тему оценки криптовалюты по закону Меткалфа. Для описания цены Bitcoin использовались различные вариации, и с использованием корреляций Pearson за период с 2010 по 2018 год было обнаружено, что стоимость сети имеет порядок:

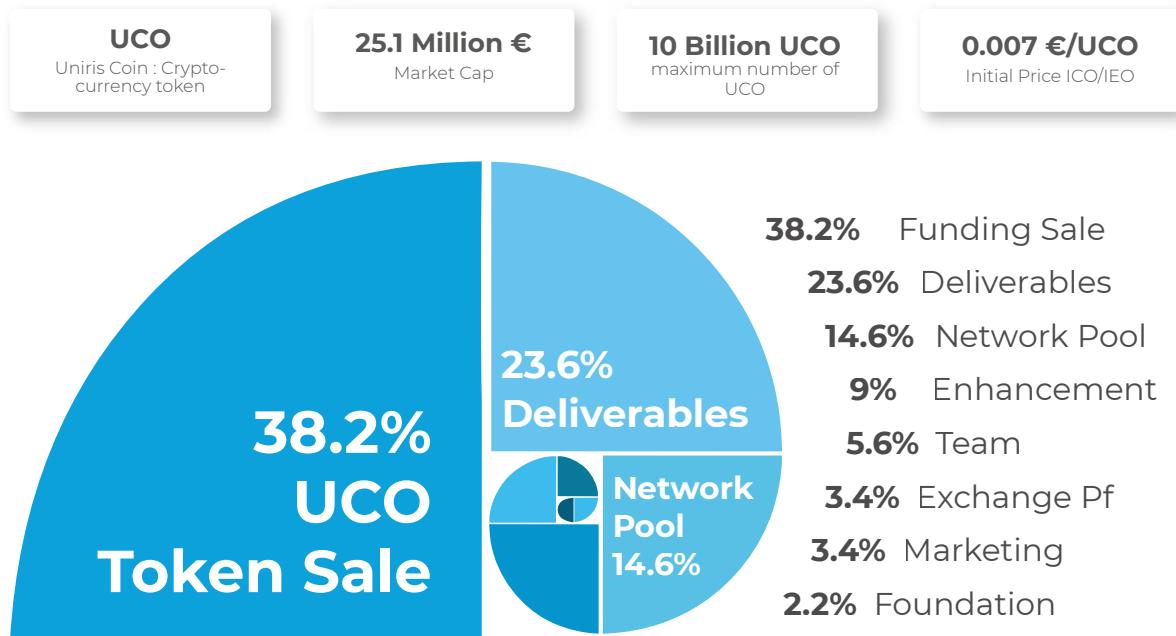
$$value \text{ of } blockchain \approx (number \text{ of } users)^{1.5} \quad (1)$$

Таким образом, данный закон обеспечивает аппроксимацию стоимости сети как функции от количества пользователей. Например, если мы рассмотрим такое событие, как Парижские Олимпиады 2024 года, которые только соберут 8 миллионов человек, и зная, что максимальное количество UCO, которые могут быть проданы на рынке в течение этого периода, составит 75% (7,5 миллиардов UCO), то мы получим :

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

6 Раздача токенов и распределение средств

6.1 Модель, способствующая разделению ценностей



Количество жетонов UCO, начальная стоимость UCO и рыночная капитализация инициализируются в соответствии со средствами, необходимыми для реализации экосистемной сети на основе предположений о росте и приоритетов проекта. В ICO Uniris (Initial Coin Offering) предпочтение было отдано двум участникам:

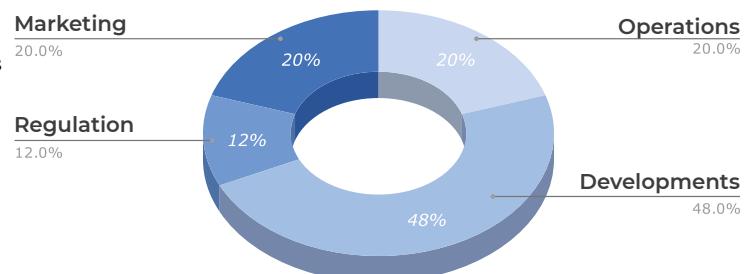
Первичным инвесторам жетоны, доступными в первые два года, будут почти исключительно жетоны от ICO.

Поставщики мобилизовались до момента поставки экосистемы (10% токенов при отправке кода и 90% после эффективного и функционального развертывания функций).

За исключением проданных жетонов, другие жетоны Uniris Tokens (UCO) будут поставляться по ставке 20-33% в год в течение 2-5 лет. 14,6% резерва сети будет использовано для гарантии материального поощрения майнеров в ожидании периода самофинансирования. Наконец, 9%, выделенные на "Усовершенствования" будут использованы для разработки новых случаев использования, но могут быть проданы только в том случае, если единичная стоимость UCO больше, чем в 100 раз стартовая стоимость (т.е. 0,7 евро/UCO).

6.2 Распределение средств

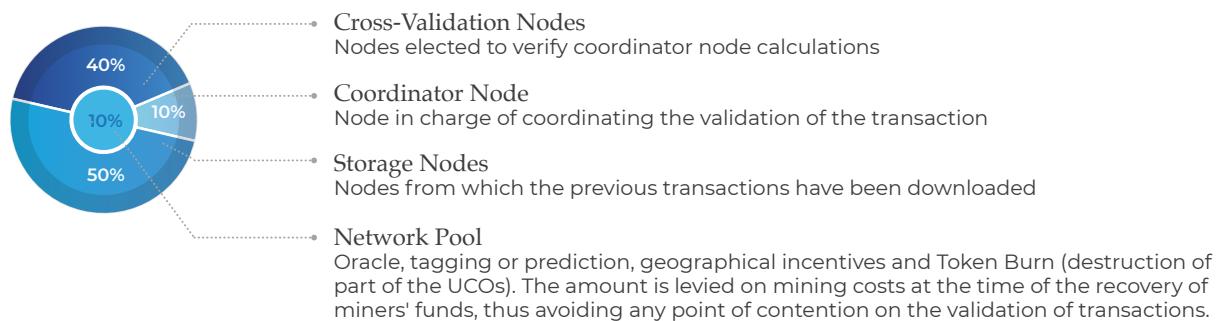
Частные и публичные продажи направлены на привлечение средств для развития сети и инноваций, опубликованных в Жёлтой бумаге. На диаграмме напротив представлено функциональное распределение собранных средств.



