.arianee

Smart-Link connecting owners, assets, and brands.

WHITE PAPER

Table of Contents
Arianee White Paper

Arianee's mission is to build the first *perpetual, anonymous and trusted record* all the world's asset, enabling a revolutionary link between owners and brands.

Arianee aspires to become the world's leading universal protocol for the creation and transfer of *digital certificates of ownership and authenticity for objects.*

All subsequent-generation owners will manage the journey of their valuable assets through time while maintaining contact with their creators: the Smart-Link.

....

"**Tomorrow, the ownership of our assets will be safely stored in a blockchain, making robbery a word of the past, and bringing augmented features to your physical goods.**"

•

Introduction
Mission statement

A rianee offers the opportunity to add a new layer of trust in the certification of goods to existing layers (paper certificates, RFIDs, holograms, etc.) – without asking a brand to set its current processes aside – by creating a certificate and allowing other parties to grant it to the original owner of a product.

Arianee adds a unique paradigm to this eternal battle against counterfeiters and pirates: from now on, the ability to verify a product's authenticity and origin will be distributed widely to a range of stakeholders. There is no doubt that having a digital asset linked to the physical product will significantly reinforce an owner's or potential purchaser's trust in the authenticity of the product. Along with the respective physical asset and its physical certificate, there will be a digital asset that adds an incontrovertible layer of insurance.

Because the paradigm uses blockchain technology, the asset is published in a unique chain and is directly linked to a single physical serial number. Rather than resting solely with brands, the burden of vouching for a product's authenticity is now shared by everybody and accessible to anyone.
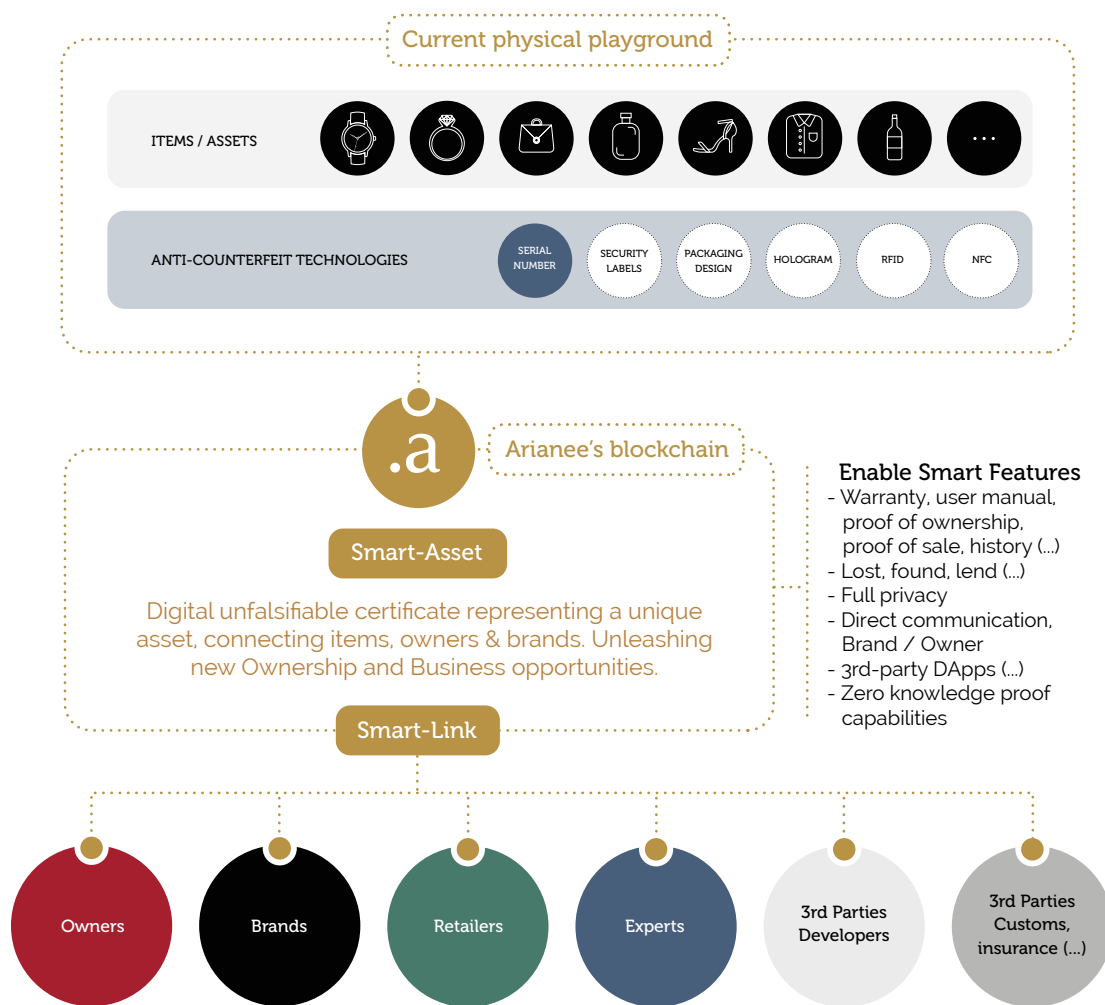
Arianee Open Source Protocol

Introduction
Problem statement

Owners

Storing a product's relevant documentation is often done using physical paper, which can be misplaced or destroyed in an accident.

Some brands offer product registration that will prove ownership. However, the owner has no control over how this information is used and access is restricted by a brand's terms of use. Moreover, each brand provides its own system and owners need to register their ownership in multiple incompatible proprietary databases with different user interfaces.

Owners need a simple solution allowing them to securely store their products' proof of ownership, authenticity and other documentation, like warranties, in one place. They also have to retain complete control over how, when, and by whom this information can be accessed.

Brands

Brands maintain customer relationship management (CRM) technologies to record interactions between individuals and the brand's employees or other communication channels. Due to the fragmented nature of the distribution network, customer records are often unreliable and even, in some cases, non-existent.

The current owner of a product is often unreachable by the brand as products can change hands after purchase. This can lead to mistargeted communications if a product was, for example, purchased as a gift or resold on the second-hand market.

Brands need a solution that would allow them to have an open communication channel with a product's current owner at all times. Although it may sound obvious, the ability to maintain direct contact with the owners of its products - without an intermediary - is a great leap forward for brands.

Ultimately, maintaining a permanent link with a product's owner will allow a brand to better address grey market activities and to protect distribution networks from fraudulent actors.
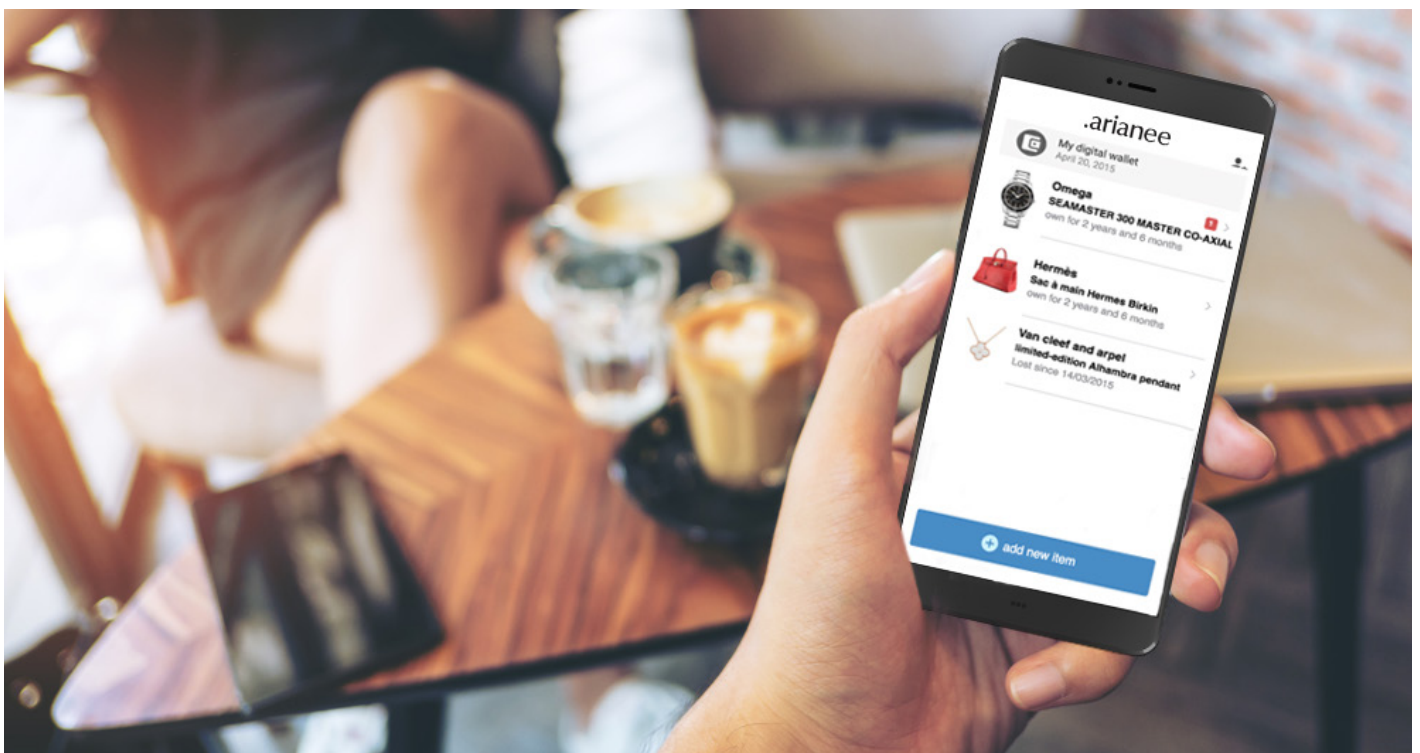
Introduction

Arianee platform

The Vault

The Vault is an easy-to-use online repository where owners can register all their products free of charge. Information entered by owners is stored on the Arianee blockchain, which assures that it cannot be changed by a third party.

