ARCHETHIC
PUBLIC BLOCKCHAIN

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

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

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

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

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

ARCHETHIC GIVES BACK TO HUMANITY CONTROL OVER TECHNOLOGY, AND TO EACH INDIVIDUAL, CONTROL OVER THEIR IDENTITY

LIGHTHNING BLOCKCHAIN

1 million transactions/second
< 5 sec to become irrepudiable

THE SAFEST NETWORK

0.0000001% risk of fraud (10^{-9})
even with 90% of malicious nodes

LOWEST ENERGY CONSUMPTION

3.6 Billion times less energy consumption than Bitcoin - 42000 times less energy consumption than Internet

CHEAPER FEES

0.1% of transaction amount with upper and lower transaction fee

NEW SMART-CONTRACT ERA

Most advanced and easy-to-program smart-contracts on the market fully based on UTXO (accountability)

QUANTUM-SAFE

Based on transactions-chains & derivation keys, all transactions have a different cryptographic key

DECENTRALIZED IDENTITY

Compatible with w3c standards (U2F) thousands of identities are able to interact with all apps & IoT without privacy disclosure

CRYPTO-BIOMETRICS

5 dedicated patents allowing to transform fingerveins network as the most secure cryptographic keys (full RGPD without any data storage)

PETA-BYTES STORAGE

Thanks to auto-repair and prediction mechanisms, all data are kept safe even with natural disasters

WEBSITES & E-COMMERCE

As unhackable as a blockchain transaction! all Identity, databases, payments, communication natively integrated, the Archethic ecosystem is designed to be a booster of the economy to lower the entry barrier

NFT

New era of art tokenization and royalties management

EMAILS & COMMUNICATION

Most secure emails, messages, call & videoconference solutions, all data are stored only once and encrypted (whatever the number of recipients)

ARCHETHIC PILARS

INTERNET OF TRUST

The Archethic mission is to provide the foundation of the Internet of Trust, based on a scalable, accountable & unbreakable decentralized network (Archethic Public Blockchain)

IDENTITY & PRIVACY

The purpose of Archethic Decentralized Identity is to bring back to humanity control over technology and to provide a better technological inclusion of the population by removing all the complexity through an unforgeable biometric identification

UNLIMITED DAPPS

The Archethic smart-contracts were designed to improve all the current apps (eCommerce, website hosting, voting and access) with smart contracts that can be modified, autonomous, self-triggered and with an unfailing reliability.

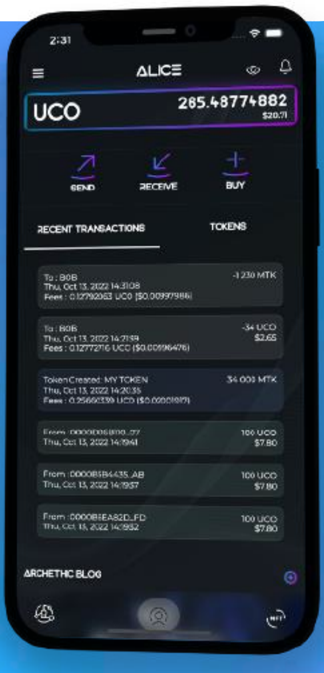
JOIN US

BUY UCO

TRAILER

APPS

ARCHETHIC WALLET



2:31

ALICE

UCO 285.48774882 $20.71

SEND RECEIVE BUY

RECENT TRANSACTIONS TOKENS

To : BOB Thu, Oct 13, 2022 14:31:08 Fees : 0.12792063 UCO ($0.00997986)	-1 230 MTK
To : BOB Thu, Oct 13, 2022 14:21:59 Fees : 0.12772716 UCO ($0.00996476)	-34 UCO $2.65
TokenCreated: MY TOKEN Thu, Oct 13, 2022 14:20:35 Fees : 0.25660339 UCO ($0.02001817)	34 000 MTK
From : 0000D06B10..77 Thu, Oct 13, 2022 14:19:41	100 UCO $7.80
From : 0000B5B4435..AB Thu, Oct 13, 2022 14:19:37	100 UCO $7.80
From : 0000B5EA82D..FD Thu, Oct 13, 2022 14:09:32	100 UCO $7.80

ARCHETHIC BLOG

Download on the App Store

GET IT ON Google Play

ARCHETHIC PUBLIC BLOCKCHAIN

WHITE PAPER / ONE-PAGER

OVERVIEW

Archethic Public Blockchain offers the first integrated services platform capable of meeting a fundamental need:

GIVING EVERYONE BACK THE CONTROL OVER TECHNOLOGY

In this way, Archethic is part of the promise of a safer, more inclusive, and truly decentralized world.

4 YEARS OF RESEARCH AND 12 STRONG INTERNATIONAL PATENTS endow Archethic with the technological attributes that its predecessors have lacked - scalability, speed, reliability and simplicity of native biometric recognition. These patents will be given to the open source community to foster participation and hence accelerate the pace of innovation.

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

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

ARCHETHIC GIVES BACK TO HUMANITY CONTROL OVER TECHNOLOGY, AND TO EACH INDIVIDUAL, CONTROL OVER THEIR IDENTITY.