7 Майнеры и майнинг в сети Uniris

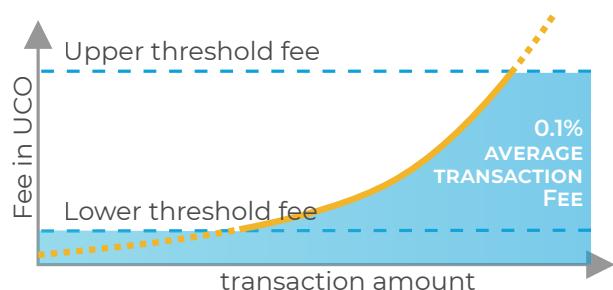
Больше не нужны сапоги и рабочий шлем!

Майнинг и доказательство выполнения работ в сети Uniris основываются уже не на затраченных вычислительных мощностях и электроэнергии, а на криптографической верификации для подтверждения и обеспечения безопасности происхождения транзакции (биометрические устройства, смартфоны, аппаратные или программные ключи и т.д.). Прямыми следствием консенсуса ARCH является то, что для обеспечения вычислительной мощности сети Bitcoin, которая насчитывает ~ 100,000 майнеров, требуется только 295 майнеров.



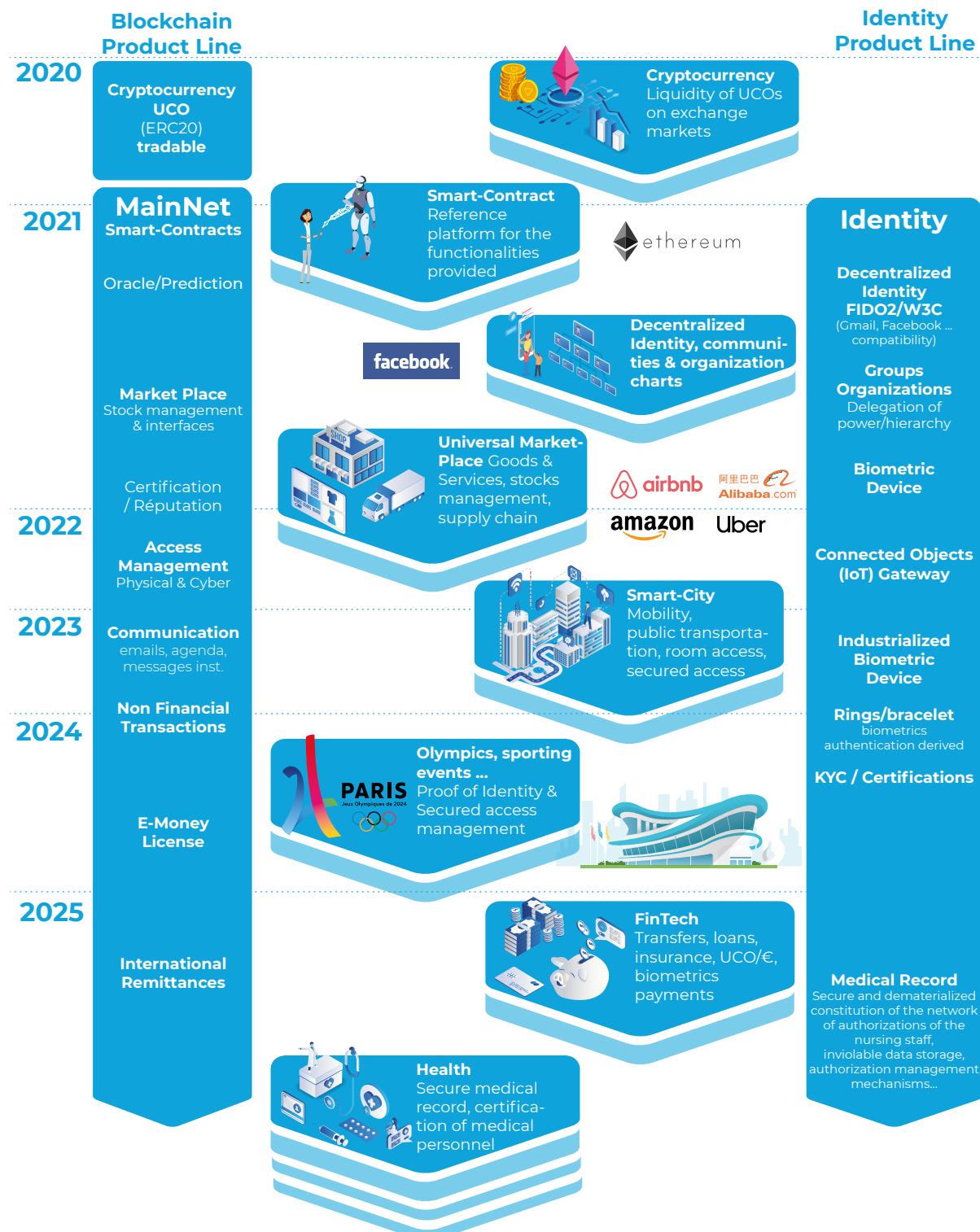
Таким образом, любой человек может владеть узлом хранения и получать соответствующее вознаграждение, но только майнеры, выбранные самой сетью, могут стать майнерами, подтверждающие транзакцию. Цель этих выборов, осуществляемых на основе "умного" контракта, заключается в том, чтобы максимально расширить географическое распределение майнеров, а также гарантировать достаточный уровень доходов для всех выбранных майнеров (таким образом, избегая риска того, что майнинговые фермы могут поставить под угрозу надежность децентрализованных сетей). Первые шахтеры будут избираться в первую очередь из числа первых инвесторов, которые сделали возможным финансирование сети.

Сборы рассчитываются в соответствии с реальными затратами сети (размер, сложность ...). Максимальные и минимальные сборы определяются с помощью цепочки Oracle, которая способна корректировать эти два лимита в соответствии со стоимостью электроэнергии или рыночной стоимостью криптовалюты UCO - таким образом, делая финансовую модель устойчивой как для майнеров, так и для пользователей.



