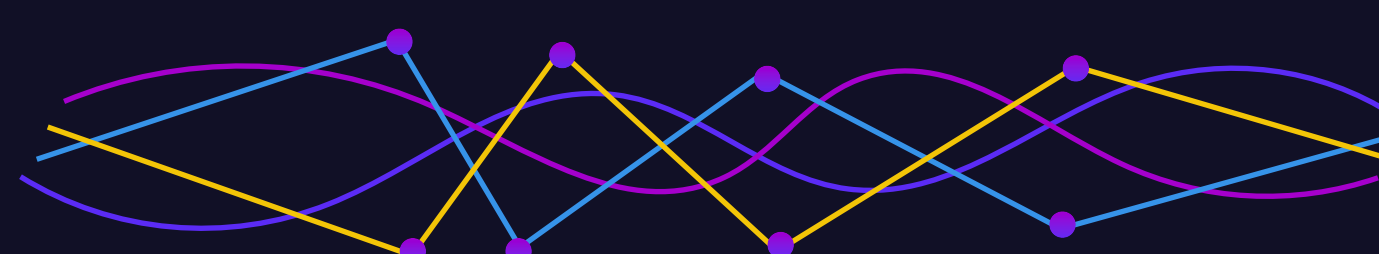


# Archethic

Digital sovereignty  
at your fingertips



Archethic  
Public Blockchain



2024



# ABSTRACT

Imagine a technology that not only simplifies your daily activities but also safeguards your security.

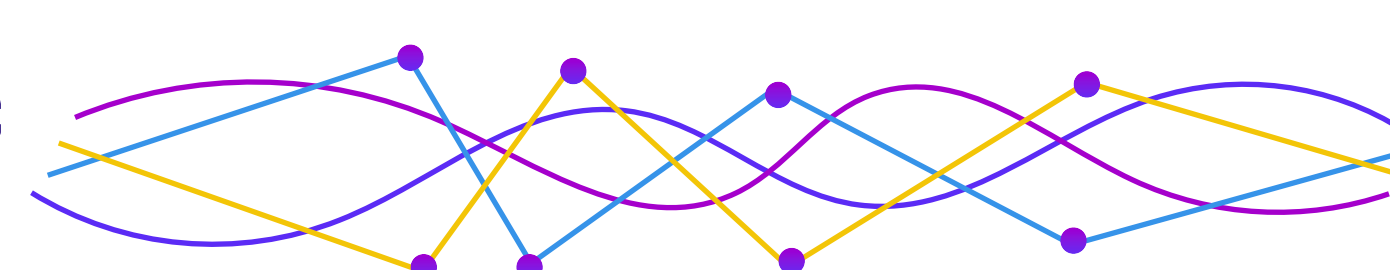
What if you could engage in creating wealth through technological advancements while focusing on your primary skills, not just technological knowledge?

Archethic aims to democratize access to all forms of technology with just a simple touch. Our team has engineered a highly secure, tamper-proof system, rivaling the security of a bank card chip. This innovation allows you to bypass traditional passwords, keys, or other authentication methods, using a unique biometric solution based on your fingerveins. Archethic's technology operates globally, free from any control or intervention by individuals, companies, or organizations. Rooted in opensource, we've enhanced blockchain technology to substitute any application or service, facilitating universal access to a suite of features including financial autonomy, data sovereignty, freedom of expression, decentralized identity, immediate payments, fractional ownership, collective health insights, smart cities, and more.

To foster a decentralized, autonomous network controlled by people worldwide, Archethic incentivizes participants (miners) who maintain network servers. These individuals validate transactions on the Archethic Public Blockchain.

The ecosystem is underpinned by its native cryptocurrency, \$UCO, created at the project's outset. This currency rewards development efforts, ensuring every contributor plays an integral role in the network's growth.

In an ever-changing world, your involvement is key to shaping the future of humanity through this groundbreaking technology.