BORN TO BE VIRAL

SMART-CONTRACTS UNCHAINED

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

THE FASTEST, SAFEST, AND MOST ENERGY-EFFICIENT BLOCKCHAIN

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

DECENTRALIZED IDENTITY GUARANTEEING PRIVACY

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

RELIABLE CRYPTOCURRENCY BACKED BY THE MOST ADVANCED SMART-CONTRACTS

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

COMMUNITIES AND ORGANIZATIONS

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

END-TO-END E-COMMERCE

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

SMART-CITY

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

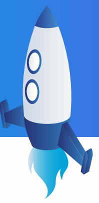
PROGRAMMABLE FINTECH

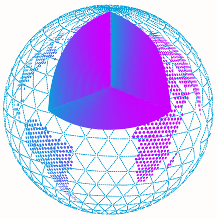
From community loans with automated repayment, to automated and impartial insurance, to payments by the touch of a finger.

SECURE HEALTH RECORDS

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

COMPETITIVE LANDSCAPE AND ARCHETHIC ADVANTAGE





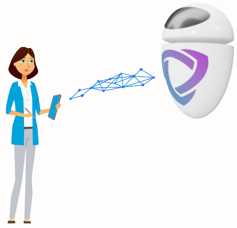
THE SAFEST, MOST SCALABLE, AND ENERGY-EFFICIENT BLOCKCHAIN THANKS TO THE ARCH CONSENSUS

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

	Validation Time	txn/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)	1.36s	10 Millions	-	66 %	yes	Random Secured Sharding	Account	yes	Gossip (UDP QUIC)
Archethic (ARCH)	5 sec.	Unlimitted	0.0001167 Wh/txn	97.5 %	no	Geo-Secured Heuristic Sharding	UTXO	yes	Supervised Multicast

SMART-CONTRACTS: AUTONOMOUS ROBOTS OF THE DIGITAL AGE

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



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

A DECENTRALIZED IDENTITY THAT RESPECTS OUR PRIVACY

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

THE END OF PASSWORDS AND UNNECESSARY MEDIA

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

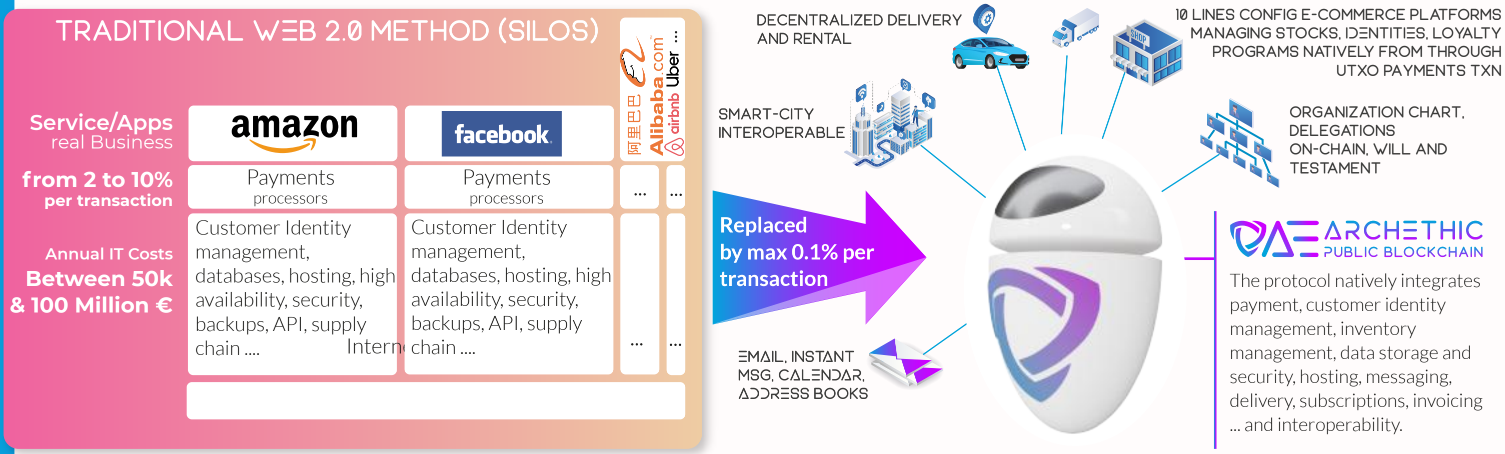
The biometric data from inside one of our fingers will generate several cryptographic keys that will never be disclosed and from which our digital identity will be encrypted. Only the person capable of regenerating one of these keys will be able to decipher their digital identity and hence prove their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

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

AN ALMOST UNLIMITED MARKET

THE RIVER ALWAYS CHOOSES THE MOST EFFICIENT ROUTE

THE TRUST REVOLUTION WILL UNLEASH A NEW GENERATION OF SERVICES



TRADITIONAL WEB 2.0 METHOD (SILOS)

	amazon	facebook	Alibaba.com 阿里巴巴	airbnb Uber ...
Service/Apps real Business				
from 2 to 10% per transaction	Payments processors	Payments processors	...	...
Annual IT Costs Between 50k & 100 Million €	Customer Identity management, databases, hosting, high availability, security, backups, API, supply chain	Customer Identity management, databases, hosting, high availability, security, backups, API, supply chain	...	...
	Internet			

Replaced by max 0.1% per transaction

DECENTRALIZED DELIVERY AND RENTAL

10 LINES CONFIG E-COMMERCE PLATFORMS MANAGING STOCKS, IDENTITIES, LOYALTY PROGRAMS NATIVELY FROM THROUGH UTXO PAYMENTS TXN

SMART-CITY INTEROPERABLE

ORGANIZATION CHART, DELEGATIONS ON-CHAIN, WILL AND TESTAMENT

EMAIL, INSTANT MSG, CALENDAR, ADDRESS BOOKS

ARCHETHIC PUBLIC BLOCKCHAIN

The protocol natively integrates payment, customer identity management, inventory management, data storage and security, hosting, messaging, delivery, subscriptions, invoicing ... and interoperability.