8 План развития

Сеть Uniris - важнейший структурный элемент и катализатор создания Нового Мира Услуг, которому доверяют, который взаимодействует, доступен и контролируется всеми.



9 Команда

Созданная в 2017 году по окончании первых двух лет фундаментальных исследований Себастьяном, Нилешем и Кристофором, UNIRIS SAS частично принадлежит Политехнической школе (Paris Saclay), финансируемой BPI во Франции и инвесторами smart-city на сумму 1 млн. евро. По итогам ICO (публичная продажа UCO cryptomonnaie) будет создана организация в форме ассоциации для организации сообщества вокруг мероприятий, чтобы к 2025 году позволить публичному блокчейну летать на своих собственных крыльях.

За последние несколько месяцев мы разработали некоторые модули блокчейна и прототип биометрического устройства, что позволило нам пройти сертификацию в Стратегическом Комитете Индустриальной Безопасности для контроля доступа на Летних Олимпийских Играх 2024 года в Париже.

Наша команда - это уникальное сочетание взаимодополняющих, сплоченных и опытных личностей из таких компаний, как Thales, Mastercard, Barclays, Orange, Mozilla, Google, PwC, а также исследователей из École Polytechnique/CNRS. Большинство из нас знали друг друга задолго до создания проекта, как профессионально, так и лично, что позволило нам сэкономить значительное количество времени при реализации каждого из кирпичиков решения.

Руководство

 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 Aina CIO International PMO: Identity Number Altran, AXA Insurance, Energy Engie/GRDF, DCI	 in Christophe CSO Ex-Special Forces - Technip Security Manager (Niger), RGPD safety consultant
 in Virginie Community Manager Head of Web Content Management and Communities for the Gueudet Group - Publishing	 in Akshay R&D Maths École Polytechnique - Researcher in Maths, Blockchain and Biometrics
	 in Victor CBizDevO Coordinator/BizDev Crypto-Mondays & Chain Accelerator - MIT BlockChain Biz Innov&Apps

Консультанты по технологиям, стратегические и коммуникационные советы

 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, Mentis	 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

Большое спасибо всем тем, кто сопровождал нас с самого начала приключения: всей команде HEC Challenge+, ускорителю Ecole Polytechnique X-UP, программе StationF Founders Program, GICAT, CEPS, Cap Gemini, нашим инвесторам, без которых все это было бы невозможно: Стефану, Фредерику, BPI и всем нашим инвесторам с частных продаж. Большое спасибо также всем людям, послам и советникам, которые помогли нам усовершенствовать как технологическое, так и человеческое измерения проекта.

Партнеры

Партнерства Uniris сосредоточены на инновациях и росте сообществ. Научно-исследовательские институты дают нам доступ к передовым технологиям и проверке наших инноваций.



10 Блокчейн Uniris - разработан для глобального использования

10.1 По-настоящему децентрализованная и безгранична сеть

Учитывая универсальные физические и материальные ограничения, миллиарды операций не могут быть интегрированы в единую блочную цепь. Аналогичным образом, независимо от метода консенсуса, невозможно обеспечить консенсус по миллиардам транзакций путем опроса всех узлов сети. Наконец, учитывая работу распределенных сетей (P2P), невозможно гарантировать свежесть (согласованность) данных в асинхронной сети, кроме как в случае с сетью Bitcoin, за счет существенного замедления работы сети путем вычисления монахини блока в доказательство своей работы. Uniris решил эти проблемы следующим образом:

10.2 Бесконечные цепочки транзакций против цепочки блоков

Вместо цепочных блоков транзакций, каждый блок сводится к своему атомному варианту, т.е. каждый блок содержит только одну транзакцию, каждая транзакция имеет свою собственную цепочку.

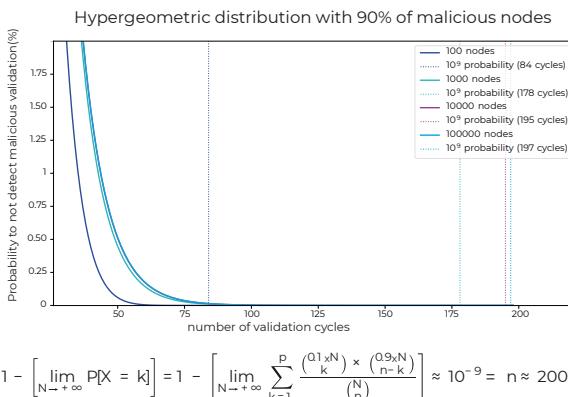
10.3 Консенсус ARCHE: абсолютный консенсус

Это новое поколение консенсуса. « Atomic Rotating Commitment Heuristic (ARCH) » или на русском "Эвристика атомных вращающихся обязательств (ARCH)". Разбираем по-отдельности каждый элемент:

Атомная валидация (Атомное обязательство) является формой "абсолютного" Консенсуса, который подразумевает 100% согласие и положительную реакцию или отказ от валидации сделки.

Эвристика это набор алгоритмов, программного обеспечения и параметров, которые управляют всей сетью, позволяя, например, сети децентрализованно и согласованно выбирать узлы, отвечающие за проверку и хранение цепочек транзакций.

Вращая полностью распределенную сеть (без центральной или привилегированной роли), узлы, выбранные для каждой операции, изменяются навсегда, так что ни один узел не может предсказать до прихода транзакции, какие узлы будут выбраны.



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 Прогнозируемая, оптимизированная, гео-безопасная система репликации

способна самостоятельно восстанавливать себя, вместо того, чтобы синхронизировать транзакции беспорядочным образом по всей сети, каждая цепочка транзакций будет храниться

в воспроизводимом и упорядоченном виде на множестве узлов - так, чтобы каждый узел, автономно, знал все узлы, на которых проводятся те или иные транзакции, и мог разгрузить сеть, опрашивая только самые близкие "избранные" узлы. Выбор узлов хранения объединяет географическое положение для обеспечения безопасности данных даже в случае катастрофы в одном или нескольких географических районах.