# TABLE OF CONTENTS

**01.**

Vision

**02.**

Foundational Principles

**03.**

Archethic's Current Position

**04.**

Infrastructure Layer

**05.**

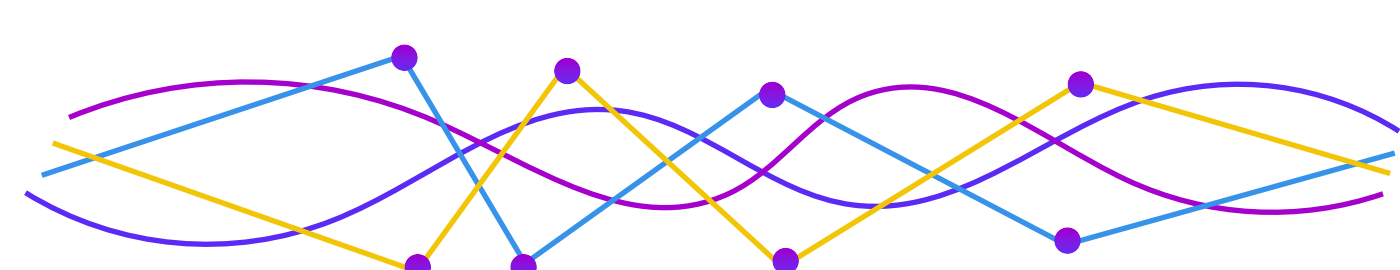
Trust Layer — Grail Of Mass Adoption

**06.**

Governance Layer — Community / Common Goods

**07.**

Archethic's Beating Heart : \$UCO





# VISION

## An almost unlimited market ...

Archethic unleashes a new generation of services moving away from the traditional Web2.0 silos supported by centralized models.

In the pre-historic model of the web (still prevalent since its 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

Archethic 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



Archethic stands as a pioneering platform, offering integrated services to fulfill a crucial purpose: Empowering everyone with control over technology.”

**Sébastien Dupont**  
CEO – CoFounder



## ... through unlimited Decentralized Services :

### Programmable Fintech

Streamline banking processes, offer cost-effective transactions, and facilitate decentralized lending and crowdfunding platforms.

### End-to-End E-Commerce

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

### 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.

### Energy

Improves patient data security, interoperability, and research capabilities, ensuring the authenticity and privacy of electronic health records.

### Smart-Cities

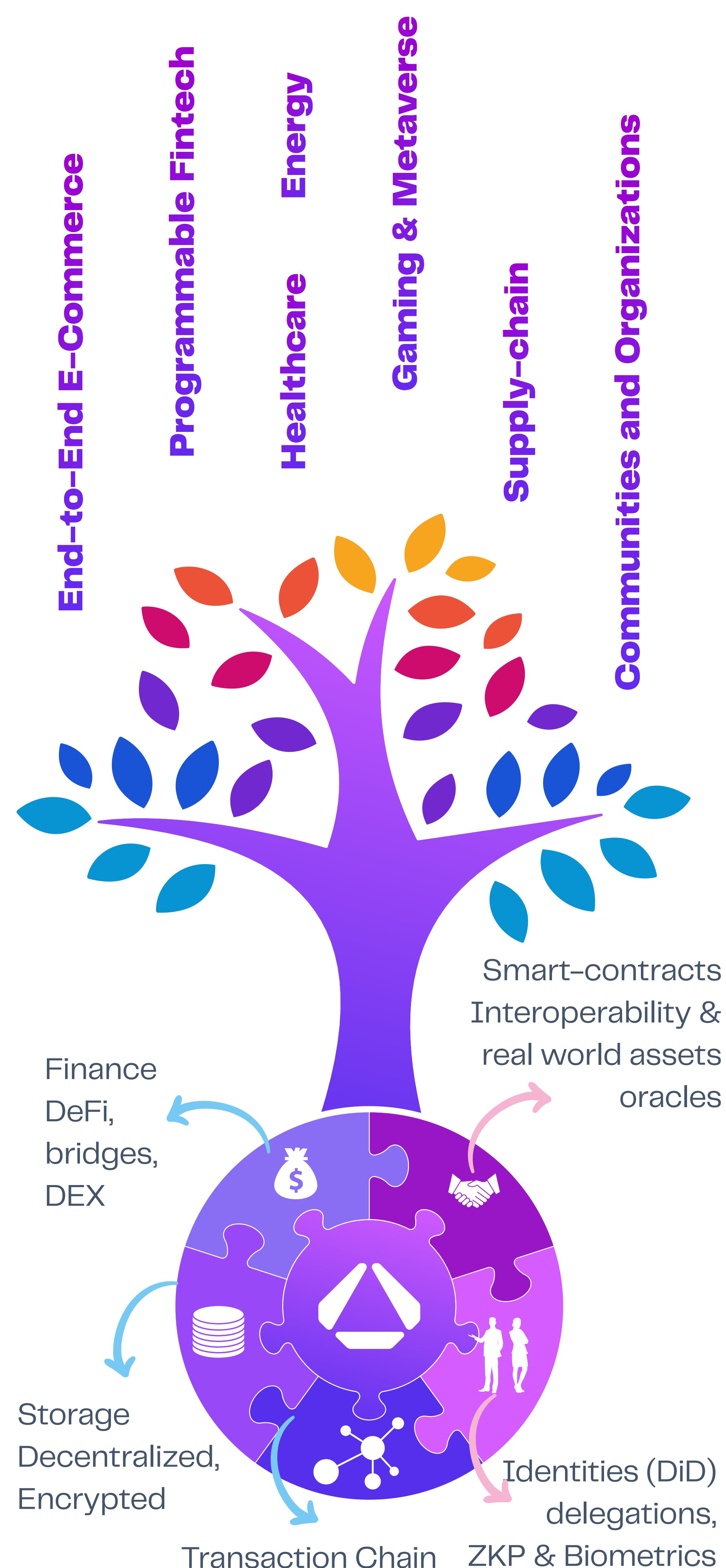
From automatic access to a hotel room or a car in the street without a key, to the metro without a ticket. Finally, it is possible to have a fluid interaction with our environment leveraging IoT.