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

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

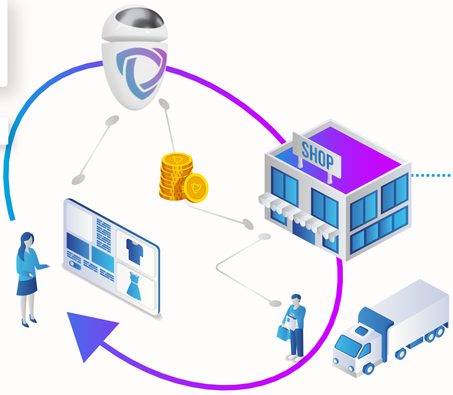
The Blockchain + Decentralized Identity model finally rationalizes this operating model by directly integrating all the layers necessary for the creation of new services.

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

Ξ-COMMERCE SMART-CONTRACT EXAMPLE

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

```
@Alice1 : ...
```



@MyShop : Stock : 100 T-shirts & 10 Pants

```
{
  "address": "@MyShop2,"
  "type": 3,
  "timestamp:"1557131179  ,
  "DATA": {
    "Ledger": {
      "UCO": [{ "fee": 1 }],
      "STOCK": [{
          "category": "t-shirt,"
          "description: "t-shirt eco 200g"
          "price policies": [{ "threshold:"10, "policy": "10%" }],
          "vouchers policies: [{ "vouchers": "NFT TOWN,"policy": "20%"}],
          "default price": 100,
          "pictures: [{ "url: "https://myshop.com/tshirt.png"}],
          "items:"[
            {  "id": "tbm", "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"
}
```

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

ROADMAP FOR THE FUTURE

THE ARCHETHIC NETWORK, THE ESSENTIAL BUILDING BLOCK AND CATALYST FOR THE CREATION OF A NEW WORLD OF SERVICES WITH PROVEN TRUST, INTEROPERABILITY, ACCESSIBILITY, AND CONTROL BY ALL.

BLOCKCHAIN PRODUCT LINE

2020

Cryptocurrency UCO (ERC20) **tradable**

2021

Smart-Contracts

Oracle/Prediction

Market Place Stock management & interfaces

Certification / Reputation

2022

Access Management Physical & Cyber

2023

Communication emails, calendar, instant messaging

Non-Financial Transactions

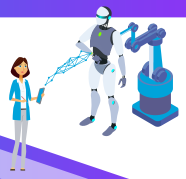
2024

E-Money License

2025

International Money Transfers

Cryptocurrency Liquidity of UCOs on exchange markets



Smart-Contract A Reference platform for the functionalities provided

ethereum

Decentralized Identity, communities & organization charts

Universal Market-Place Goods & Services, stock management, supply chain

Smart-City Mobility, public transportation, real estate, secured access

Olympics, sporting events ... Proof of Identity & Secured access management

FinTech Transfers, loans, insurance, UCO/€, biometric payments

Health Secure medical record, certification of medical practitioner

IDENTITY PRODUCT LINE

IDENTITY

Decentralized Identity FIDO2/W3C (Compatible with Gmail, Facebook ...)

Groups Organizations Delegation of power/hierarchy

Biometric Device

Connected Objects (IoT) Gateway

Industrialized Biometric Device

Rings/bracelets biometrics authentication derived

KYC / Certifications

Medical Record Secure and dematerialized constitution of the network of authorizations of the nursing staff, inviolable data storage, authorization management mechanisms...

THE UNDERLYING TECHNOLOGICAL REVOLUTION

ECONOMY DESIGNED TO GROW

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

SUITABLE FOR ALL APPS

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

SUSTAINABLE GOVERNANCE

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

DECENTRALIZED IDENTITY

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

GEO-SECURED DATA

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

UNBREAKABLE CONSENSUS

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

UNLIMITED P2P NETWORK

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

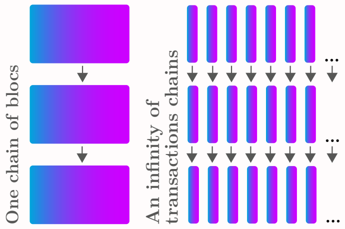
BLOCKCHAIN DESIGNED FOR GLOBAL USE

A TRULY DECENTRALIZED AND UNLIMITED NETWORK

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

Archethic solved these problems in the following ways:

INFINITE CHAINS OF TRANSACTIONS VS A SINGLE CHAIN OF BLOCKS Instead of chained blocks of transactions, each block is reduced to its atomic form, i.e. each block contains one transaction and each transaction will be chained in its own chain.