10.5 Вмешаемая распределенная сеть (P2P)

Основанная на контролируемой многоадресной передаче (Supervised Multicasting), одноранговая сеть использует механизм самообнаружения, основанный на входящих соединениях, и механизм цепочки сетевых транзакций для поддержания квалифицированного и достоверного представления, генерируя минимальное количество новых транзакций.

10.6 Цепочки разметок(Beacon Chains)

Ни один узел не имеет физической возможности знать статус каждой транзакции в безграничной сети. Сеть Uniris использует набор специфических цепочек транзакций, каждая из которых содержит подмножество адресов последних транзакций на определенную дату, что позволяет, например, любому узлу автоматически пересинхронизировать себя в случае отключения.

10.7 Цепочки Oracle

"Состояние мира" обновляются консенсусом каждый раз, когда обновляется какая-либо информация (например, когда выходит новый прогноз погоды, новости, фондовый рынок и т.д.)

10.8 Модуль прогнозирования

Для того чтобы децентрализованная сеть выживала на протяжении веков, она должна быть способна адаптироваться к угрозам и реагировать соответствующим образом. Для этой цели в сети Uniris имеется модуль прогнозирования, способный установить связь между помехами в сети (например, отсутствие узлов в географическом районе) и событием (например, распространение нового прогноза погоды, информации, фондовой биржи и т.д.).

10.9 Майнинг,доказательство работы& потребление энергии

Поскольку избрание узлов и синхронизация сети обеспечивается Эвристическими алгоритмами, доказательство работы используется для проверки того, что узлы в начале валидации и устройство в начале транзакции хорошо авторизованы (например, биометрическое устройство), что позволяет завершить валидацию по ее контексту (например, электронное голосование, требующее реальной идентичности избирателя). Так как случайный выбор узлов больше не связан с расходами на энергию, потребление сети, таким образом, делится на 3,6 миллиарда по сравнению с сетью Bitcoin..

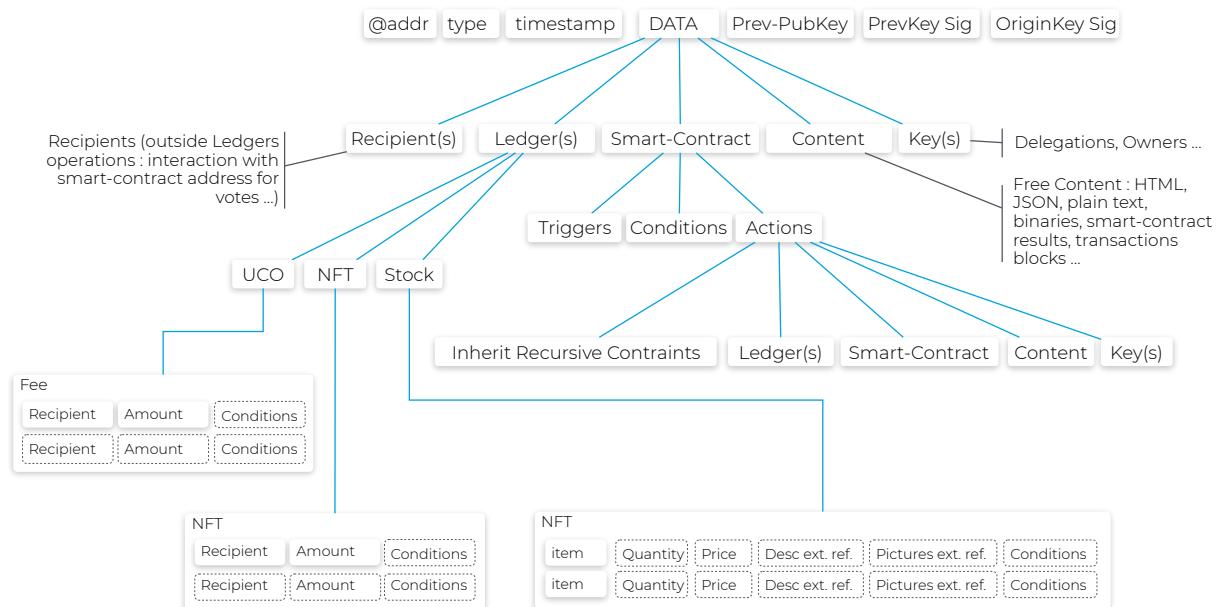
Note: All those elements are explained in a detailed manner inside [Yellow Paper](#)

11 Умные контракты, созданные для того, чтобы улучшить любое приложение или услугу

Сначала созданная сетью Bitcoin для обновления общего реестра, затем усовершенствованная возможность выполнять запланированные действия через интеллектуальные контракты и вплоть до возможности управлять целыми системами, технология блокчейн постоянно изобретает себя заново. В отличие от смарт-контрактов, составленных в Ethereum, смарт-контракты в сети Uniris напрямую интерпретируются майнерами. Поскольку каждая транзакция или смарт-контракт хранится на определенной группе узлов (эвристический ротационный выбор ARCH), они могут синхронно обрабатывать набор новых функций: например, они могут знать состояние складов, количество голосов и транзакции, предназначенные для этого смарт-контракта (любая транзакция, предназначенная для смарт-контракта, уведомляется и хранится на соответствующей группе узлов), или они могут автоматически запускать действие при наступлении события (дата, погода и т.д.).), что позволяет поддерживать любой реальный случай использования.

Для обеспечения безопасности и безотказности смарт-контрактов они полностью основаны на модели UTXO (вывод неизрасходованных транзакций), которая может быть использована в качестве входа в новую транзакцию. Другими словами, "умные" контракты зависят не от состояния внутренней базы данных, а только от уже выпущенных транзакций.

Будь то простая передача, правило доступа в здание, интернет-магазин, хостинг веб-сайта, голосование по всей стране или даже весь код, используемый в самой сети, любая сделка соблюдает следующую схему:



Получатели (в дополнение к получателям, упомянутым для операций с реестром: например, взаимодействие с "умными" контрактами: голоса и т.д.).