While the Arianee blockchain is accessible to anyone, all information in a user's Vault is encrypted using time-tested encryption methods to protect the owners' privacy. Furthermore, the integrity of the information stored on the blockchain is certified by zero-knowledge proof technology (once it's ready).

Smart-Link

The Smart-Link is a process that gives owners full control of how they give access to their Vaults. They can choose which data they share, with whom and under which conditions. Numerous types of operations are allowed by the Smart-Link, from simple read access to delegation of authority.

Authenticity is at the core of Arianee's value proposition and therefore, smart authenticity is the primary signature in the Arianee protocol. Verified brands can authenticate products stored in a Vault at the owner's request. As long as the authenticity is valid, the brand maintains a communication channel open with the product owner regardless of future changes in ownership.

Community – business partner toolkit

While the Arianee platform can be used on its own, it is even more powerful when used in coordination with legacy IT systems (ERP, CRM, etc.) or other distributed ledger platforms. The ecosystem toolkit will facilitate the creation and distribution of decentralized solutions built by developers (SAP, Accenture, IBM, etc.) on the Arianee protocol.

Smart-Asset

Products registered on the Arianee blockchain are displayed as "Smart-Assets". The Smart-Asset lists all the products' proof of ownership, authenticity and other documentation, like warranties. Each Smart-Asset is unique, immutable and transferable between Vaults.

Brand Data Hub

The data hub is the center of brands' interactions with the Arianee platform. It provides product life analytics in three core modules:

- The Product Registry, where brands manage authenticated objects.
- The Communication Center, where brands reach out to product owners.
- The Distribution Network Management System, where brands interact with their distribution networks.

Introduction
Blockchain

Proof of Authority protocol

Anybody can run a public node that allows them to verify all data recorded on the Arianee blockchain. While everybody can verify the blockchain, Arianee uses a Proof of Authority protocol to record new information. Authority nodes are the only nodes allowed to seal blocks on the Arianee blockchain. Arianee will be launched with a large number of pre-approved authority nodes. New authority nodes have to be voted in by already-approved authority nodes. This system assures that a malicious miner cannot inflict damage on the network. This allows the Arianee network to run faster than a classic proof of work protocol as node computing power is only used for processing transactions.

Arianee will deploy its own Proof-of-Authority Ethereum-based permissioned blockchain.

Token model

The ARIA token is the basis of the Arianee protocol. It is an ERC20 token traded freely on exchanges. The token is used to pay for paid features on the Arianee protocol.

Recent examples with Bitcoin and Ethereum show that token price volatility can lead to wild fluctuations in transaction costs on blockchain platforms. This is an obstacle for user adoption as it becomes difficult to predict the cost of a future transaction with a high degree of certainty, which is not conceivable for companies.

In addition to our token, ''Gas'' will be used to secure the blockchain and prevent spam and malicious behavior. This Gas will be provided under circumstances to be determined.
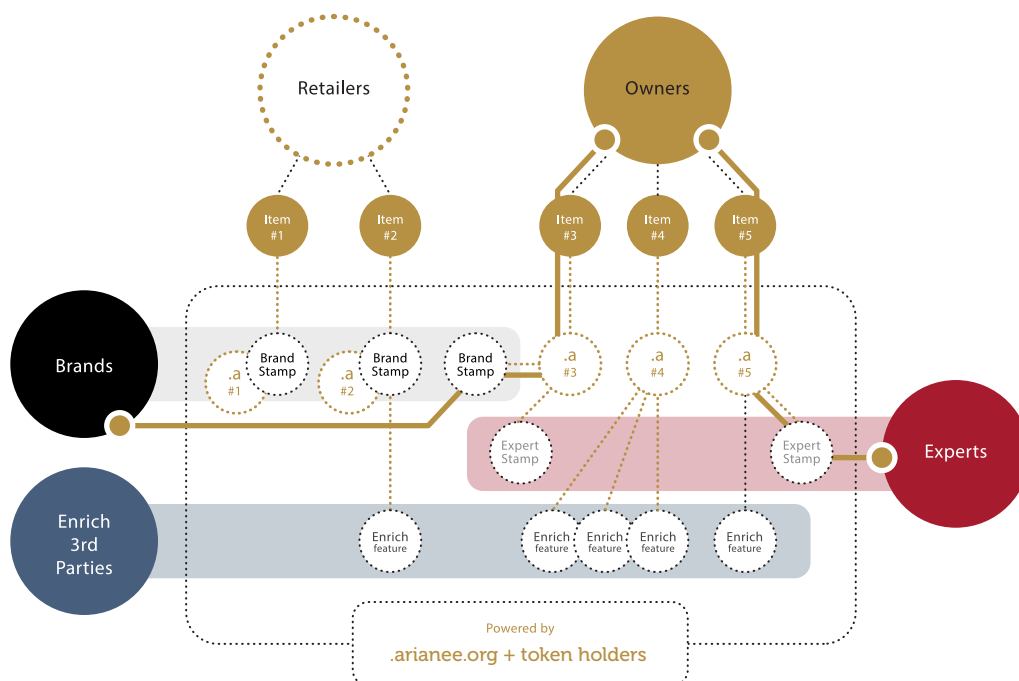
Arianee's ecosystem

Problems with current product records

Authenticity and the fight against counterfeiting

Society has struggled with counterfeiting for millenia. It's sometimes tempting to take the rather cynical view that the marketing of fake products is natural human behavior. In many cases, there are significant rewards to be reaped from counterfeiting or pirating the goods produced by quality brands.

However, taking credit for the R&D successes of others or copying innovations and breakthroughs that have been developed by others has a large negative impact on health and safety, social structure, innovation, and economic activity.

Unfortunately, studies from the OCDE reported a substantial increase in counterfeiting trends[1]. Between 2008 and 2013, counterfeiting increased from 1.9% of the total volume of international trade to 2.5%, a figure that represents more than 460 billion dollars worth of transactions[3]. Research conducted by Frontier Economics extended those figures with the addition of domestic production and consumption of counterfeit goods and the digital piracy of films, music

and software, bringing the total value of counterfeit goods to about a trillion dollars.

Millions of jobs worldwide[4] have been eliminated due to counterfeit black markets and the potential profitability of illicit trade increasingly attracts organized crime, with costs from related criminal activity estimated at some 60 billion dollars. Moreover, local workers are exploited by becoming unwitting participants in counterfeiting and piracy schemes.

Finally, for governments, counterfeiting means lost tax revenue, higher unemployment and expenses associated with compliance with anti-counterfeiting legislation, and the need to react to public safety threats and labor market distortions.

> " **The negative impacts of counterfeiting and piracy are projected to drain \$4.2 trillion from the global economy and put 5.4 million legitimate jobs at risk by 2022.**[1] "
>
> **Jeff Hardy** | International Chamber of Commerce

....

– 1 "Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy - World Trademark Review," May 18, 2017.
http://www.worldtrademarkreview.com/Intelligence/Anti-counterfeiting/2017/Introduction/Estimating-the-global-economic-and-social-impacts-of-counterfeiting-and-piracy.

– 2 Frontier Economics. "ICC-BASCAP-Frontier-Report-2016-," 2016.
https://cdn.iccwbo.org/content/uploads/sites/3/2017/02/ICC-BASCAP-Frontier-report-2016.pdf.

– 3 "Global Trade in Fake Goods Worth Nearly Half a Trillion Dollars a Year - OECD & EUIPO - OECD." April,18,2016. http://www.oecd.org/industry/glo al-trade-in-fake-goods-worth-nearly-half-a-trillion-dollars-a-year. htm.

– 4 "Trade in Counterfeit and Pirated Goods | OECD READ Edition." OECD iLibrary. 2016 edition.
http://www.keepeek.com/Digital-Asset-Management/oecd/governance/trade-in-counterfeit-and-pirated-goods_9789264252653-en.

Problems with current product records

ESTIMATE	2013	2022 (forecast)
Total international trade in counterfeit and pirated goods	$461 billion	$991 billion
Total domestic production and consumption of counterfeit pirated goods	$249 - $456 billion	$524 - $959 billion
Digital piracy in movies, music and software	$213 billion	$384 - $856 billion
- Digital piracy in film	$160 billion	$289 - $644 billion
- Digital piracy in music	$29 billion	$53 - 117 billion
- Digital piracy in software	$24 billion	$42 - 95 billion
Total value of counterfeit and pirated goods	**$923 billion - 1.13 trillion**	**$1.90 - $2.81 trillion**
wider economic and social costs		
- Displacement of legitimate economic activity	$470 - $597 billion	$980 - $1244 billion
- Estimated reduction in FDI	$111 billion	$231 billion
- Estimated fiscal losses	$96 - $130 billion	$199 - $270 billion
- Estimated costs of crime	$60 billion	$125 billion
Total Wider economic and social costs	**$737 - $898 billion**	**$1.54 - $1.87 trillion**
Estimated employement losses	**2 - 2.6 million**	**$4.2 - 5.4 million**
Foregone economic growth in OECD 2017	**$3 billion to $54 billion**	

Source | Frontier estimates based on OECD 2013 data on counterfeiting in international trade, and UN trade and GDP data to derive estimates for domestic production and consumption. Data for Piracy based on latest industry sources (2015).

Problems with current product records

A | The failure of physical certificates

Physical certificates have been introduced as a way to authenticate objects without the need for a detailed expert assessment. However, physical certificates present several areas of vulnerability.

Methods of combating counterfeiting with proof of authenticity have a long history. One of the oldest examples might be the seal of the sovereign, which would vouch for the authenticity of a message. Later on, paper money, bearer bonds acting as corporate shares, and other negotiable financial instruments bore watermarks intended to prevent counterfeiting.

As the years passed, these methods were replaced by modern equivalents. Technologies like RFID, holograms, and NFC are, in effect, contemporary tools intended to add a layer of protection that makes a product more difficult to copy.