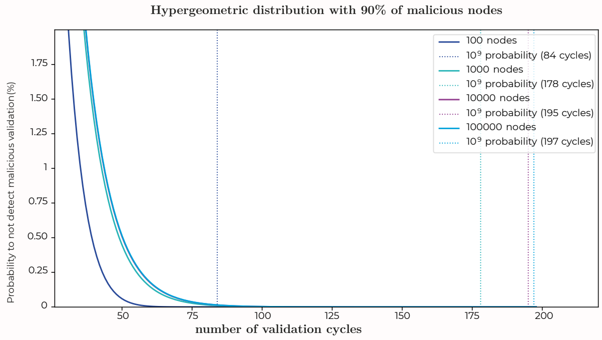


ARCH CONSENSUS: THE ABSOLUTE CONSENSUS ARCH or "Atomic Rotating Commitment Heuristic (ARCH)" is a new generation of Consensus. The detailed explanation of each concept of ARCH is as follows:

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

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

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



$$1 - \left[\lim_{N \to +\infty} P[X = k]\right] = 1 - \left[\lim_{N \to +\infty} \sum_{k=1}^{p} \frac{\binom{0.1 \times N}{k} \times \binom{0.9 \times N}{n-k}}{\binom{N}{n}}\right] \approx 10^{-9} = \ n \approx 200$$

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

PREDICTIVE, OPTIMIZED, GEO-SECURE REPLICATION SYSTEM CAPABLE OF SELF-REPAIR Instead of synchronizing transactions in a disorganized way across the entire network, each transaction chain will be stored in a reproducible and ordered way on a set of nodes - thus each node, independently, will know all the nodes hosting a given transaction and will thus be able to relieve the network by interrogating only the closest "elected" nodes. The election of storage nodes also includes the geographical position to ensure data security even in the event of a disaster in one or more geographical areas.

DISTRIBUTED NETWORK (P2P) WITHOUT SATURATION POINT Based on Supervised Multicasting, the peer-to-peer network uses a self-discovery mechanism based on incoming connections and the network transaction chain mechanism to maintain a qualified and trusted vision while generating a minimum of new transactions on the network.

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

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

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

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

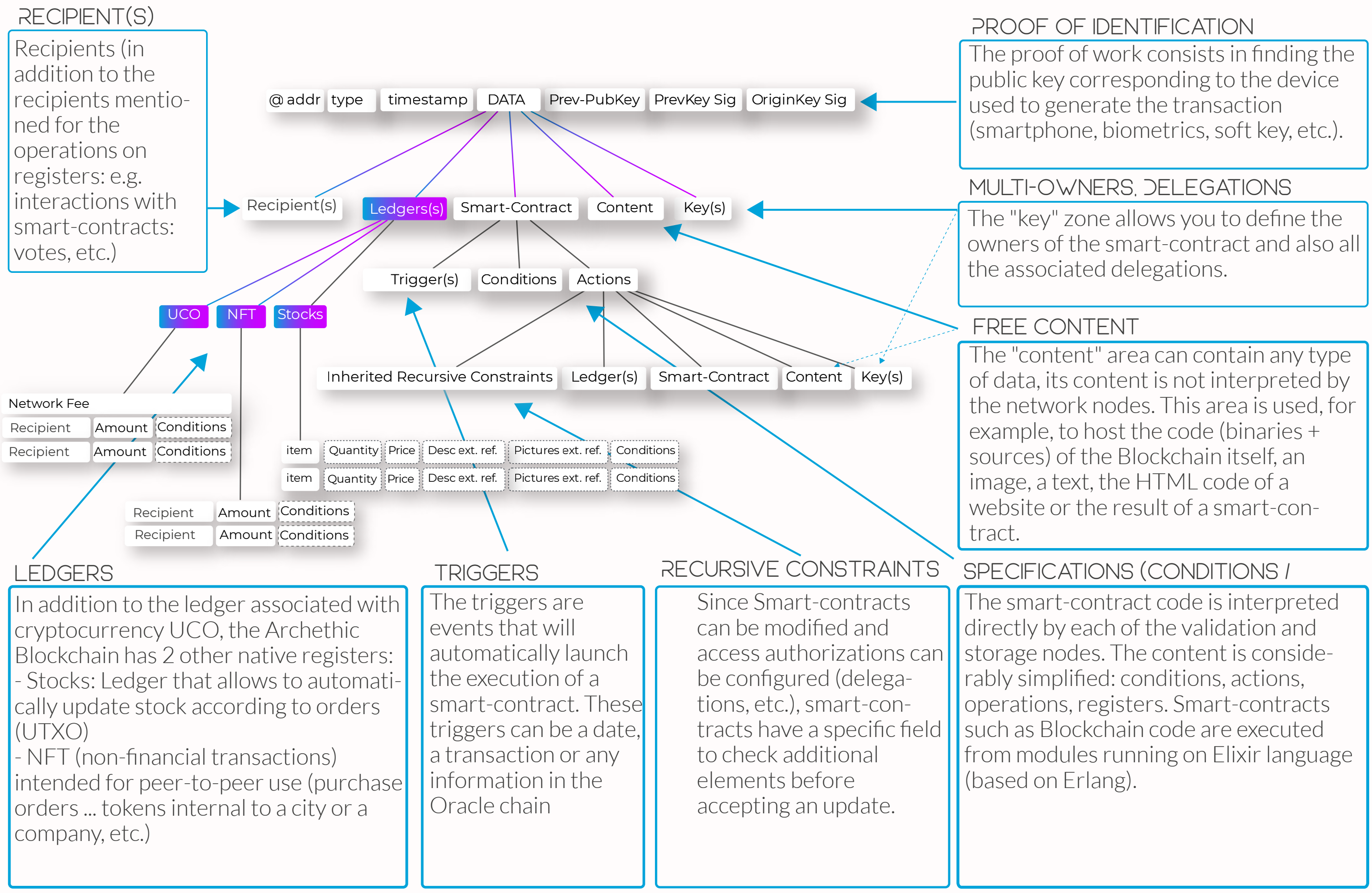
Read the Yellow Paper: https://archethic.net/Yellow-Paper.pdf