Регистры в дополнение к регистру, связанному с криптографией UCO, блокчейн uniris имеет еще два "родных" регистра: Регистр, который позволяет автоматически обновлять склады в зависимости от заказов

(UTXO)NFT (нефинансируемые транзакции), предназначенными для использования peer-to-peer (ваучеры ... город или компания в местной валюте, и т.д.).

Триггеры - это события, которые автоматически запускают выполнение смарт-контракта. Этими триггерами могут быть дата, транзакция или любая информация в цепочке Oracle.

Рекурсивные ограничения Поскольку смарт-контракты могут модифицироваться, а разрешения на доступ могут быть настроены (делегации и т.д.), в смарт-контрактах есть специальное поле для проверки дополнительных элементов перед тем, как принять обновление.

Доказательство идентификации Доказательства работы является нахождение открытого ключа, соответствующего устройству, используемому для генерации транзакции (смартфон, биометрия, программный ключ...).

Многопользовательский Зона "ключи" позволяет определить владельцев смарт-контракта, а также все связанные с ним де-

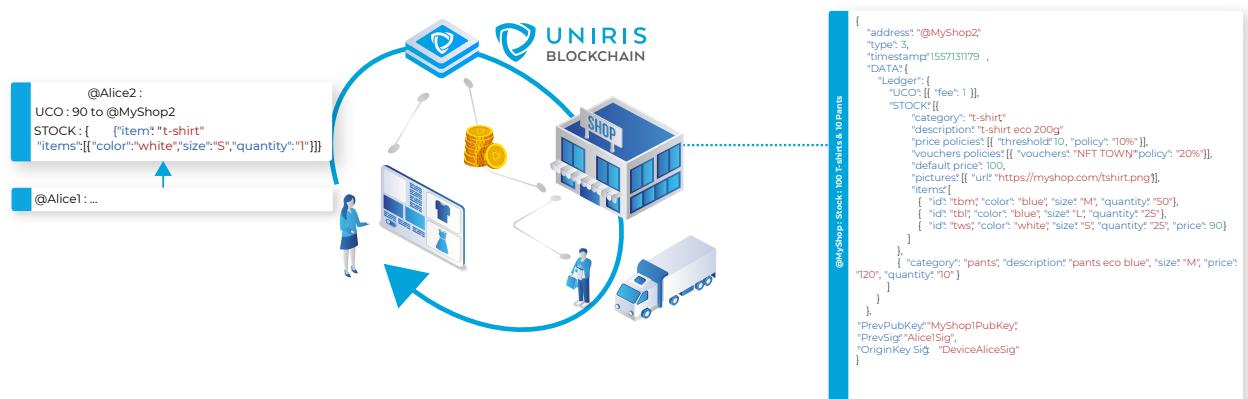
легации.

Свободный контент Область "контент" может содержать данные любого типа, ее содержание не интерпретируется узлами сети. Эта зона используется, например, для размещения кода (binary+sources) самого блокчейна, изображения, текста, HTML-кодом сайта или результата смарт-контракта.

Спецификации Код смарт-контрактов интерпретируется непосредственно каждым из узлов проверки и хранения. Содержание значительно упрощено: условия, действия, операции регистрации. Смарт-контракты, такие как блокчейн-код, выполняются из модулей, работающих на языке Elixir (на базе Erlang).

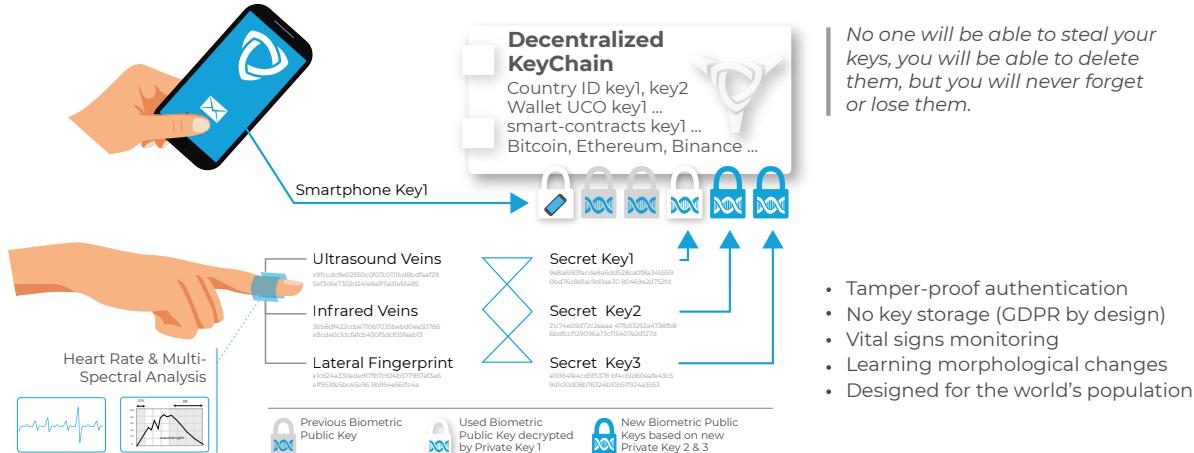
11.1 Пример смарт-контракта для рыночной площадки

В модели UTXO единственными ссылками являются подтвержденные транзакции. Например, для сайта продавца статус запасов не изменяется в самом "умном" контракте, а восстанавливается из подтвержденных транзакций. Опыт пользователя или торговца абсолютно идентичен, но каждый статус неопровергим и однозначен.



12 Децентрализованная идентификация и биометрия : Графаль массового принятия.

12.1 Децентрализованная идентичность и биометрия



Аутентификация, которая не может быть использована без нашего ведома. В отличие от отпечатков пальцев, радужной оболочки глаза, лица, которые могут быть легко воспроизведены и сфальсифицированы с фотографии на Facebook или на улице - невозможно восстановить внутренность пальца - устройство проверяет жизненные показатели во время каждой проверки подлинности, чтобы убедиться, что палец не был отрезан и что человек полностью осведомлен и согласен, прежде чем любая сделка будет подтверждена.