### Healthcare

Improves patient data security, interoperability, and research capabilities, ensuring the authenticity and privacy of electronic health records

### Supply-chain

Enhances supply chain transparency,



traceability, and efficiency, preventing counterfeiting and reducing fraud.

### Gaming & Metaverse

Introduces new models of ownership and monetization in gaming, allowing the creation and trading of digital assets



# FOUNDATIONAL PRINCIPLES

## Internet of Trust – Cloud 3.0

Archethic's vision is to lay the groundwork for the Internet of Trust. It's anchored in a scalable, transparent, and invulnerable decentralized network—the Archethic Public Blockchain. This network is tailored for widespread adoption, featuring a novel, highly secure validation consensus (ARCH) capable of handling an unlimited number of transactions seamlessly.

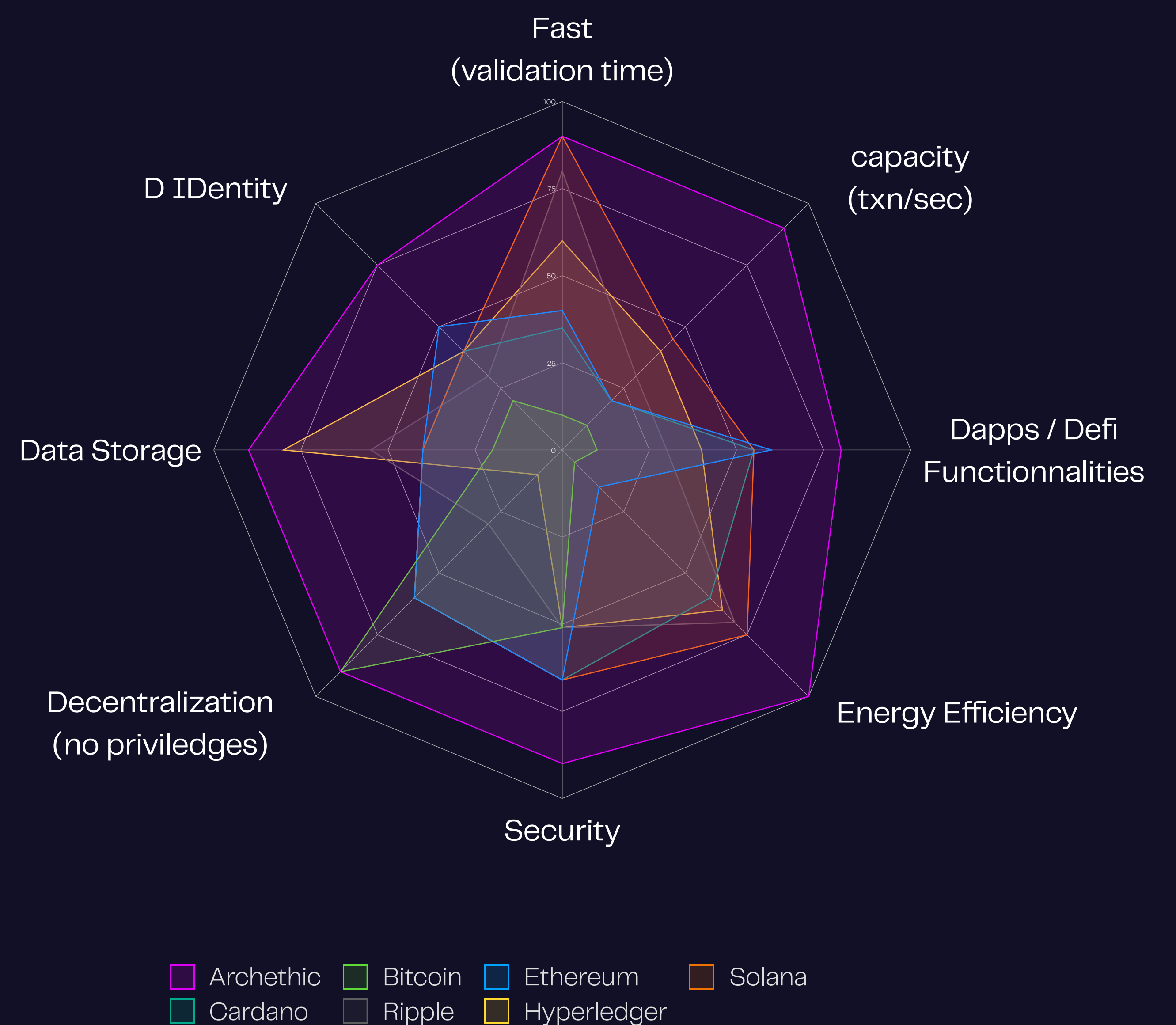
## Open Innovation

After four years of intensive research and securing 11 robust international patents, Archethic possesses key technological advantages over its predecessors: scalability, speed, dependability, and innate biometric recognition simplicity. These patents will be contributed to the open-source community, encouraging widespread participation and accelerating innovation.

Archethic is redefining technological engagement, giving back control of technology to humanity, and ensuring individual sovereignty over identity.

## Unlimited DApps

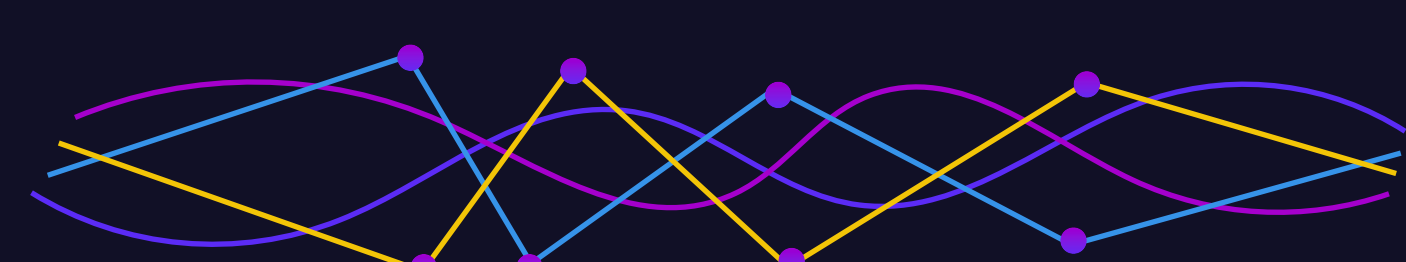
Archethic's blockchain is designed to not only replace but also enhance existing applications. It establishes a versatile, open ecosystem that transitions users from relying on centralized entities (like Facebook, Google, Amazon, Banks, etc.) to a decentralized framework. In this



framework, individuals maintain sovereignty over their data, assets, and privacy.

## Identity and Privacy

Archethic's Decentralized Identity initiative focuses on returning technological control to humanity. It aims to foster broader technological inclusion by simplifying processes through an unfalsifiable biometric identification system. This system inherently integrates biometric technology, using the complex inner patterns of fingerprints—a unique trait for each individual. Notably, it achieves this without storing any biometric data, ensuring privacy and security.





# ARCHETHIC'S CURRENT POSITION

## ARCH Consensus: Enhancing Safety, Scalability, and Energy Efficiency

For the first time, blockchain technology operates without a centralized authority, providing a system that's not just unbiased but also transparent and immutable. Archethic's innovative ARCH Consensus relies on the random selection of a small group of nodes (approximately 197 per 100,000) for transaction validation and storage. This approach, coupled with supervised multicasting, ensures efficient data location and a linear increase in transaction processing speed relative to network size, achieving about 100 times scalability. Below is a comparison with other blockchain technologies:

## Smart Contracts: Digital Age Automation

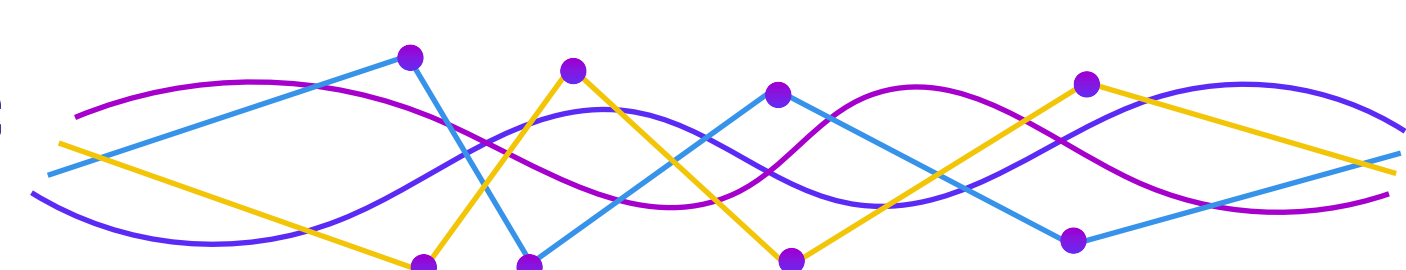
Smart contracts in the digital realm are akin to robots in the physical world, executing tasks based on specific triggers. Archethic's smart contracts represent a technological advancement. They are self-operating and can be activated by internal events (like dates, transactions) or external realities (via the Oracle channel, which is verified through consensus and cross-referencing). This includes variables like weather, stock market fluctuations, and news updates. These contracts are fully customizable, capable of managing diverse operations from stock control and payments to web hosting, all within the verified transaction framework (UTXO).

## Decentralized Identity for Enhanced Privacy

Archethic's decentralized identity system eliminates the reliance on third parties, like Google or Facebook, for identity management, preventing potential conflicts of interest and unauthorized data usage. Identity information is stored across numerous nodes, ensuring its longevity and integrity. This setup not only maintains privacy but also ensures interoperability with other applications. Combined with smart contracts, this decentralized identity becomes key to our interactions, facilitating access to various services (like public events, transportation, and messaging) without revealing identity specifics.

## Eliminating Passwords and Redundant Media

Archethic integrates biometric technology directly into the blockchain, enabling effortless and secure identification without storing any biometric data. This method uses biometric data from a finger to generate multiple cryptographic keys, which are never revealed. These keys encrypt the digital identity, accessible only to the individual capable of regenerating a key. This approach doesn't just exhibit technological finesse by generalizing biometrics safely; it also addresses blockchain's widespread adoption challenge, removing conventional barriers like passwords.





# INFRASTRUCTURE LAYER

## THE TECHNOLOGICAL LAYER : ARCHETHIC'S TRANSACTION CHAIN

Archethic addresses the challenges of scaling blockchain technology for worldwide adoption. Traditional blockchains struggle to integrate billions of transactions into a single block chain, and no consensus method can universally verify such a vast number of transactions across all network nodes. Additionally, current peer-to-peer (P2P) networks can't consistently ensure data freshness on asynchronous networks without significant slowdowns, such as the excessive computation of block nonces (Proof of Work) seen in Bitcoin's network. Archethic's innovative solutions include:

### ARCH Consensus

Atomic Rotating Commitment Heuristic

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

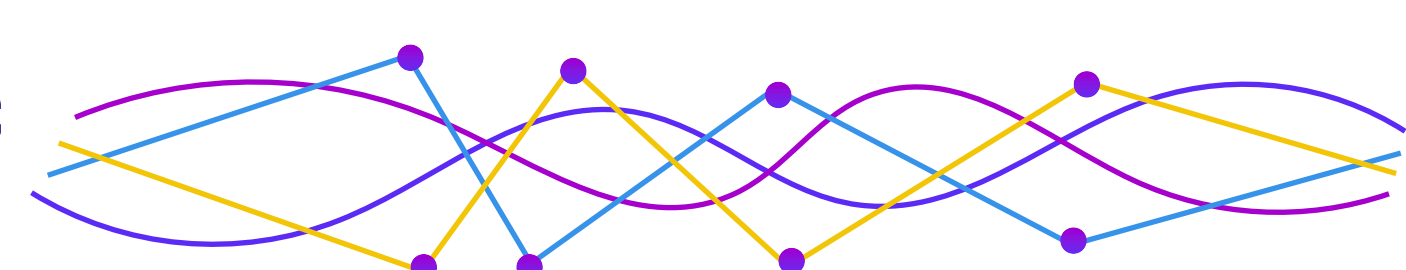
**Heuristics** is the set of algorithms, software, and parameters that manage the entire network, allowing the network to elect, in a decentralized and coordinated way, the nodes in charge of validating and storing transactions chains.

**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.



“We are building a scalable, simple, and sustainable infrastructure that will catapult the digitalization of services that have remained excluded due to commercial and technological barriers.”