SMART-CONTRACTS
DESIGNED TO IMPROVE ANY APPLICATION OR SERVICE

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

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

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



RECIPIENT(S)

Recipients (in addition to the recipients mentioned for the operations on registers: e.g. interactions with smart-contracts: votes, etc.)

PROOF OF IDENTIFICATION

The proof of work consists in finding the public key corresponding to the device used to generate the transaction (smartphone, biometrics, soft key, etc.).

MULTI-OWNERS, DELEGATIONS

The "key" zone allows you to define the owners of the smart-contract and also all the associated delegations.

FREE CONTENT

The "content" area can contain any type of data, its content is not interpreted by the network nodes. This area is used, for example, to host the code (binaries + sources) of the Blockchain itself, an image, a text, the HTML code of a website or the result of a smart-contract.

LEDGERS

In addition to the ledger associated with cryptocurrency UCO, the Archethic Blockchain has 2 other native registers:
- Stocks: Ledger that allows to automatically update stock according to orders (UTXO)
- NFT (non-financial transactions) intended for peer-to-peer use (purchase orders ... tokens internal to a city or a company, etc.)

TRIGGERS

The triggers are events that will automatically launch the execution of a smart-contract. These triggers can be a date, a transaction or any information in the Oracle chain

RECURSIVE CONSTRAINTS

Since Smart-contracts can be modified and access authorizations can be configured (delegations, etc.), smart-contracts have a specific field to check additional elements before accepting an update.

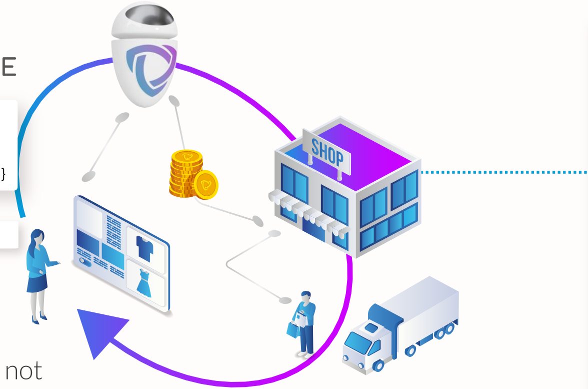
SPECIFICATIONS (CONDITIONS /

The smart-contract code is interpreted directly by each of the validation and storage nodes. The content is considerably simplified: conditions, actions, operations, registers. Smart-contracts such as Blockchain code are executed from modules running on Elixir language (based on Erlang).

E-COMMERCE
SMART-CONTRACT EXAMPLE

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

```
@Alice1 : ...
```



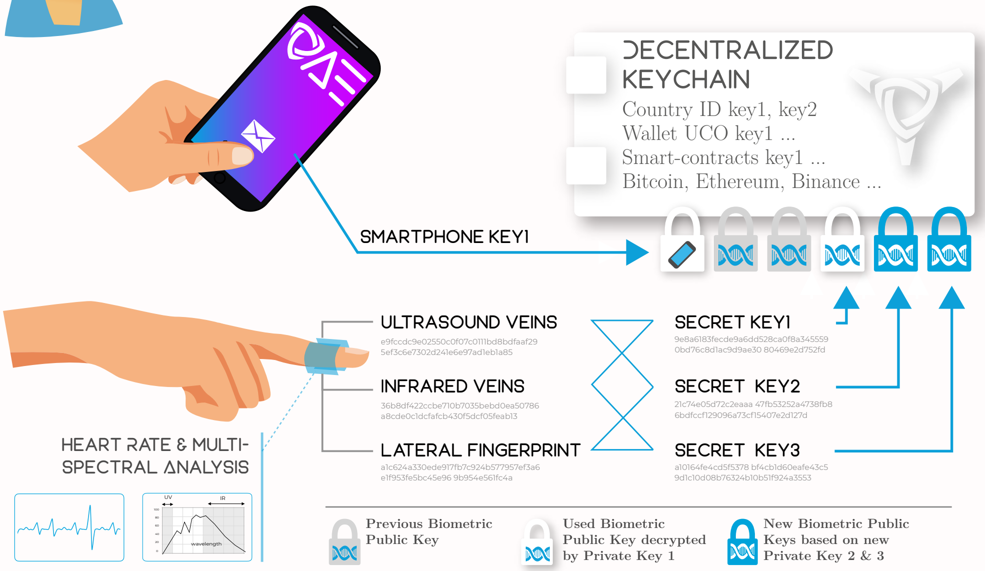
In the UTXO model, the only references are the validated transactions, for example, for a merchant site the stock status is not changed in the smart-contract itself but is reconstructed from the validated transactions. The experience of a user or a merchant is absolutely identical since each state is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