Без хранения ключей Все существующие биометрические идентификации основаны на одном и том же принципе:

- сбор биометрических данных и хранение данных распознавания(образец)
- сравнение измерения с образцом
- Если совпадение превышает определенный порог, то личность идентифицирована (soft)

Идентификация с помощью биометрического устройства Uniris больше не основывается на пороге распознавания и, следовательно, больше не нуждается в хранении для сравнения. Как показано на рисунке напротив, частные или секретные криптографические ключи генерируются "на лету"(а затем удаляются), позволяя пользователю извлекать и расшифровывать свой децентрализованный "брелок". Выявление толерантности обеспечивается описанным выше механизмом обучения. Наконец, аутентификация больше не является программной, а является криптографической, что делает любую попытку атаки программного обеспечения бесполезной.

Устройство независимой аутентификации мирового населения В отличие от биометрической идентификации на смартфоне, которая будет работать только на одном смартфоне, аутентификация Uniris работает на любом человеке и на любом устройстве. Поскольку ключ не хранится, он совместим с самыми строгими правилами защиты данных (RGPD, CNIL и т.д.), что делает биометрию широко используемой.

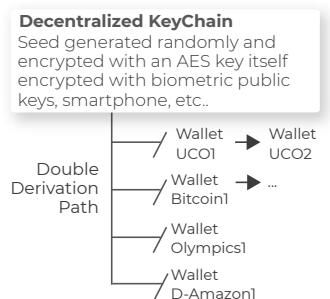
Автоматическое обучение на протяжении всей жизни Как показано на рисунке выше, ключи генерируются парами из биометрических измерений. Если одно из измерений отличается (порез, ожог и т.д.), то только один ключ будет соответствовать и сможет подтвердить подлинность, а два новых ключа будут добавлены для шифрования (с помощью связанных открытых ключей) децентрализованного брелока, что позволит узнать новые биометрические измерения человека без необходимости хранить ключи.

12.2 Доказательство происхождения аутентификации с помощью доказательства работы

Идентификация в сети Uniris не ограничивается биометрическими устройствами, и, как показано на рисунке выше, каждый метод доступа (смартфон, USB-ключ, программный ключ и т.д.) будет иметь свой собственный метод сертификации (см. [Yellow Paper Season 1](#)). Так как метод идентификации связан с транзакцией (см. схему смарт-контракта: "OriginKey Sig") и доказательством работы, это позволит, таким образом, модулировать безопасность, связанную с любым смарт-контрактом или кошельком - например: транзакция стоимостью менее 1000 UCO может быть осуществлена как с конкретного смартфона, так и с биометрического устройства, если стоимость превышает 1000 UCO. Вход в здание с высоким уровнем безопасности может быть осуществлен с помощью NFC в рабочее время и с помощью биометрии вне работы.

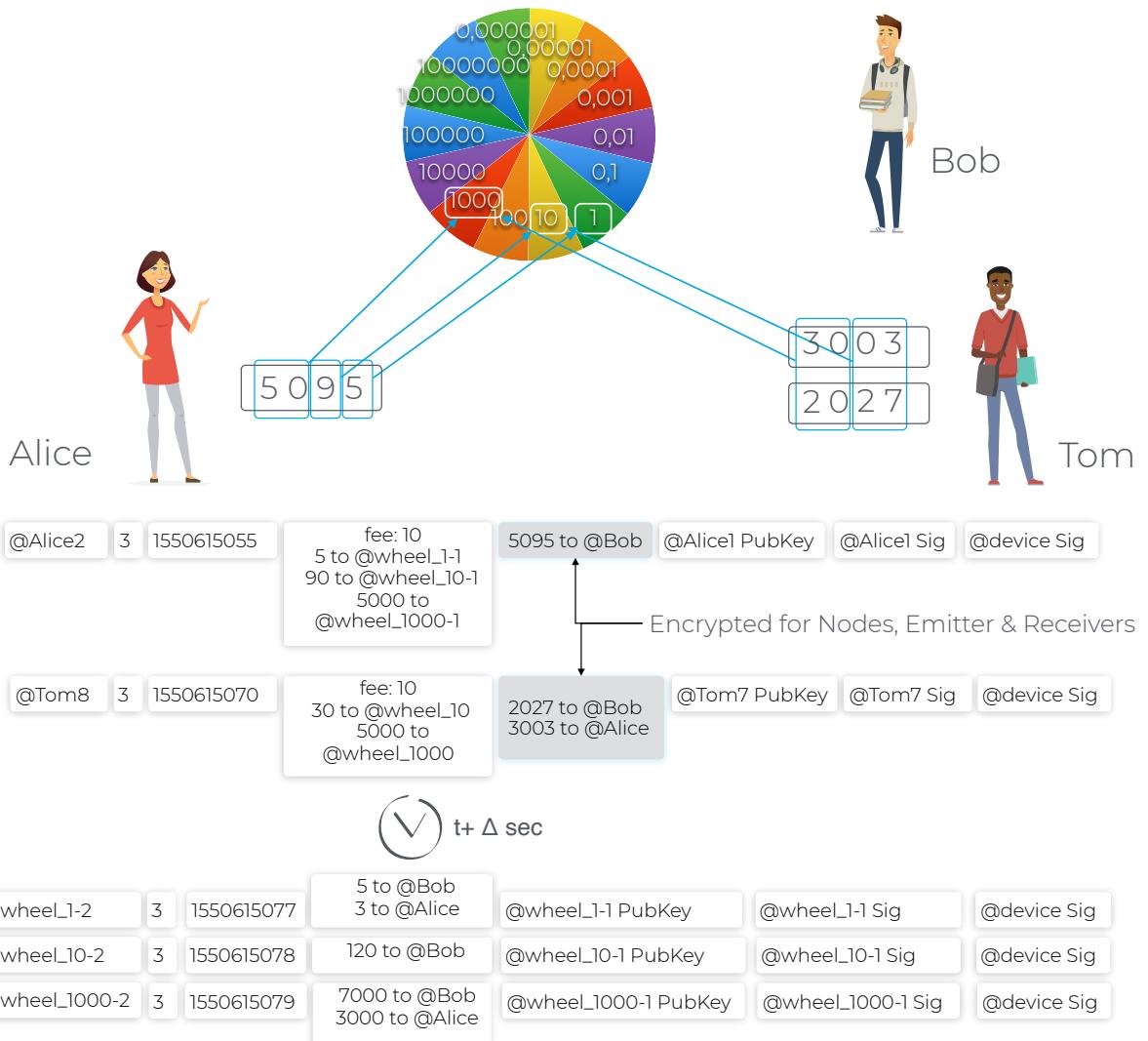
12.3 Децентрализованная и интероперабельная идентичность