Physical certificates of any sort are copyable - some more easily than others - and are therefore susceptible to counterfeiting. Accordingly, a physical certificate is, just like the product itself, difficult to authenticate beyond all doubt.

A close look at the luxury market, where counterfeiting is a major issue, makes it clear that the brands provide little or no information that enables a consumer to understand how to distinguish a genuine product from a copy. Each brand has its own way to create certificates, which it doesn't communicate publicly.

Because it can be falsified, a physical certificate of authenticity is often linked to a serial number. This serial number is useful only if it can be referenced to a database. Access to these databases is usually restricted and therefore of little use for the second-hand market.

B | The limits of expert assessment

The only way to confirm the authenticity of a product when it is impossible to trace its origin is to request an expert assessment. The expert will compare the details, materials, and craftsmanship of the object to assess its authenticity. This process is costly and is only as reliable as the brand's network of specialists. The sad reality is that the majority of brands only use third-party resellers (e.g. Macy's, Galerie Lafayette, etc.), which tend not to have staff with brand-specific training. And even a visit to a brand's own boutique or retailer reveals that most of the team members in these shops don't have the skills to confirm - beyond all doubt - the authenticity of a certificate.

Furthermore, the rise of the so-called "super-fakes", copies with high attention to detail and superior craftsmanship, demonstrates the limits of expert assessments. The copies are increasingly difficult to distinguish from the originals[5].

●

....

−5 Biggs, John. "The Attack of the SuperFakes." TechCrunch (blog). December 3rd, 2017.
http://social.techcrunch.com/2017/12/03/the-attack-of-the-superfakes/.

Problems with current product records

Proving ownership while preserving the owner's privacy

Proving ownership is necessary for all customers as it allows them to access such services as insurance or manufacturer guarantees. It also protects them from theft.

The need for a proof of ownership should always be balanced against the need for the owner's privacy, as any record of ownership could potentially identify them as targets for criminals.

A | Proof of purchase

Claims of ownership are usually confirmed with a proof of purchase such as an invoice or a receipt. **These titles of ownership are easily lost, misplaced, or destroyed because they are either not digitized** (paper receipt) or, if they are digitized, not safely secured (no backup).

Moreover, these proofs of purchase can easily be altered or falsified. While an original seller can check his/her records, a third party (second buyer, insurance company, etc.) will suffer a high administrative burden and operational costs in order to verify any information provided by a claimant with the seller, particularly as retailers are generally not in a position to provide evidence of a purchase from a past customer. CRMs collect data between product and buyers in a centralized database. Without an update that includes the new owner's name, CRM databases are inefficient.

It should also be noted that the possession of a valid proof of purchase and a product is a poor proof of actual ownership as the receipt/invoice may not make any reference to the purchaser's identity.

B | Product registration

Another solution in current use is product registration, which some brands have already implemented. This solution requires products owners to enter a product's serial number, their personal identity, and other relevant information in a centralized database. While this approach offers the advantage of linking proof of purchase and identity, it generates additional problems.

This approach puts customer privacy at risk. In order to register product ownership, owners need to register their personal information in the database. This can be particularly risky as burglars and thieves are interested in acquiring information about where valuables are stored.

Current product registration solutions also create additional incentives for criminals. These centralized non-anonymized databases at the brand level are "honeypots" for hackers looking to identify high-potential targets for thefts/burglaries, thus increasing the likelihood of hacking.

Furthermore, customers are not in control of their data. These databases are usually the sole property of the brands and do not allow customers to share access easily with a third party.

Finally, these solutions offer poor data portability. The responsibility for the first registration of a new product is the responsibility of the brand or retailer for the original owner. This registration is often impossible to transfer to subsequent owners and therefore compromises the second-hand market.

Problems with current product records

Authorized third parties

In order to assure the quality of the network of retailers and partners distributing or offering services around a product, brands need to be able to audit these actors and grant them "authorized" status. This status is an acknowledgement that they meet the thresholds of quality, reliability and excellence to which the brands aspire.

While many brands have a network of authorized resellers and service companies, this status of authorization can be fraudulently claimed by companies that are neither audited nor authorized and which can deceive unsuspecting owners. There is a clear need to provide a cost-effective, universally accessible way - which is absolutely inviolable - for brands to deliver their verified seals of approval to legitimately authorized third-party companies.

Serious consequences are caused by non-authorized dealers: they damage brands' profit margins and undermine the customer experience. Unlike a brand or an authorized retailer, these unsanctioned resellers have neither the overhead nor the operational costs – for example, advertising, quality control, and customer service – that are generally associated with running a legitimate business. They essentially benefit from the reputation and the goodwill that brands and their authorized representatives have built so conscientiously.

Problems with current product records

When brands present their products, they define the parameters they use, including colors, counter displays, up-to-date communication materials and so on. These are all among the most important touch points at the defining moment of the customer journey: the in-store experience. From a customer's perspective, warranty activation generally has to be done through an official retailer in order to be approved by a brand's customer service organization. In cases involving high-priced items, the associated repair costs – if necessary – will also have to be negotiated between these two parties.

Brands need a more effective way to communicate the "authorized" status of a third party to their clients. Customers can only benefit from this effort as they are among the most affected victims of unscrupulous third parties.

Product journey data

Product journey data acquisition is cumbersome and costly because of the number of participants involved in a product's journey from resellers to service providers, including insurance companies, and local authorities such as law enforcement.

This situation leads to poor product journey data, which has negative impacts on both business productivity and customer experience.

A ı Lost time for customer care research in product history

The lack of easily accessible records of a product's post-purchase events (repairs, servicing, etc.) is a strain on brands' customer service apparatuses. Customer service agents tend to spend a majority of their time investigating a product's history and recording relevant data points.

These hours are an unnecessary time burden for customer service employees. This leads to productivity loss that could be alleviated by better record-keeping systems. It also has a severe negative impact on the quality of the customer experience as customers spend more time being "interrogated" than served.

B ı Lack of a lasting link between brand and owner

The absence of a link between a brand and an object means that the brand is usually unaware of major events in an owner's journey and worse, loses contact with the owner in the case of a change of ownership. Brands therefore have difficulty in identifying events which could lead to

cross- and up-selling opportunities and initiate an outbound communication with the owner. It should also be noted that this information is usually recorded without consumers' knowledge and with little available recourse to indicate how their information might be used.

There is a need for complete and accurate information about a product's journey that could be inexpensively recorded after the purchase. The owner should, however, be able to retain absolute control of how and with whom this information is shared.

Problems with current product records

C | Data Protection Regulation and cybercrime

The scale of data breaches is enormous. Every day, nearly five million sets of data are lost or stolen; this means that each second of every day, 57 records are affected.[7]

The increase in the number of data breaches over the past few years has raised greater concerns about who is responsible for taking care of the world's data. Individuals hear on a weekly basis that their personal data have been compromised, while corporate entities and brands realize how vulnerable they are to hackers who would wish to do them financial and reputational harm.

Even with the support of the most talented cyber-security specialists, committed black hats know how to exploit software breaches, and companies can only take action after these breaches have taken place. Government regulations, while important, represent a challenge to a company's ability to adapt while preserving its marketing power. In light of those events and the absence of best practices from companies, the European Union decided to take a step forward in data governance by implementing the General Data Protection Regulation (GDPR), an EU regulation intended to strengthen and unify data protection for individuals living in the European Union.

When it becomes enforceable in May of 2018, it will also regulate the export of personal data outside the EU. The GDPR aims to give the control of personal data back to citizens and residents by unifying the regulation within the EU. Considering the risks, this kind of regulation can only become more widespread and brands will have to comply.

....

– 6 "Fake Apple Store in China so Convincing That Even Its Staff Are Fooled | Daily Mail Online," 22 of july 2011.
http://www.dailymail.co.uk/news/article-2016885/Fake-Apple-store-China-convincing-staff-fooled.html.

– 7 "E-Commerce Fraud Rising, Report Warns." Inside Retail Asia (blog), December 13, 2017.
https://insideretail.asia/2017/12/13/e-commerce-fraud-rising-report-warns/.

Arianee's value proposition

Arianee's blockchain perfectly complements those organizations, processes, and technologies, like RFID, holograms, NFC and all tagging mechanisms, that are already working to organize product data in inexpensive and universally accessible ways and to combat counterfeiting.

While these are focused on hardware solutions, Arianee's contribution will deliver a completely universal protocol that enables the matching of all goods in all markets. The creators of hardware solutions won't lose any value; in fact, their activities will be complemented. The primary value added by an open protocol like Arianee's is its ability to allow all of humankind the opportunity to collaborate on a single layer, without specific hardware. Keep in mind that in a world of centralized technology, authenticity can only be insured by the owner of the system, a situation which – by its very nature – undermines trust.

With Arianee, anyone can verify the authenticity of a product simply and confidently with a smartphone. This offers a unique chance to build trust between brands, owners, and all other parties concerned without removing added value at any level. But more than that, it unleashes new opportunities to the existing marketplace, particularly for brands, with what we call Smart-Link Marketing, which creates a revolutionary link between producers and the current owners of the goods they produce. There is also the benefit of added value, both to brands and their customers, when the authenticity of an asset is reliably verified by Arianee.

For owners

A | protection

• Trust in transactions

Protecting owners' property starts by ensuring that the product they buy is authentic and that the seller is authorized to sell the good in question. Although we all have proof of our good faith (invoices, warranty cards, etc.), usurpers know how to manipulate physical documents to make them look real. They trick buyers by making them think they are purchasing an authentic asset. Even the most sophisticated and cautious buyers can be fooled and can end up with stolen or fake assets. We all accept responsibility for ourselves but navigating an ocean full of traps adds stress and uncertainty to our lives.