@MyShop : Stock : 100 T-shirts & 10 Pants

```
{
   "address": "@MyShop2,"
   "type": 3,
   "timestamp:"1557131179  ,
   "DATA": {
      "Ledger": {
         "UCO": [{ "fee": 1 }],
         "STOCK": [{
               "category": "t-shirt,"
               "description": "t-shirt eco 200g,"
               "price policies": [{ "threshold:"10, "policy": "10%" }],
               "vouchers policies": [{ "vouchers": "NFT TOWN,"policy": "20%"}],
               "default price": 100,
               "pictures": [{ "url": "https://myshop.com/tshirt.png"}],
               "items:" [
                 {   "id": "tbm", "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"
}
```

DECENTRALIZED IDENTITY AND BIOMETRICS

THE GRAIL OF MASS ADOPTION


DECENTRALIZED KEYCHAIN
Country ID key1, key2
Wallet UCO key1 ...
Smart-contracts key1 ...
Bitcoin, Ethereum, Binance ...
SMARTPHONE KEY1
ULTRASOUND VEINS
e9fccdc9e02550c0f07c0111bd8bdfaaf29
5ef3c6e7302d241e6e97ad1eb1a85
INFRARED VEINS
36b8df422ccbe710b7035bebd0ea50786
a8cde0c1dcfafcb430f5dcf05feab13
LATERAL FINGERPRINT
a1c624a330ede917fb7c924b577957ef3a6
e1f953fe5bc45e96 9b954e561fc4a
SECRET KEY1
9e8a6183fecde9a6dd528ca0f8a345559
0bd76c8d1ac9d9ae30 80469e2d752fd
SECRET KEY2
21c74e05d72c2eaaa 47fb53252a4738fb8
6bdfccf129096a73cf15407e2d127d
SECRET KEY3
a10164fe4cd5f5378 bf4cb1d60eafe43c5
9d1c10d08b76324b10b51f924a3553
HEART RATE & MULTI-SPECTRAL ANALYSIS
UV
IR
wavelength
Previous Biometric Public Key
Used Biometric Public Key decrypted by Private Key 1
New Biometric Public Keys based on new Private Key 2 & 3

AN AUTHENTICATION THAT CANNOT BE USED WITHOUT OUR KNOWLEDGE

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

WITHOUT KEY STORAGE

All current biometric identifications are based on the same principle:

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

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

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

DECENTRALIZED IDENTITY AND BIOMETRICS

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

- TAMPER-PROOF AUTHENTICATION
- NO KEY STORAGE (GDPR BY DESIGN)
- VITAL SIGNS MONITORING
- LEARNING MORPHOLOGICAL CHANGES
- DESIGNED FOR THE WORLD POPULATION

AN AUTHENTICATION OF THE WORLD POPULATION INDEPENDENT OF THE SYSTEM

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

AUTOMATIC LIFELONG LEARNING

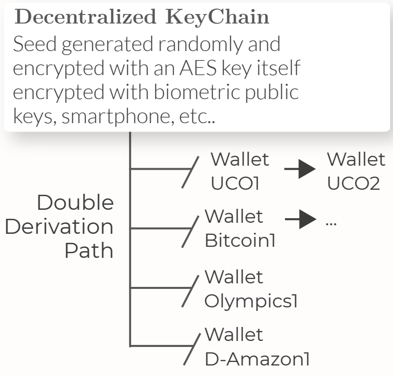
As shown in the figure above, the keys are generated in pairs from the biometric measurements. If one of the measurements is different (cut, burn, etc.) then only one key will match and can validate the authentication while the two new keys will be added to encrypt (via associated public keys) the decentralized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

PROOF OF THE ORIGIN OF THE AUTHENTICATION VIA

Identification on the Archethic network is not limited to biometric devices and, as shown in the figure above, each access method (smartphone, USB key, software key, etc.) will have its own certification method (see Yellow Paper Season 1). The identification method being associated with the transaction (see smart-contract schema: "OriginKey Sig") and the proof-of-work will thus allow adjustment of the required security with any smart-contract or portfolio - for example:

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

DECENTRALIZED AND INTEROPERABLE IDENTITY



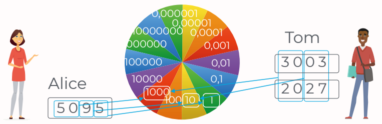
Decentralized KeyChain

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

Technically, the decentralized identity of a person or a connected object is made up of randomly generated Seed (root key) from which it is possible to generate all keys according to a path of derivation. So, for any access to a service or an application, a key will be calculated on the fly from the seed (root key) and the first public key associated with a service or an application. Thus allowing creating an infinite number of identities without even having to store related keys. All features associated with this decentralized identity will be detailed in the Yellow Paper Season 4: Automated address books, email, FIDO2.