Технически, децентрализованная идентичность человека или связанного объекта состоит из Seed (корневого ключа), из которого случайным образом генерируется набор ключей в соответствии с производным путем - Таким образом, для любого доступа к сервису или приложению ключ будет рассчитываться "на лету" из ключа, выданного из seed, и первого открытого ключа, связанного с сервисом или приложением - таким образом, позволяя создавать бесконечное число идентификаторов без необходимости даже хранить ключи - все функциональные возможности, связанные с этой децентрализованной идентификацией, будут подробно описаны в "Желтой бумаге Сезон 4": Автоматические адресные книги, электронная почта, FIDO2



12.4 Колесо конфиденциальности

Поскольку сделки являются публичными, в сети существует механизм, называемый "Колесо конфиденциальности" который позволяет устраниТЬ корреляцию между отправителем, получателем, временем и суммой сделок. Этот механизм используется, в частности, в контексте электронного голосования и позволяет, не ставя под сомнение последовательность реестров, каждому человеку сохранить контроль над своей личной жизнью.



13 Управление, которое включает лучшее из каждого

13.1 Управление, которое включает лучшее из каждого

DAO (Децентрализованная автономная организация) - это децентрализованная организация, правила управления которой автоматизированы и написаны непреложным и прозрачным образом в блокчейн.

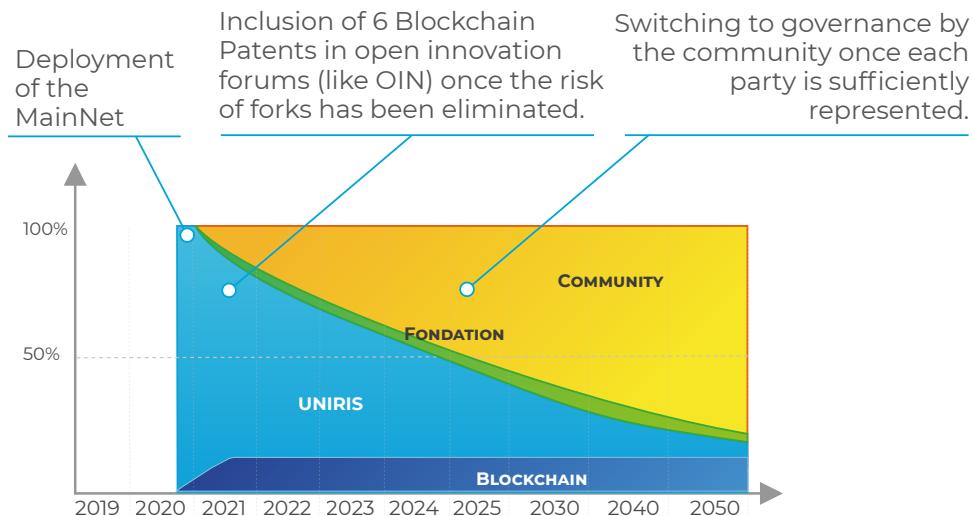
Управление - это, пожалуй, самая большая проблема, с которой сталкиваются блокчейны. Сегодня сеть Bitcoin имеет наиболее успешное децентрализованное управление с теперь уже известным выражением "code is law" (код это закон). Однако это управление основано только на одном типе участников "владелец майнера" или, как следствие, самая большая группа майнеров - это на самом деле код, установленный самой большой вычислительной мощностью и, следовательно, фермами профессионального майнинга, которые на самом деле управляются сетью.

Несмотря на то, что это управление децентрализовано, оно скрывает целую часть экосистемы, начиная с самих пользователей, поставщиков приложений, технических специалистов и даже самого Blockchain, ограниченного кодом, установленным на самой большой вычислительной мощности.

Для того чтобы сеть выжила со временем и приспособилась к изменениям в обществе, управление блокчейна Uniris основано на нескольких технических и функциональных основах:

	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.
	Code «On-Chain» The code used by the nodes is hosted by the Blockchain itself, so the network is certain that all the nodes will immediately apply the decided updates (via Elixir hot-reload modules and from the information stored in the "smart-contract content" area). The Uniris Blockchain is also equipped with the ability to test the impact of a new feature in real time.
	Modifiable Smart-Contract Each smart-contract is stored in the form of a specific transaction chain allowing the network to version (git...) all updates, but also to force each update according to a specific governance (voting quorum, veto right...).
	Incentives Financing of the work associated with updates, new features and contributions is an essential element. The network has a reserve of one third of the tokens (with progressive distribution constraints) for this purpose.

13.2 Планируемое управление сообществом



13.3 Управление на основе 8 различных групп

Пользователи: Любой человек, способный доказать свою уникальность (с помощью биометрического устройства или другого процесса).

Майнеры: Владельцы узлов майнинга и те, кто составляет саму сеть.

Приложения и услуги: Поставщики приложений с весом, который тем более важен, так как они генерируют использование.

Фонд (или ассоциация), роль которого заключается в том, чтобы оживлять сообщество и организовывать управление.

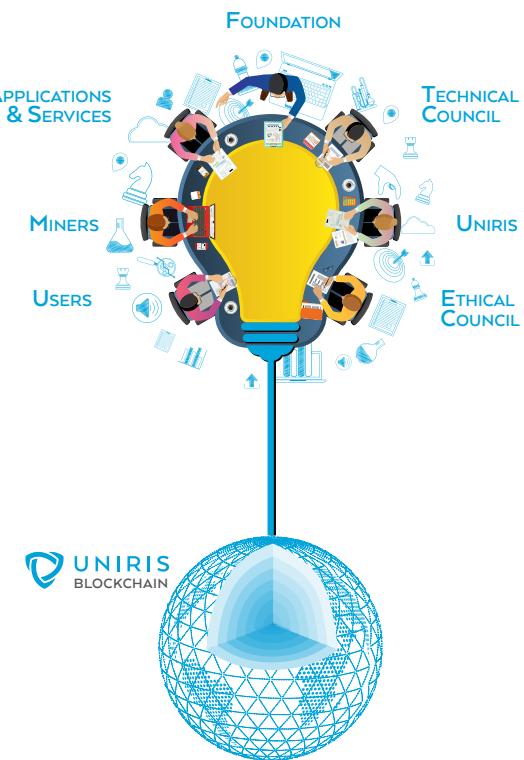
Технический совет: Состоит из "центральных разработчиков которые становятся более значимыми, потому что они вносят свой вклад в код.