The Arianee certificate will build indisputable trust between owners and third parties as it is backed by a decentralized, transparent, and unalterable blockchain that makes it impossible to falsify and easy for anyone to verify.
Arianee is here to help owners face these challenges with confidence, through the creation of its blockchain certificate

for each unique asset. Moreover, the Arianee blockchain will list the product's service history ensuring that the current owner has maintained the product adequately.

• Lost items and theft protection

Current lost and found systems are imperfect because objects cannot easily be identified in a database. Having a single reference source that can be used to check and verify the legal and ownership status of valuable assets will reunite a lost or stolen product with its rightful owner faster and more effectively. Furthermore, if a valuable asset is registered on the Arianee blockchain, robbery becomes pointless. At that point, a thief would be limited to a single option: selling the item to someone who would willingly traffic in stolen goods. When Arianee is up and running, the buyer of such a product will be assuming an ethical and moral responsibility as well as a legal risk.

Arianee's value proposition

Thefts of some so-called connected devices have already been made futile by the owner's ability to deactivate a stolen phone, tablet, etc. so that it becomes useless for anyone else. An Arianee ownership certificate will add another layer of protection to these "connected" products, but will also reduce the attraction of theft and burglary and significantly undermine the market for stolen goods.

B | Data ownership

These days, companies tend to be channel agnostic. Whether they represent a social media platform, a search engine, or a third-party website, they build marketing funnels that lead customers to where the companies want them to go. In the process, customers cross a number of trackers that collect their personal data. Intermediaries then store the navigation history and analyze their behavior. Those intermediaries never offer proof of their own authenticity or their goodwill. They may offer a certain level of know-how, but they don't, in fact, have direct relationships with brands/producers.

It is time for customers to regain control of their data.

The Arianee blockchain technology will protect consumers from exposure to such unauthorized and hidden trackers. They will be free to build the relationships they want with brands they choose without having to reveal their personal data unwillingly.

C | Convenience

Arianee is a brand-agnostic platform where customers can easily register all their products in one place. They can also store documents related to a registered product. Each asset can be linked to content such as the Terms & Conditions of a sale, a warranty contract, instructions, a product description, videos, photographs, etc. Arianee is the owner's repository for all information related to their valuables.

This repository will reduce cost and greatly facilitate the sharing of information with third parties, such as in the case of insurance claims. In fact, the advent of the Arianee certificate will streamline processes with insurers. The inarguable proof of authenticity and ownership of a product will reduce red tape, save time, and avoid bureaucracy. If your property is lost or stolen, you could be compensated by your insurance company in a matter of minutes.

For Brands

> "Our brands tell us that they are having a dramatic lack of success, and all you have to do is go on the website and see the proliferation of counterfeits every day.[8]

Juanita Duggan | CEO of American Apparel and Footwear Association

A | The fight against counterfeiting

Arianee's certificates represent a digital hallmark for original branded products. The authenticity of the physical products with which certificates are associated is verified because the certification is immutable and cannot be falsified or compromised. These digital verifications of authenticity are accessible at a single common location – to everyone, anywhere, anytime.

By producing a digital representation of an asset, Arianee connects the actual property to a network, thus linking the asset to software. The value of the asset is transferred from the physical object to its digital certificate of authenticity.

An Arianee certificate offers companies, brands and institutions an added level of protection, which complements and reinforces their other counterfeiting solutions like RFIDs or serial numbers.

– 8 "U.S. Online Fraud Attempts Increase 22 Percent during 2017 Holiday Shopping Season." ACI Worldwide. Accessed February 20, 2018. https://www.aciworldwide.com/news-and-events/press-releases/2018/january/us-online-fraud-attempts-increase-22-percent-during-2017-holiday-shopping-season.

Arianee's value proposition

B | Maintain links with owners

In order to maximize their access to markets, brands turn to wholesalers and e-resellers. These intermediaries create a barrier between brands and their customers. While retailers generally know their most loyal buyers well, they do not, as a rule, share their own databases. This is understable but on occasion, a dealer may want to call the attention of a particular group of customers to a special release or a limited edition product.

Even in the case of direct sales, brands might lose track of the final owner. For instance, informal intermediaries importing luxury goods illegally into countries with high tariffs prevent any attempt to build customer knowledge or to interact with them. The well-documented phenomenon of Chinese daigous[10] is a perfect example of these informal intermediaries.

Thanks to the Arianee Smart-Link, brands will have instant access to the ownership information of its registered products like a VIP card. It allows a brand to target the ideal potential customer base for a rare or unusual product and to develop a meaningful and highly personal experience in store both for the brand and the owner.

> ## Today, when people buy watches, we don't know who the buyers are because we have retailers in between.[11]
>
> FRANÇOIS-HENRY BENNAHMIAS | CEO of Audemars Piguet

C | Protection from "moonlighting" and grey markets

Arianee will allow brands to monitor their products up and down the supply chain whether during the manufacturing process at subcontractor factories or when they are with a distributor. One major issue for brands is linked to subcontractors "moonlighting" during off hours and overproducing. These factories produce unauthorized genuine products and resell them on the black market. The Arianee protocol will prevent this moonlighting, as a fake certificate cannot be reproduced. Down the supply chain, in order to maintain a certain service quality in distribution, brands grant "authorized reseller" status to resellers who agree to respect certain constraints. These resellers often receive early delivery of special models or even exclusive

distribution. Some of these retailers fraudulently resell to non-authorized grey market resellers that do not respect the service quality and pricing constraints imposed by the brand. Arianee, thanks to the traceability of products, will allow brands to identify the origin of these grey market products and restrict supplies.

> ## " In luxury goods, when you break the illusion of prestige, the dream, the prices, it takes away the confidence. It means slow death for luxury goods.[11] "
>
> JEAN-CLAUDE BIVER | Head of LVMH's Watch Division

D | Customer care efficiency

Customer care services need an accurate history of a product in order to troubleshoot a problem being experienced by a customer. A significant share of a customer relation agent's time is spent retracing the product's history.

With Arianee's protocol, customers can grant instant access to accurate information about their product. This allows the customer care agent to bypass the cumbersome questionnaire a client has to endure and focus instead on the customer relationship.

....

− 9 Gemalto. "Data Breach Statistics by Year, Industry, More." Breach Level Index.
http://breachlevelindex.com.

− 10 It is common for Chinese consumers to dodge the high price of luxury goods in their own country by buying them on so-called daigou websites: a shopper might buy a handbag in Europe, then resell it on one of these websites for more than the European retail price but less than the Chinese one

− 11 Gray Market Has Become a Necessary Evil for Luxury Watchmakers." Reuters, April 13, 2017.
https://www.reuters.com/article/us-swiss-watches-grey-market/grey-market-has-become-a-necessary-evil-for-luxury-watchmakers-idUSKBN17E2E8.

Arianee's value proposition

For third parties

A | Resellers

Reputation is an important factor for resellers and service providers as it offers proof of the quality of their services and the integrity of their workforces. These days, however, reputations are influenced by reviews placed on a wide range of platforms. These, by their nature, are susceptible to unverified biased reviews which, so far, have proven difficult to prevent efficiently.

Arianee will allow third-party service providers to collect reviews from customers who can prove that they have actually used the services delivered by these parties.

Moreover, resellers will be able to stay in touch with past clients easily, thanks to the communication channels opened by the Arianee platform. This will allow them to send messages or respond to inquiries from past or potential clients.

B | Expert

Third-party experts can provide authenticity certification and an appraisal of a product's value. These services can be marketed to owners and brands directly on the Arianee platform.

Moreover, their expert assessments benefit from the same traceability and guarantee of authenticity as all assets stored on the Arianee blockchain are also protected with the same level of security that all certificates receive.

C | Enriching third parties

• *Information Technology Solution Providers*

Information Technology (IT) Solution Providers will be the necessary bridge between legacy IT systems and the Arianee blockchain. They will build the interface for brands and other third parties to interact with the Arianee blockchain.

Thanks to the Arianee protocol, IT Solution Providers will be able to offer a new "Owner Relationship Management" service to brands. This new service will offer analytics dashboards and other tools to handle a brand's relationship with its product owners.

• *Insurance*

While many third parties will benefit from using the Arianee platform, the insurance sector is probably the most obvious potential beneficiary.

Insurance companies will, for example, be able to process their customers' claims much more efficiently. The Arianee blockchain will allow them to prove the authenticity and ownership of a claimant as well as to check the accurate repair or replacement costs as indicated by a brand or third-party reseller.

The information stored on the Arianee blockchain could also allow insurers or other fraud prevention organizations to monitor potential insurance fraud. Tracking the history of an asset will allow them to identify fraud cases, both before and after a claim has been processed.