ANONYMISATION & ACCOUNTABILITY BY DESIGN

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



GOVERNANCE (DAO)

A GOVERNANCE THAT INTEGRATES THE BEST OF EVERYONE

ON-CHAIN AND OFF-CHAIN DECENTRALIZED GOVERNANCE

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

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

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

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

DECENTRALIZED IDENTITY & PROOF OF IDENTITY

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

CODE «ON-CHAIN»

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

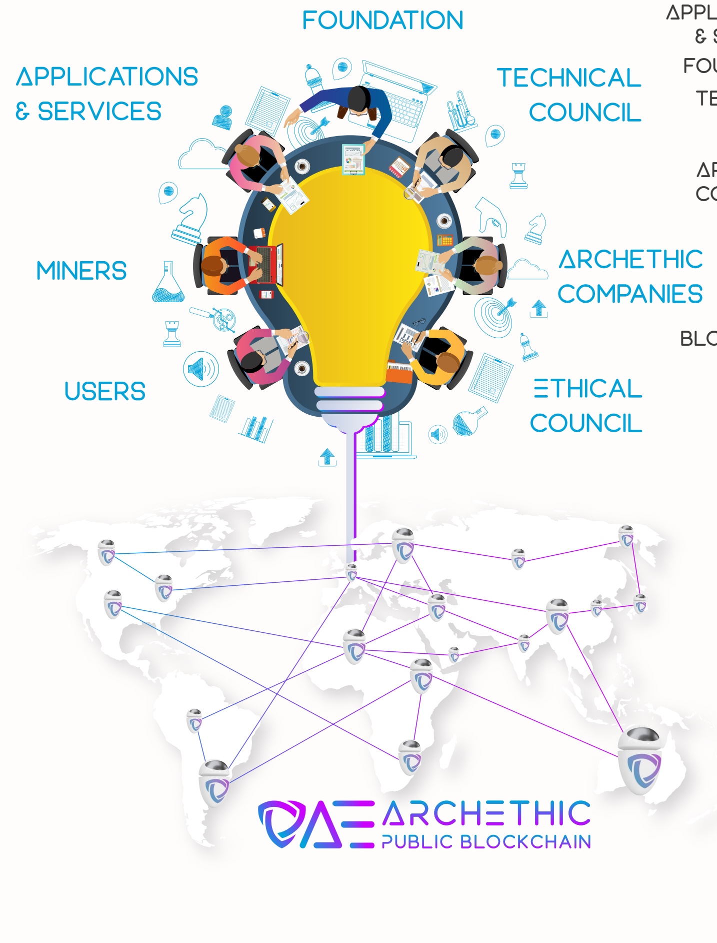
MODIFIABLE SMART-CONTRACT

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

INCENTIVES

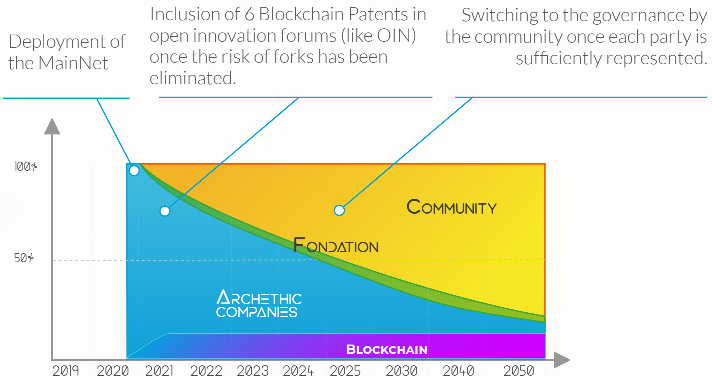
Financing of the work associated with updates, new features, and contributions is an essential element. The network has a reserve of one-third of the tokens (with progressive distribution constraints) for this purpose.

THE GOVERNANCE OF THE ARCHETHIC NETWORK IS BASED ON 8 DISTINCT GROUPS:



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

PLANNED GOVERNANCE BY THE COMMUNITY


Deployment of the MainNet

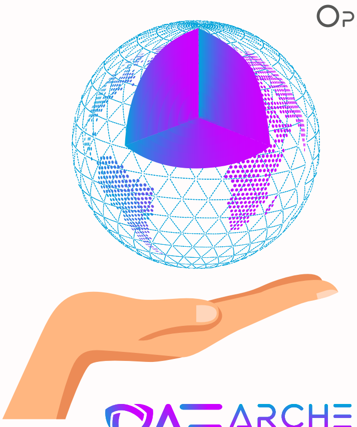
Inclusion of 6 Blockchain Patents in open innovation forums (like OIN) once the risk of forks has been eliminated.

Switching to the governance by the community once each party is sufficiently represented.