**Niles Patankar**  
COO – Co-Founder





# TRUST LAYER

## Grail Of Mass Adoption

### **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.

### **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.

### **Automatic lifelong learning ... Without key storage**

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**

Current biometric identifications involve

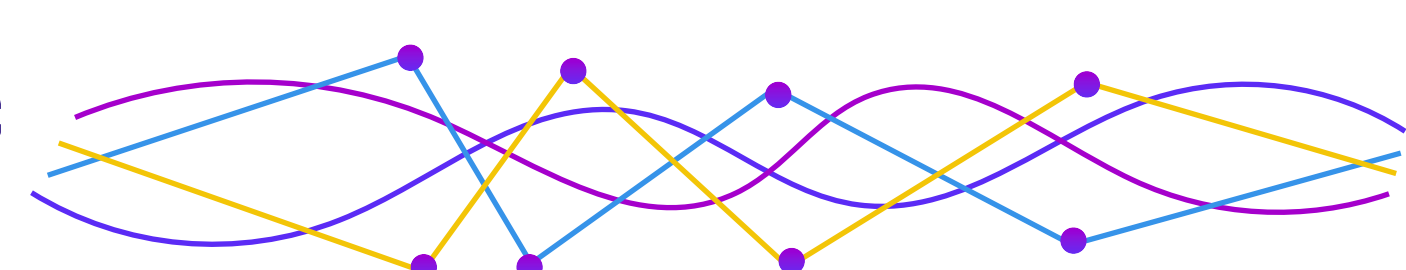
capturing and storing recognition data, comparing measurements with patterns, and identifying individuals if they exceed a certain threshold. However, the Archethic biometric device generates private cryptographic keys on the fly, eliminating the need to store data for comparison. Identification tolerance is ensured through a learning mechanism, and authentication is done through cryptography, making software attacks futile.

### **Decentralized+Interoperable Identity**

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.

### **Anonymization+Accountability by Design**

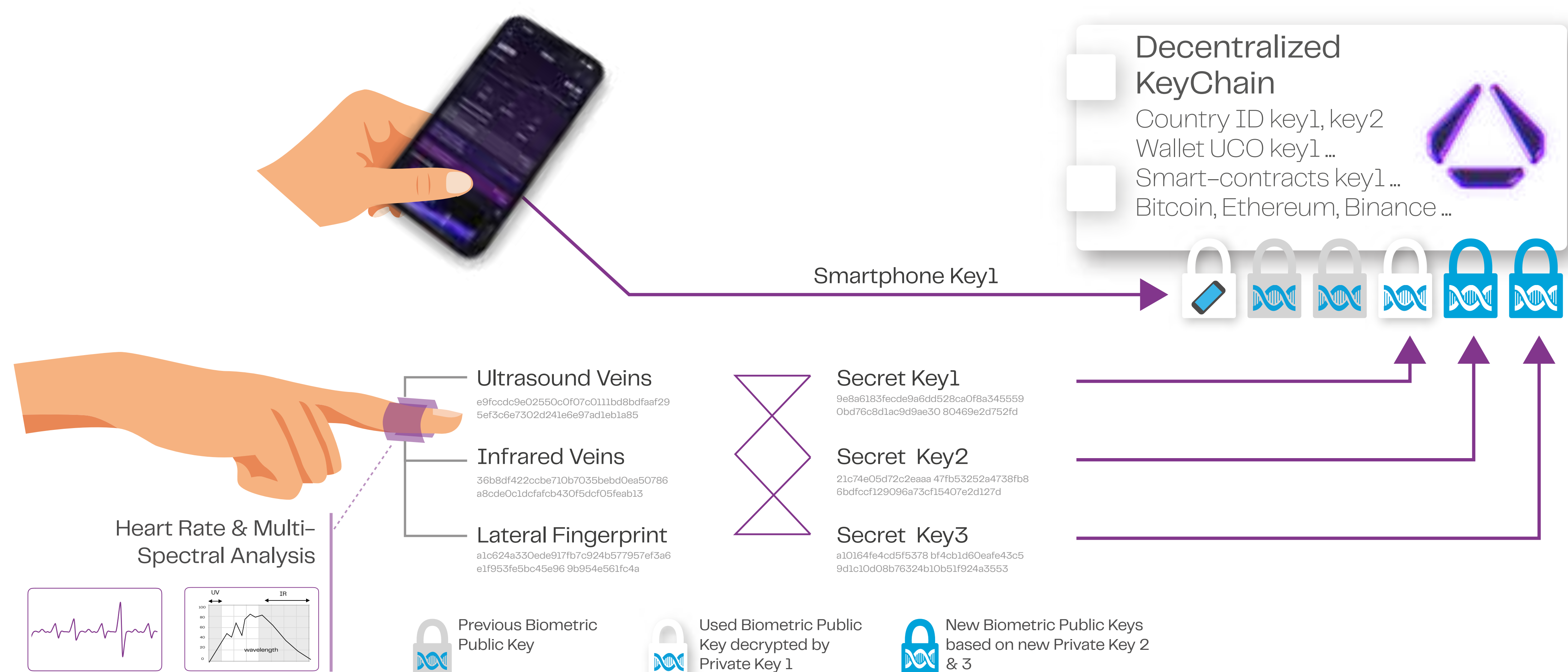
As all transactions are public, the network has a mechanism called the "Wheel of Privacy" to remove correlations between the sender, the recipient, the time, and the amount of transaction. This mechanism is used in particular for electronic voting and allows everyone to keep their vote private without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