●

Arianee
User Journeys

The Arianee platform serves three types of users: owners, brands, and a multitude of third parties. In this section, we will explore the user journey of the two key groups of users: owners and brands. These user journeys should be understood as simplified examples rather than as reflections of the entire complexity of the Arianee platform.
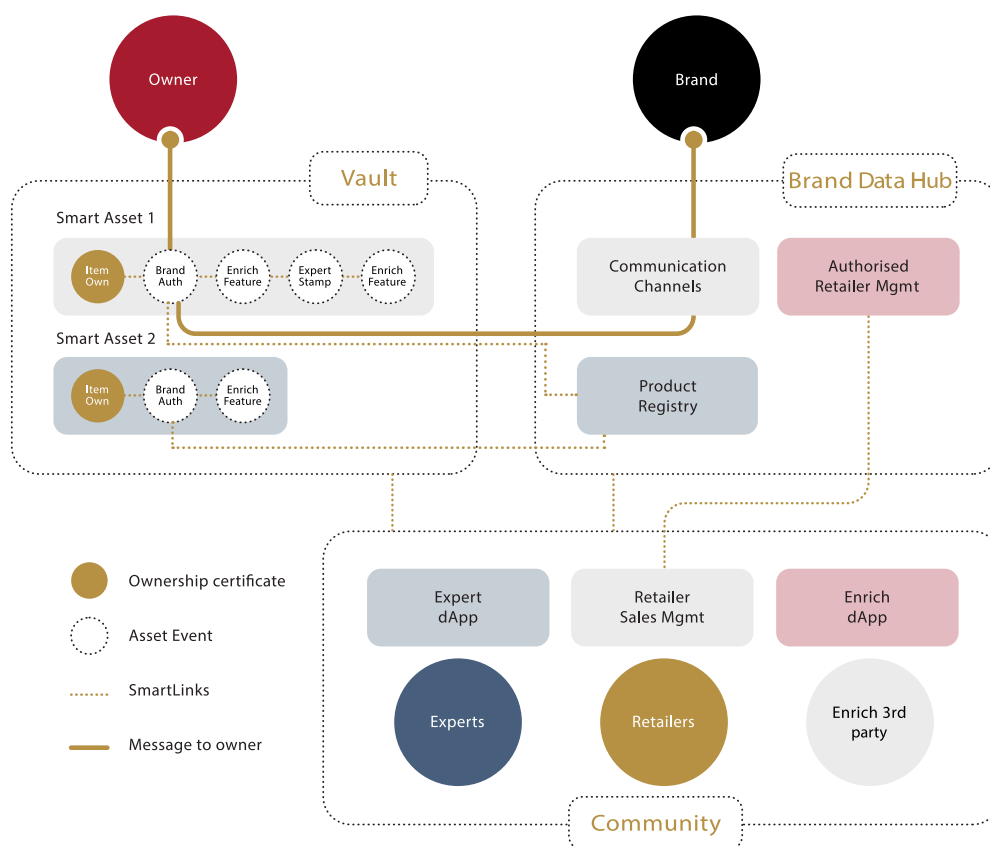
Owners

A | Create Vault

The first action an owner will take on the Arianee platform is to create a Vault. The Vault is a secure and convenient repository for all of an owner's products. The owner will be prompted to create a private key, which will secure the access to the Vault. Its creation will then generate a Vault public key, which is the Vault's address.

Key Action:

• Create a Vault by generating a public key and create a private key for security.

Key Value proposition:

• The Vault is a convenient repository for all of an owner's products.

Arianee
User Journeys

B | Add a Smart-Asset
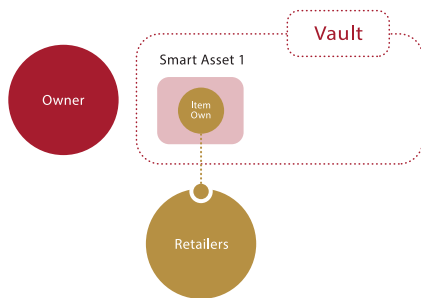
The second step for an owner will be to create a Smart-Asset by registering a product and adding it to the Vault. The creation of a Smart-Asset will also create the first certificate in your Smart-Asset history: a certificate of ownership. This certificate of ownership is a unique, unfalsifiable proof of your right of ownership of your product.

Alternatively, you might receive the Smart-Asset directly from the retailer or the brand from which you purchased your product. The product might come with some additional history of events that were associated with the product prior to your purchase.

Key Actions:

• Register a product by creating a Smart-Asset and add it to the Vault.

• Generate a certificate of ownership - proof that you are the rightful owner of this product.

Key Value proposition:

• The Smart-Asset is an unfalsifiable proof of ownership.

C | Authenticate an object with manufacturing brand
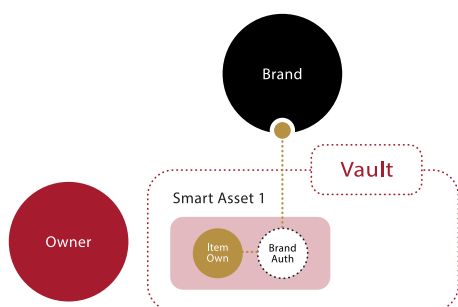
An owner can send his/her Smart-Asset to the manufacturing brand to confirm the product's authenticity. This will add a certificate of authenticity to the Smart-Asset and the brand can automatically attach all relevant documentation.

The certificate of authenticity is linked to the brand with a Smart-Link, which allows the brand to send communications to the owner for as long as the certificate of authenticity is valid. The owner may elect to share updates on his/her Smart-Asset history with the brand.

Key Actions:

• Share a Smart-Asset ID with manufacturing brand.

• Receive a certificate of authenticity.

Key Value proposition:

• A Smart-Asset certifies the authenticity of a product.

D | Get insurance for all your Smart-Assets
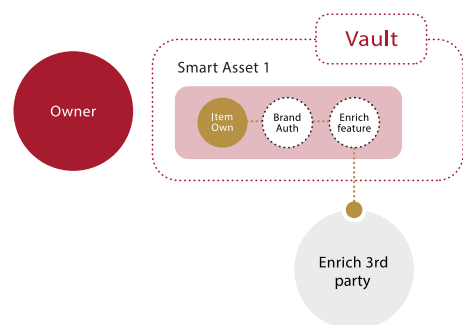
An owner might elect to receive services through third parties. Here we will examine the example of insurance.

To receive insurance, an owner will first grant the insurance company a "read access" to the entire Vault or to the selected Smart-Assets. The insurer will use the certificate of ownership and the certificate of authenticity to estimate the value of the products to be insured and to calculate the associated premium.

Key Actions:

• Grant "read access" to a third party.

• Authorize the third party to add a product history event to the Smart-Asset.

Key Value proposition:

• Facilitate the sharing of product information with a third-party service provider.

Arianee
User Journeys

E | Get an appraisal for your Smart-Asset
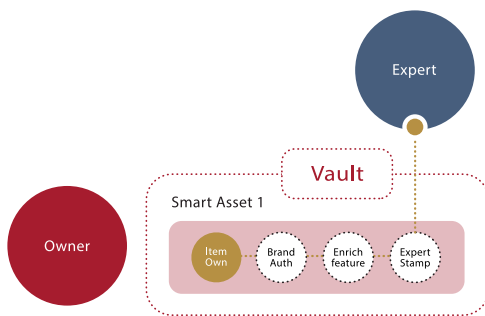
An owner is considering selling a product and decides to get an expert appraisal in order to have a more accurate estimate of the selling price. He/she searches for an expert third party who has gone through the Arianee validation process or has received delegation from a verified brand.

The owner then shares access to the Smart Asset with the expert, who is then granted the right to add an appraisal stamp to the Smart-Asset. Once the appraisal has been completed, the owner can elect to share the information with the insurance company to update the premium.

Key Actions:
- Find an expert in the Arianee community.
- Check the expert's reputation with actual customers.
- Grant "writing access" to the expert third party, who can add an appraisal certificate to the Smart-Asset.
- Automatically share from third party to third party.

Key Value proposition:
- The Arianee third-party community leverages the blockchain to provide enhanced services to owners.
- Automatic transfer of information from third party to third party.

F | Maintenance for your product

The owner wishes to service the product before selling it to increase the likelihood of a sale. In order to preserve the warranty, the servicing needs to be performed by a reseller authorized by the brand. The owner's local watchmaker claims that it is authorized by the brand. The owner then checks the watchmaker's authorized status on the Arianee blockchain and grants it a "writing access" to add a servicing event to the Smart-Asset.
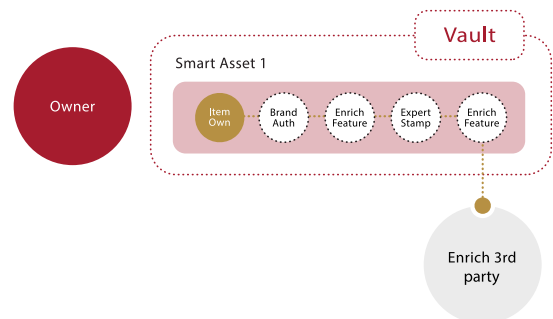
Key Action:
- Verify authorized status.
- Write access.

Key Value proposition:
- Instant unfalsifiable proof of authorized status protects the owner from unscrupulous retailers.
- Proof of servicing.

G | Receive a message from brand
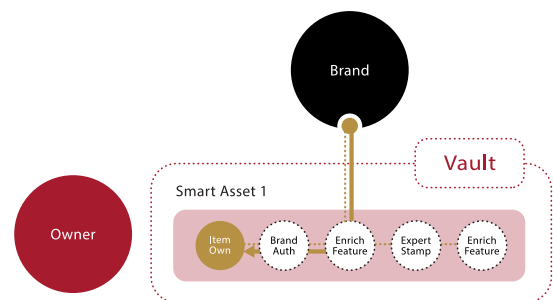
Because the authorized reseller shares information with the manufacturing brand, the manufacturing brand uses its certificate of authenticity Smart-Link to send a message to the owner. This message informs the owner that a new accessory collection is now available.

Key Actions:
- Information sharing between third parties and brands.
- Messaging channel directly connected to the owner.

Key Value proposition:
- Messaging channel to the owner is open thanks to the certificate of authenticity.
- Brands receive owner journey insights.

Arianee
User Journeys

H | Sell your product to another person
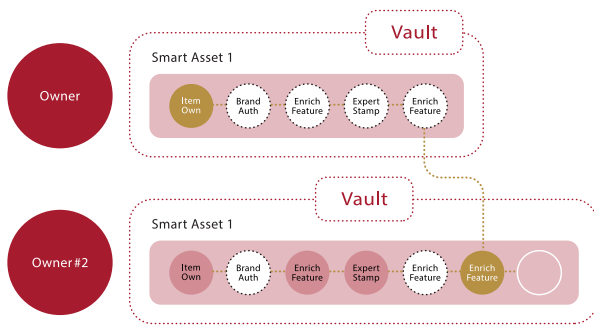
The owner has found a buyer. To transfer the ownership of the product, the owner only needs the public address for the buyer's Vault. However, in order to prevent fraud, the two parties will create a smart contract that will deliver the certificate of ownership only when the payment has been received. Until that happens, the certificate of ownership is locked. Once the Smart-Asset has effectively been transferred, the new owner still has a view of past events but sensitive data is encrypted to protect the previous owner's privacy.