OPEN INNOVATION

PATENTS AS A PILAR OF A COMMON GOOD

Open Governance
Open Innovation
Open Source
Network



ARCHETHIC
PUBLIC BLOCKCHAIN

ARCHETHIC, A HUMANITARIAN AND COMMUNITY PROJECT

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

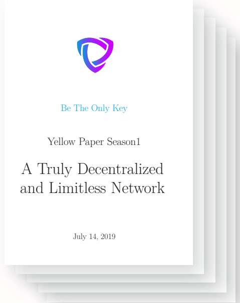
A VOLUNTARY STRONG PEDAGOGICAL APPROACH, GIVING EVERYONE THE OPPORTUNITY TO UNDERSTAND THE ARCHETHIC TECHNOLOGY

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

The first part, already published, describes the functioning of the network (Consensus ARCH, Supervised Multicasting (p2p) and all the mechanisms that have led to an unlimited network) :

https://archethic.net/Yellow-Paper.pdf

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



Be The Only Key

Yellow Paper Season1

A Truly Decentralized and Limitless Network

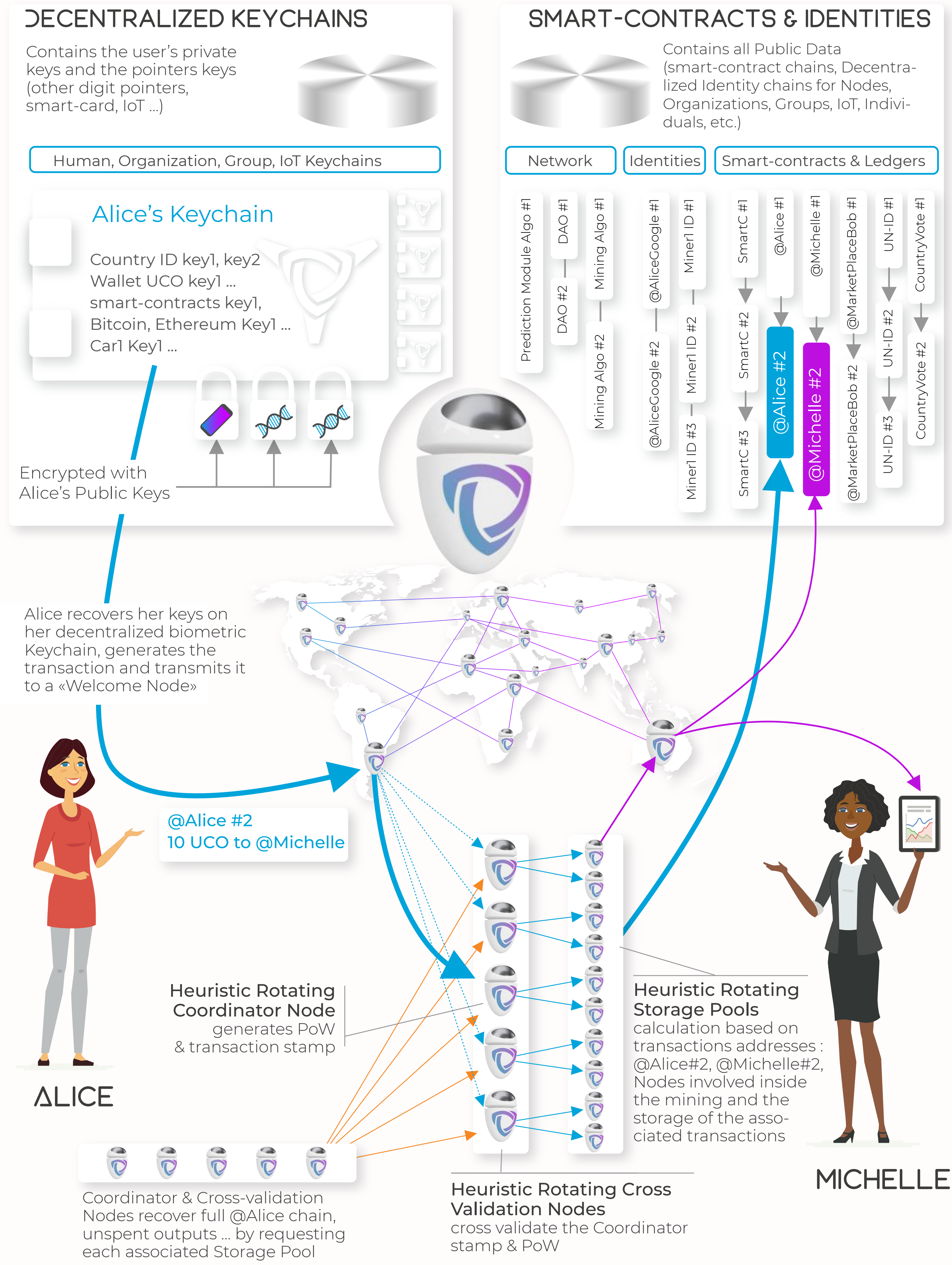
July 14, 2019

LIST OF PATENTS

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

BIG PICTURE

EXAMPLE OF CRYPTOCURRENCY TRANSFER



DECENTRALIZED KEYCHAINS

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

Human, Organization, Group, IoT Keychains

Alice's Keychain

Country ID key1, key2
Wallet UCO key1 ...
smart-contracts key1,
Bitcoin, Ethereum Key1 ...
Car1 Key1 ...

Encrypted with Alice's Public Keys

SMART-CONTRACTS & IDENTITIES

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

Network | Identities | Smart-contracts & Ledgers

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

@Alice #2
10 UCO to @Michelle

Heuristic Rotating Coordinator Node
generates PoW & transaction stamp

Heuristic Rotating Storage Pools
calculation based on transactions addresses : @Alice#2, @Michelle#2, Nodes involved inside the mining and the storage of the associated transactions

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

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