Uniris как создатель сети.

Совет по этике, члены которого будут предложены/избраны сообществом и который будет иметь право вето на все технические характеристики, влияющие на конфиденциальность пользователей.

Блокчейн: Блокчейн сам по себе, в частности, благодаря своей способности тестировать функциональность в реальной жиз-

ни, прежде чем разворачивать ее в сети. Например, максимальный размер транзакций не привязан к точке зрения и может быть напрямую проверен, чтобы знать реальное воздействие на сеть с учетом рассматриваемой потребности.



14 Открытая инновация: создание условий для обобщения

Uniris - проект, имеющий гуманитарную и общественную направленность.

Как только риск, связанный с вилкой, будет исключен, все Патенты будут переданы в наследие технологий с открытым исходным кодом. Скорее всего, это наследие будет передано в OIN (Open Invention OPEN GOVERNANCE Network), при этом весь исходный код будет находиться под лицензией AGPL 3.0.

Асертивный подход добровольной педагогики, дающий возможность каждому понять технологию.

На полпути между научной публикацией и популярными статьями, лежащая в основе технология будет подробно описана в 5 "Желтых бумагах".

Первая часть, уже опубликованная, описывает функционирование сети (Консенсус ARCHE, контролируемая многоадресная передача (p2p) и все механизмы, которые позволили создать неограниченную сеть): <https://uniris.io/UNIRIS-Yellow-Paper.pdf>

Следующие части будут последовательно посвящены: прикладному программированию, открытому управлению, операционным кирпичикам децентрализованной идентичности, чтобы закончить на биометрических устройствах и их производных.

СПИСОК ПАТЕНТОВ

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 Общая картина

Пример перевода криптовалюты

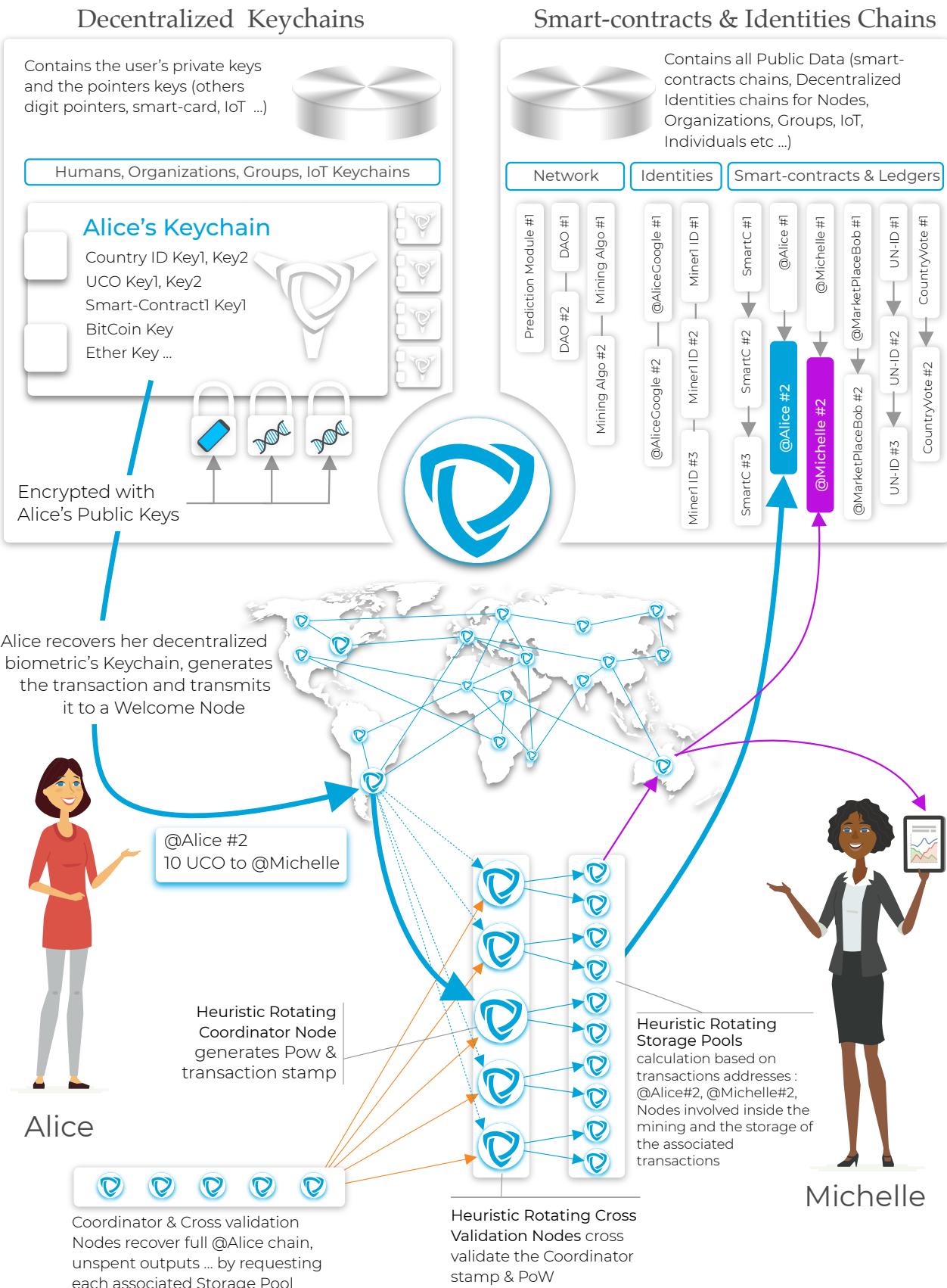


Рис. 1: Uniris Chain Overall Functioning