Key Actions:

• Transfer of the certificate of ownership from one Vault to another.
• Creation of a smart-contract that conditions the release of the certificate of ownership upon payment.

Key Value proposition:

• Verification process to ensure certificates of authenticity are genuine when issued.

Brand Journey

A | Register as a verified brand

A brand's first action will be to register as a verified brand with the Arianee brand verification process. While any person can grant an expert stamp attesting to the authenticity of a Smart-Asset, Smart Authenticity certificates can only be delivered by the manufacturing brand. Smart-Atuthenticity certificates grant the verified brand special access to the owner, and brands can receive alerts associated with certain types of Smart-Asset events.

Key Actions:

• Register as a verified brand by going through the Arianee brand verification process.

Key Value proposition:

• Ensure trust in transactions.
• Prevent fraud.

B | Initiate your Brand Data Hub

Once the brand is granted verified status, it can initiate its data hub. The data hub is the center of the brand's interactions with the Arianee platform. The data hub is composed of three core modules:

• The Product Registry, where brands keep track of all objects for which they have delivered certificates of authenticity.

• The Communication Center, where brands can send communications to the owners of products that have been granted a certificate of authenticity.

• The Authorized Retailer Management System, where brands can interact with their network of authorized retailers.

Key Actions:

• Connect to the data hub.

Key Value proposition:

• Data center for brands' products, owner communication and retailer networks.

Arianee
User Journeys

C | Deliver a certificate of authenticity

Upon request from a product's owner, a brand can deliver a certificate of authenticity. The unfalsifiable certificate opens a direct link between a brand and the product's owner. The product is thereafter added to the brand's Product Registry.

Key Actions:

• Deliver a certificate of authenticity for a product.

Key Value proposition:

• Prevent counterfeiting.
• Create a direct link between the brand and the product owner.

D | Grant authorized status to a retailer

Verified brands can grant an authorized status to a retailer. This provides a badge of legitimacy to the retailer. Owners can verify the authorized status of a retailer on the blockchain before a purchase or another service. The authorized retailer is listed in the authorized retailer management system.

Key Actions:

• Grant authorized status to retailers.

Key Value proposition:

• Manage a brand's authorized retailer network.

E | Send a communication to an owner

The brand sends a communication to all its product owners inviting them to an exclusive private sale event.

Key Actions:

• Send a message to product owners in your registry.

Key Value proposition:

• Maintain a communication channel to a product's owner regardless of whether the product has changed ownership.

F | Perform analytics on your product registry

The brand wishes to send a communication about its soon-to-be-released accessories to a subset of owners. The brand queries its product registry to identify all registered product owners who purchased a specific model more than a year ago and sends them a message to them.

Key Actions:

• Perform analytics on a product's lifetime journey.

Key Value proposition:

• Identify key events for up-sell or cross-sell opportunities.
• Identify macro trends in a product's journey.

G | Control the authorized retailer network

A brand has been made aware that some of its products are on sale on the grey market. It investigates where these products come from. It finds the Smart-Asset of one or several products on sale in this marketplace and search for them in their product registry to identify which retailer sold these products to the grey market.

Key Actions:

• Perform data analysis on authorized retailers to identify potential abuse.

Key Value proposition:

• Prevent grey market sales.
• Maintain a uniform customer experience within a brand's retailer network

Arianee's protocol

.arianee's ecosystem
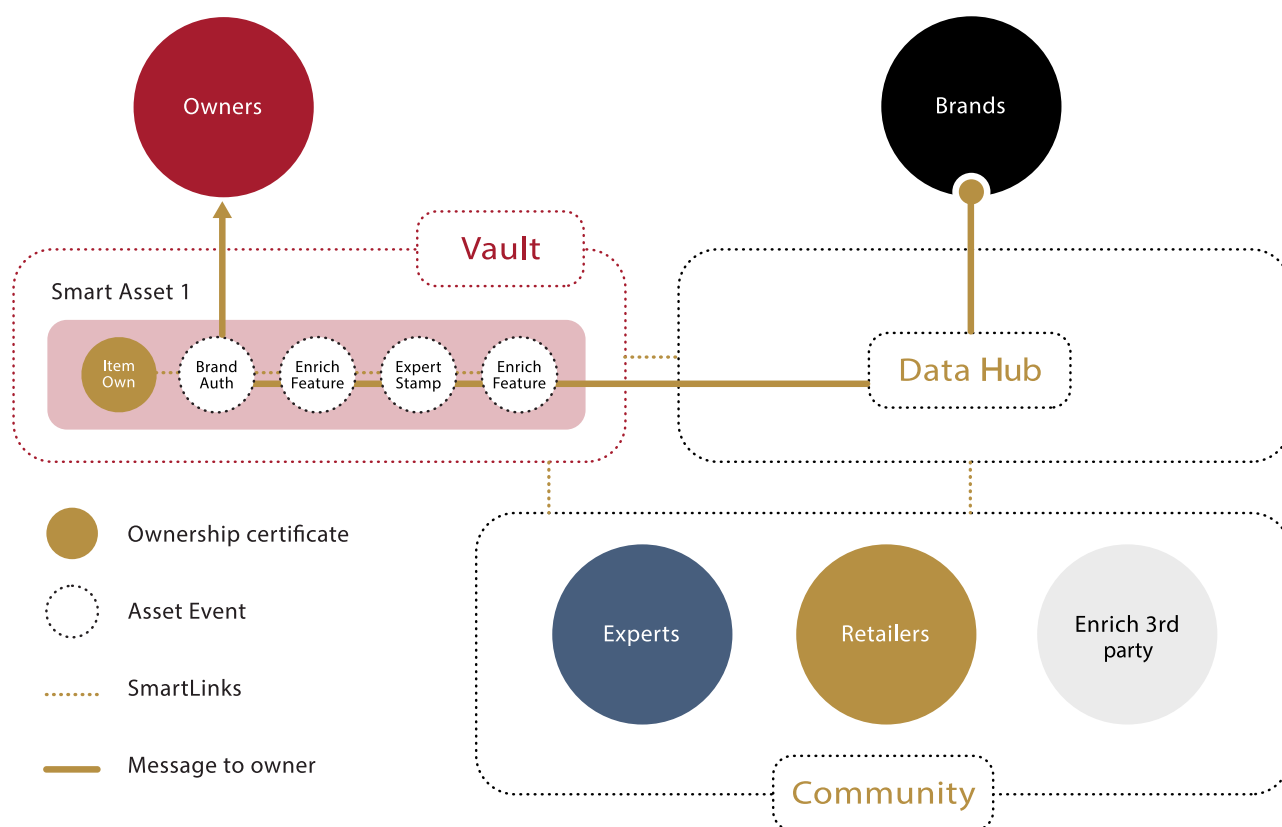
The full-feature Arianee protocol is built for three groups of users:

- Products' owners,
- Brands,
- Third parties.

Each type of user interacts with the Arianee platform using a dedicated API:

- The Vault for products' owners,
- The data hub for brands,
- The community toolkit for third parties.

All interactions between users take place through Smart-Links. All Smart-Links are recorded on the Arianee blockchain; however, user privacy is respected thanks to what is called zero-knowledge proof technology. Essentially, a zero-knowledge proof is a process that can demonstrate that a statement is true without revealing any additional information beyond what it is trying to prove.

Arianee's protocol

Owners

Owners are the primary users of the Arianee platform. They register their products as Smart-Assets in their Vaults, either by listing the products themselves or by taking possession of the Smart-Asset from another owner, a brand, or a retailer. Owners can then enrich the Smart-Assets with certificates and stamps provided by brands or third party experts. Some examples include certificates of authenticity delivered by brands, servicing history stamps from expert third parties, etc.

A ┃ Create owner's "Vault"

The Vault is an easy-to-use online repository where owners can register all their products and the associated documentation free of charge. It is, in effect, an owner's product portfolio. The Vault is pseudonymous, which allows even greater security as owners can elect not to provide their real identity.

Owner's can easily create a Vault by generating a public key (the Vault's address) on the blockchain and generate a private key (the Vault's secrete decryption key).

Information entered by owners is stored on the Arianee blockchain, which assures that it cannot be altered by anyone. The Arianee blockchain is private by design. All data is encrypted to protect the owner's privacy, and the integrity of the information stored on the blockchain is certified by the zero-knowledge proof protocol.

The owner's Vault is designed to respect the latest privacy requirements such as the General Data Protection Regulation (GDPR). The GDPR was created by the European Union to enhance and unify data protection for the citizens of its member nations. It also covers the export of personal data outside the EU and is intended to give its residents control over their data while simplifying the regulatory environment for international businesses. It was adopted in April of 2016 and will become enforceable on the 25th of May, 2018. The Arianee protocol is, by design, GDPR compliant: users are anonymous, no personal data is ever recorded on the blockchain and the users (both owners and brands) control access to all their data.

B ┃ Create Smart-Assets

"Smart-Assets" can be described as the main objects on the Arianee protocol. They are a unique representation of an owner's product on the blockchain. A Smart-Asset has at least a serial number, a brand public key, an issuing date, an owner and an ownership status (owned, lost, stolen, destroyed, consumed). Owners can register their products on the Arianee blockchain and safely store them in their Vaults. Each asset is associated with a unique and immutable ID. While the Arianee blockchain is accessible to anyone, all information including Smart-Assets are encrypted, using time-tested encryption methods to protect the owners' privacy.

Each Arianee Smart-Asset contains a log which lists all associated events. An event is a structured data with a date, a type, an issuer and a metadata.

There are three types of associated events:
- Ownership certificates which can only be granted when a change of ownership takes place.
- Authenticity certificates granted by verified brands and verified expert third parties.
- Tags that reflect other episodes in the Smart-Assets history. They can be recorded by any user with access to the Vault.