# TRUST LAYER

## Grail Of Mass Adoption



### 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 ... Without key storage

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.

### An authentication that cannot be used without our knowledge

Unlike fingerprints, irises or faces can easily be reproduced and falsified from a photo on Facebook or in the street but it is not possible 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.

### Decentralized+Interoperable Identity

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 ever creating related keys.



# GOVERNANCE LAYER

## Community / Common Goods

The governance of a Decentralized Autonomous Organization (DAO) is a crucial challenge for Blockchains. The Bitcoin network has the most advanced decentralized governance, but it is based on a single type of actor – the miner or the largest pool of miners. This ignores a significant part of the ecosystem, including users, application providers, technical contributors, and even the Blockchain itself.

Archethic's governance is based on technical and functional fundamentals to survive and adapt to changes in society, including on-chain and off-chain decentralized governance, including all of the following actors :

### 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

### 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.

### Technical Council

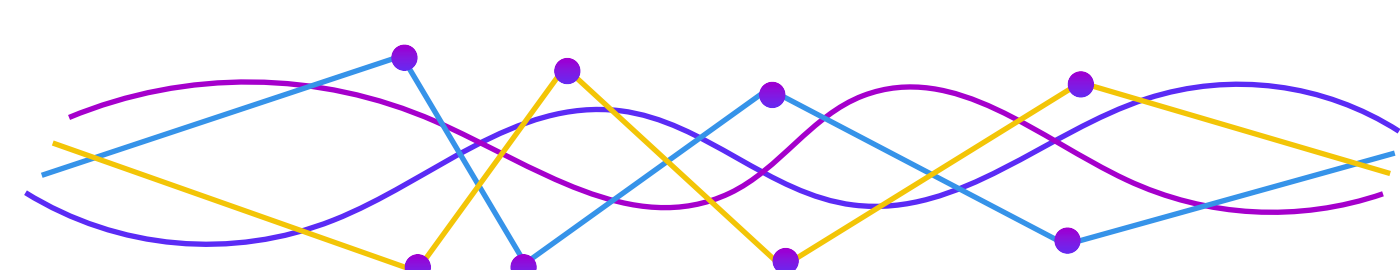
Composed of the "core developers" with a weightage based on the importance of their code contribution

### 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.

### Archethic companies

As the creators/guardians of the network





# ARCHETHIC'S BEATING HEART : \$UCO

## Network Funding – 38.2%

Used by the foundation to fund the network development. It includes the circulating supply of 216M, remaining will be used to fund the future blockchain development.

## Adoption Rewards – 23.6%

Under the control of the DAO, this wallet is dedicated to promote the use of the Archethic Public Blockchain (incentives for core & dapps developers, grants for new services and rewards for end users by using services).

## Team & Advisors – 14.5%

2 years cliff from TGE with 60 months linear release with holding incentives & 3 years Cliff from TGE + 60 Months linear release

## Staking Rewards – 9%

9M UCO per year distributed amongst people staking.

## Exchange Liquidity – 5.57%

CEX & DEX Liquidity

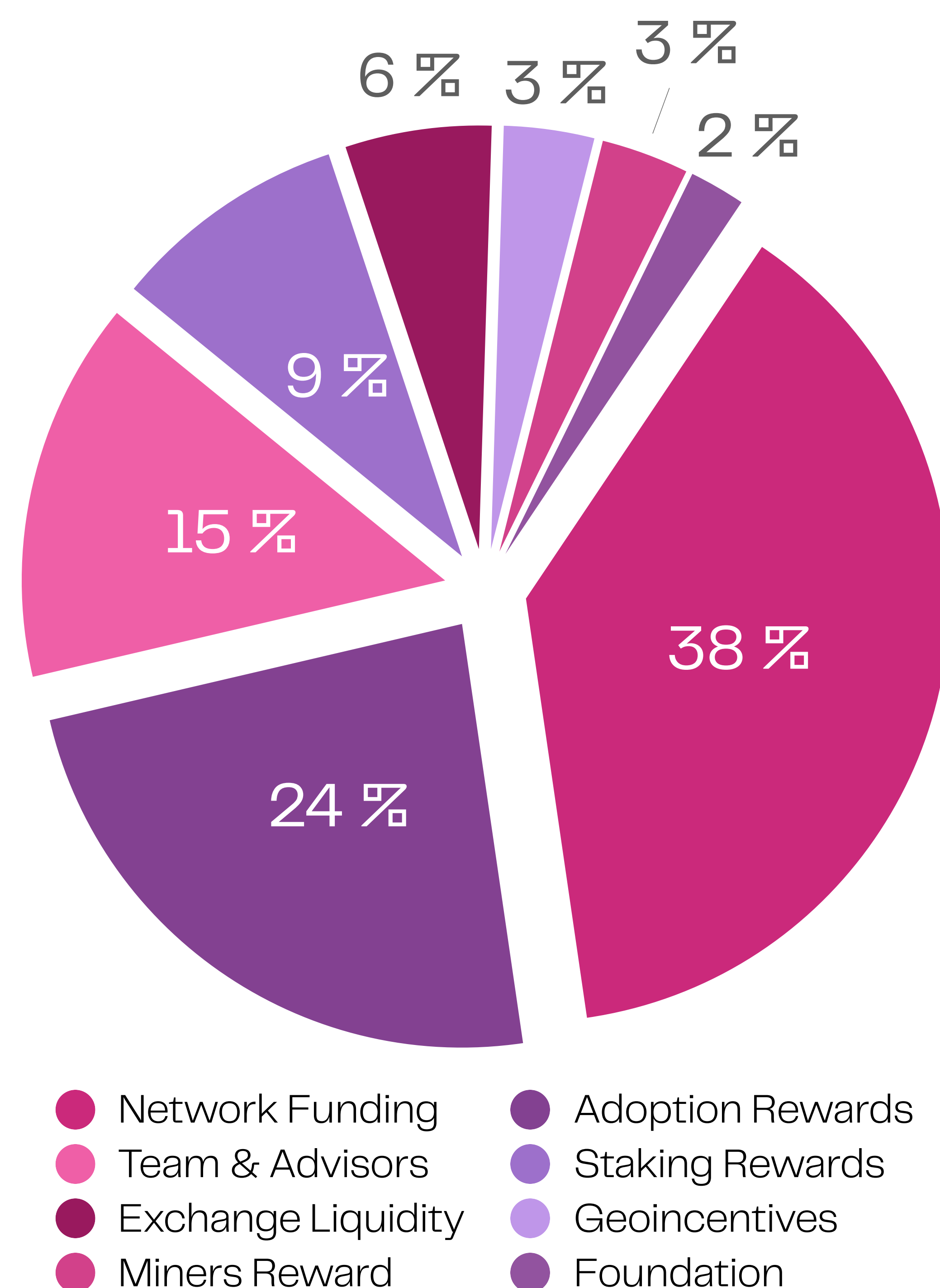
## Gamification & Geoincentives – 3.44%

Gamification can be used to incentivize network participants and reward nodes in areas not currently on the network.

## Dynamic Miners Reward – 3.34%

Supplements the transaction fees to pay fixed miner incentives until transactions fees > miners rewards. This pool helps the network through bootstrap phase leading to equilibrium and deflation.

## Foundation – DAO – 2.13%



## 90% SUPPLY BURN

After initial listing without public sale, our circulating supply compared to fully diluted supply was divergent from market standards, affecting investors trust. The core objective is the creation of self-sustaining network without compromising the trust. Based on the simulations, it has been concluded that a thriving economy can be created by redistribution of tokens and burning the excess. Archethic would be one of the few listed public blockchains to announce a burn of 90% of its tokens. This number is not a marketing ploy, it is supported by the design work done to achieve self-sustenance.

Burn : 90% of total supply (10 Billion)

Smart-contract: 0x8a3d77e9d6968b780564936d15B09805827C21fa



# JOIN OUR COMMUNITIES !

JOIN US

## Join the Community

Connect, collaborate, and engage with like-minded individuals in the Archethic community.

 Github

 Discord

 Telegram

 Twitter

 LinkedIn

 Instagram

 Medium

 YouTube



Archethic  
Public Blockchain