C ┃ Transfer of Smart-Asset ownership

When an Arianee asset is created, it is the exclusive property of the owner. Thanks to the blockchain, only the owner is able to activate primary features like, for example, transfers. A transferred asset is sealed forever, and the previous owner can't recover the right to that asset. Neither the issuer, the previous owner, nor even the Arianee team are able to change this status, guaranteeing trust and confidence in the whole ecosystem.

D ┃ Smart-Link: Read access

Owners can grant the right to third parties or brands to read data linked to assets in their Vaults. This operation allows owners to share certain information about selected assets or all the assets stored in their Vaults.

E ┃ Smart-Link: Lending Smart-Assets

Instead of a definitive transfer, some use cases need a way to lend assets (marketplace, after-sales servicing, etc.) for a certain period of time. An owner will be able to lend an item with different criteria (total duration, minimum duration, etc.) and remain the real owner of an asset. This will help define new use cases and build a global ecosystem with other parties.

F ┃ Smart-Link: Delegation

Owners can delegate their authority to a brand or a third party and allow them to perform operations. This action is the feature enabling the creation of smart contracts and decentralized apps on the Arianee blockchain.

Arianee's protocol

Brands

Brands need to go through the verification process to be granted the powers reserved for verified brands. Brands issue Smart-Authenticity certificates, which allow them to maintain contact with the current owner of a certified product. Brands can send messages through the Smart-Authenticity certificate to the owner. They can also delegate certification to relevant third parties, including experts, retailers, and anyone else qualified to enrich the brand's status.

A | Initiate Brand Data Hub

Smart Authenticity certificates can only be issued by verified brands. These brands go through a verification process to ensure that they have the legal rights to represent the brand.

The data hub is the center of brands' interactions with the Arianee platform. It provides product life analytics in three core modules:

- The Product Registry, where brands manage authenticated objects;

- The Communication Center, where brands reach out to product owners;

- The Distribution Network Management System, where brands interact with their distribution network.

B | Smart-Link: Smart Authenticity

Smart Authenticity holds a special place in the Arianee protocol. Authenticity is at the heart of Arianee's value proposition. Verified brands can grant certificates of authenticity to products stored in a Vault at the owner's request. As long as the authenticity is valid, the brand maintains an open communication channel with the product owner, regardless of future changes in ownership.

Verified brands are the ultimate authorities for the verification of the authenticity of the objects they produce. Therefore, brands should have a special relationship with owners. Brands are able to issue certificates of authenticity for owners' objects, either at the time of sale or at an owner's request at a later date. Only the authorized brand can confirm that a certificate's public key is, in fact, from the brand.

C | Smart-Link: Brand Messaging

Brands issuing Smart Authenticity certificates have the unique possibility to send messages to the certificate and then, by "rebound", to the owner of an item. Because of Arianee's characterics, the issuer will be able to send messages to the current owner of a certificate, even if they were not the initial buyer.

This messaging possibility allows brands to maintain a connection whith product owners throughout the object's lifetime, wich is something which is currently nearly impossible. For the first time in history, owner and brand will be able to reconnect even if they don't know each other. Because of the asynchronous state of the blockchain, owners will have the opportunity to select the kinds of messages they wish to receive. This will prevent spam, build trust, and create a fair environment.

D | Smart-Link: Read Access

Brands can grant the right to third parties to read data in their data hub. This operation allows brands to share different types of information about assets registered in their Product Registry. Similarly, brands can also share sent messages and authorized retailer information.

E | Smart-Link: Brand Delegation

A brand can delegate its authority to a third party, which would be allowed to perform operations normally assumed by the brand. This action is the feature enabling the creation of smart contracts and decentralized apps on the Arianee blockchain.

F | Smart-Link: Deliver Authorized Retailer Certificate

Brands can deliver an authorized retailer certificate to a third party. This certificate can be consulted by owners to confirm a third party's authorized status.

Arianee's protocol

Third-party community

A I Experts

While brands are the entities most legitimately positioned to provide authenticity certificates for products they manufacture, expert appraisals may also be necessary. Whether for antiques or fine art, experts can, in some cases, be the sources who are best qualified to provide a certificate of authenticity. Experts shall therefore be granted a right to provide authenticity certificates whose value will be enhanced by the reputations of these experts. Experts need to be verified either through the Arianee verification process or receive delegation from a verified brand

B I Retailers

In most sectors, brands only sell a limited percentage of their products directly to customers. Retailers represent a major part of the customer experience. Brands can delegate some of their prerogatives to these retailers. Moreover, retailers need access to mechanisms that will both establish their reputation and protect them from fraud.

C I Enriching third parties

Enriching third parties will develop decentralized applications leveraging the Arianee blockchain. They will provide services to owners, brands and other third parties through the blockchain data sharing process.

Business Case studies

As detailed previously, Arianee's role is to be focused on the protocol's backbone and to develop and enable many applications based on our protocol. However, to initialize and boost the ecosystem, we have planned to develop the first application based on the Arianee protocol.

Arianee Luxury

In 2017, the personal luxury good market represented a total value of €262 billon (+5% year-on-year), the highest amount on record.[12] Counterfeiting has a particularly adverse effect on the sales and profits of luxury brands, which, because of their prestige and the high prices of their products, are especially susceptible to such fraudulent behavior. Counterfeiting and the growing market for fake goods can erode the trust between a brand and its customers and can undermine a company's precious reputation.

While some luxury brands have stepped up their campaigns against counterfeiters, the legal paralysis resulting from the complexity of prosecuting a counterfeiter or a distributor of fake good creates an ideal space for Arianee. According to most forecasts, brick and mortar stores sales will remain the primary points of sale for luxury goods. Meanwhile 75% of total sales will take place in physical stores, the rise of online sales (25%)[13] will undoubtedly represent a challenge that brands need, both to maintain their images and to preserve the trust and the confidence of their online buyers.

A I Go to market: Three adoption streams

• *User centric and free of use for individuals*
The ICO will be the opportunity to build a committed community. To reinforce the use of Arianee, a portion of the tokens will be given to early users who introduce items that need certification.

• *Third parties: Experts & service companies*
The second-hand expert authentication authorities (Sotheby's, Christie's, Vestiaire Collective, insurance experts, etc.) will be able to stamp items: injecting trust and acquiring brand awareness plus the Smart-Link with the product owners. IT Service companies will work on IT tool adaptations for brands or experts and create new features (warranties, service books, social features, lost and found; or will simply create new businesses sparked by Arianee's protocol).

• *Brands*
Brands will be enrolled in protocol shaping and governance. Active lobbying will be used to communicate Arianee's virtues. Technology will be delivered that seamlessly includes Arianee in the current retail experience without too much effort. There will be an early start with the limited series of pioneering brands.

....

– **12** "Luxury Goods Worldwide Market Study, Fall–Winter 2017." **Bain Company.**
http://www.bain.com/publications/articles/luxury-goods-worldwide-market-study-fall-winter-2017.aspx.

– **13** "Luxury Goods Worldwide Market Study, Fall–Winter 2017." **Bain Company.**
http://www.bain.com/publications/articles/luxury-goods-worldwide-market-study-fall-winter-2017.aspx.

Business
Case studies

Personal luxury goods
(market value in billion dollars)

Offline sales   Online sales

Hard Luxury	Beauty	Accessories	Apparel	Other
22%	21%	30%	23%	4%

100

Source : OCDE report

https://www.businessoffashion.com/articles/news-analysis/fake-fashion-fuels-vast-illicit-profits-sea-of-human-misery
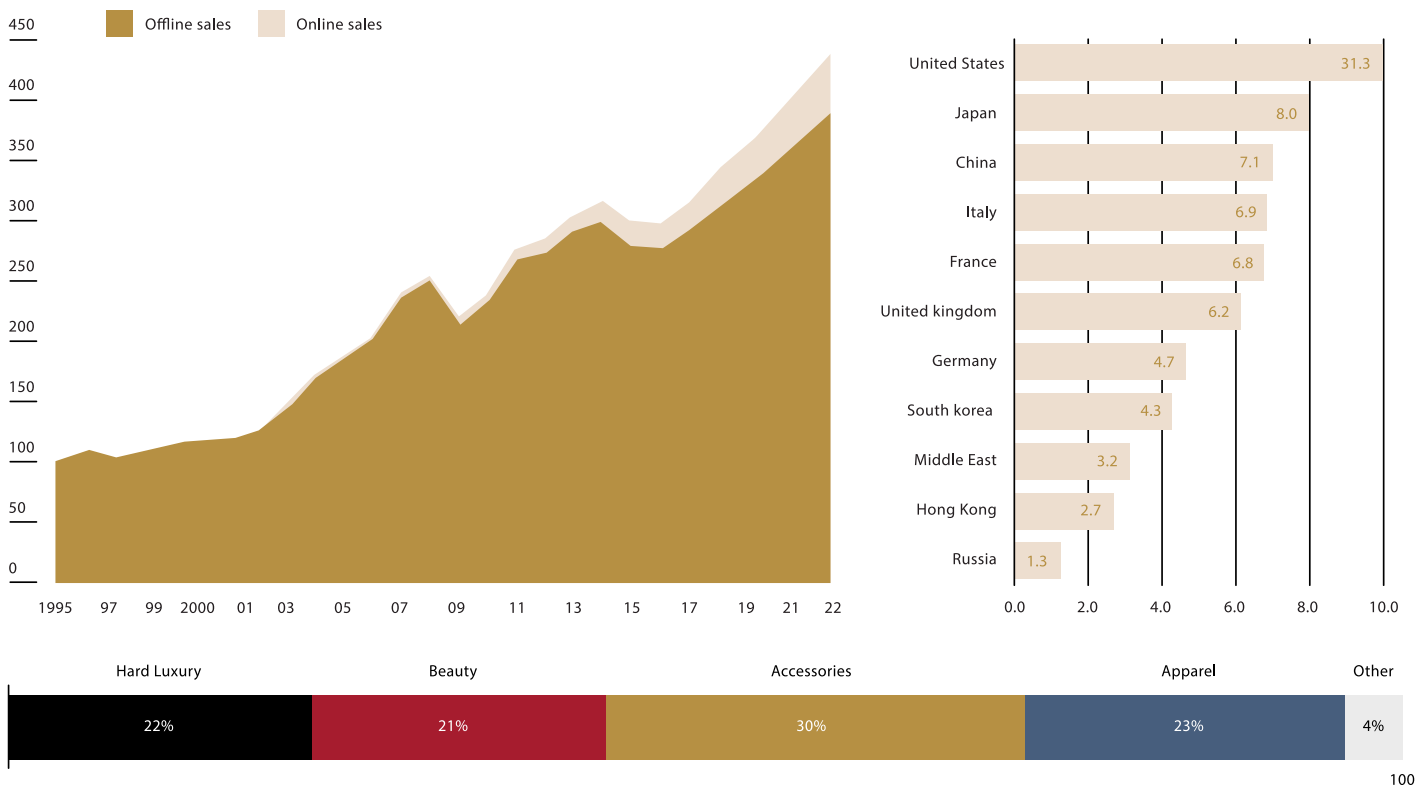
Arianee is a great fit for the luxury market; moreover, we have chosen to build our first MVP applications for the luxury industry because it presents several advantages that will facilitate the adoption of Arianee:

• The luxury industry is global and distributed worldwide. Considering all segments, the luxury market grew by 5% to an estimated €1.2 trillion globally in 2017. Worldwide, the personal luxury goods market experienced growth across all regions, driven both by more robust local consumption (up 4%) and by strong tourist purchases (up 6%).

• Serial numbers on products are common. Most luxury goods have a unique authentication identifier. Brands primarily use serial numbers, holograms tags, NFC, and RFID.

• The global personal luxury goods market is highly fragmented, with the presence of both global vendors and local players.

• With rising competition, manufacturers are bringing in innovative new products to meet the changing demands of customers in accordance with the latest fashion and lifestyle trends.

• In the luxury Industry, information technology (IT) is not internalized; brands usually use external technology company for their needs.

• As a large number of worldwide luxury brands are based in France and Switzerland, it's an industry with which the Arianee team is well connected.

Business
Case studies

B | Owner's App

The Owner's App is a mobile application which is the main user experience for luxury valuable product owners. This application is where owners can access their Smart-Assets stored in their Vault. They can also easily interact with the Arianee blockchain to perform all basic owner actions such as granting read access, adding a new asset, lending or transferring an asset.

While the application allows owners to access and write on the blockchain, the Owner's App stores some information locally, such as chat messages that are not destined to be stored on the blockchain. The Owner's App enables countless seamless experiences enabled by the Arianee blockchain. Here are a few examples:
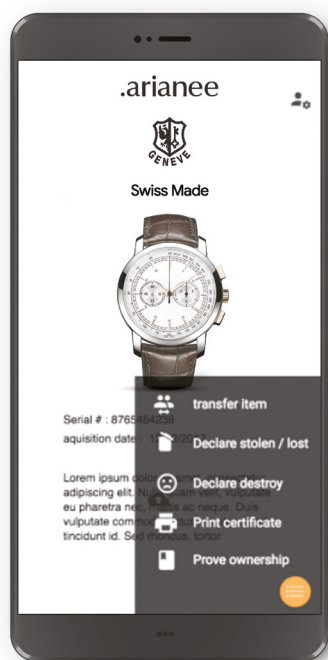
Customer Service Relationships:

Customer service is greatly facilitated through the use of the Owner's App. A customer can instantly grant access to a product's history to a customer service agent. If the product needs to be sent in for repairs, the owner can "lend" the Smart-Asset to the brand for a limited period. This action opens a communication channel with the customer service department, allowing the owner to monitor the status of the repairs directly in the app. Customer service agents or owners can also initiate chat channels to send inquiries. When the owner's product is returned, the details of the customer service relationship can still be consulted in the Smart-Asset.

VIP identification:

The in-store experience can vary according to a customer's profile. When they are in a store, owners can opt to scan their smartphones. Depending on selected metrics - which could include the type or number of products owned, the last time the customer acquired a product or any other information the owner might wish to share, the retailer will customize each owner's in-store experience to meet his or her profile.

One touch insurance claim:

The information sharing functionality on the Owner's App allows owners to greatly simplify the administrative burden when dealing with insurance companies. With a simple tap, they can share information with the insurance company about all - or selected - products in their Vaults in order to request a quote or file a claim.

Declare an object stolen or lost:

The Owner's App also allows a user to declare a product lost or stolen. The owner simply needs to select the Smart-Asset in the Vault and attach a temporary stolen or lost certificate, which is stored on the blockchain. This token is publicly visible on the blockchain in order to discourage resale.

Business Case studies

C | Brand terminal

The brand terminal is a web interface. It is the main user interface for the different functional teams in the company. It allows both basic interactions with the blockchain and additional services that can be linked to existing IT systems with third-party integrations.

Customer Care:

The customer care center is a module allowing seamless interactions with owners for their customer support needs. When contacted by an owner, customer care agents can initiate a conversation and can request access to and consult the owner's product history in order to troubleshoot instantly. If the product needs to be sent in for maintenance, the maintenance agent will log the maintenance in the Arianee blockchain and will keep the owner informed on the progress throughout the servicing.

Owner communication:

Brands can send communications to owners who received authenticity certificates for the products they produced. This communication can be tailored according to the Vault profile and relevant metrics such as the date of purchase of a specific model. For example, a brand could send a reminder for scheduled service on the second purchase anniversary or an invitation to a private sales event.

Authorized retailers:

A brand can connect to its data hub and log into the authorized retailer management system. There they can search for a retailer registered on Arianee and grant it an authorized certificate. This certificate is publicly visible and any Arianee user can verify it. The authorized status allows the brand to delegate some of its authentication privileges.

Grey market product tracing:

After identifying the serial number of an asset sold on the grey market, a brand can consult its product registry on the Arianee blockchain and follow the digital trail to the original reseller of the product. These classified transactions can then be used to perform pattern recognition analysis to uncover macro insights on the status of grey markets.

Product analytics:

The brand terminal offers access to a full suite of analytics. They will be able to access a wide range of global analytics about registered products such as the volume of transferred assets or the average holding period for specific models.

ARIA Token purchase:

Paid functionalities such as messaging and certification require a certain number of ARIA tokens to remunerate the facilitators maintaining the ecosystem. While brands can buy ARIA on the open market, they can also simply use fiat currency (dollars, euros, etc.) on the terminal instead. Fiat will automatically be exchanged for ARIA whenever a record needs to be certified to the blockchain.

D | Third party example applications

Third parties can access data on the Arianee blockchain. This will enable an ecosystem of service providers to develop apps using the open source and free Arianee protocol. Here are a few examples of apps that could be developed by third-party service providers

Insurance:

Current insurance application and claim processes are administratively cumbersome. This is a result of the high risks of insurance fraud and the need to prove the actual status of an insured product (in possession, stolen, lost, etc.).

Arianee can alleviate the need for such manual processes by providing a trustless proof of an object's status. If an owner declares an item to be lost or stolen, the Smart-Asset can be immediately frozen and only the insurer is be able to manage/update its status. It would be impossible for the user to transfer the stolen item.

Thanks to the information that is accessible through the Smart-Asset, an insurance reimbursement or a quote for a premium can be instantly assessed.

Customs:

Transporting a commercial good across international borders requires significant customs and duty filings, usually in the form of an ATA carnet. This can become a uselessly redundant task for commercial samples already registered on the Arianee blockchain. The Arianee blockchain already offers a trustless proof of a product's identity and status as a commercial sample. A single tagging on the Arianee blockchain could prevent the sale of the product and therefore offer sufficient guarantees to customs officials.

Business
Case studies

Lost and found:

With the Arianee protocol, an owner could declare an item lost or stolen the moment he/she realizes it is missing. Accordingly, based on the protocol, we can create the world's first global lost and found service. The app or website would list every item lost by or stolen from a member of the community.

This service could also add a reward system for the person who returns a lost object. Once a user finds an item, he could use the service and thanks to the Arianee protocol, determine with 100% certainty who has lost it. A message would be sent to the current owner through the Arianee app to announce that the lost item as been found. The platform can then serve as an intermediary between the two parties to manage the transactions and shipping or meeting, including the return of the item to its rightful owner and, potentially, a reward for the person who found it.

Decentralized marketplaces:

An interesting development with blockchain protocols is the emergence of decentralized marketplaces. These marketplaces free of trusted intermediaries are made possible by the trustless security that such protocols enable.

In such a decentralized marketplace, an owner could put a Smart-Asset up for sale online and request bids from potential buyers. The buyer could then unpublish the Smart-Asset once the sale has been concluded and automatically transfer the Smart-Asset to the buyer (who is, of course, the new owner). This transaction could be done completely pseudonymously and securely. Ownership heritage would also be facilitated. Imagine that a classic car had been in a family and 20 years after it had been sold, the previous owner would like - for whatever reason - to contact the current owner. If the previous owner had the public key of the Smart-Asset, it would be no problem to send a message to the current owner.

Expanding to other valuable objects

While luxury products will be the main focus of the initial Arianee development, there would be a natural, organic expansion of the Arianee solution to other valuable objects including, for example, artwork, musical instruments, wine, and antiques. Below is an overview of each market and its potential for Arianee.

Musical instruments:

The global market for musical instruments and audio gear is enormous, worth some $17 billion, according to *The Music Trades.*[14] Although there are some fake instruments on the market, the greater challenge - and the area where Arianee would be of considerable use - is the trade in stolen instruments. Quality instruments generally have unique serial numbers and the added layer of protection provided by Arianee would make it more difficult for thieves to traffic in stolen goods and easier for honest consumers to be certain that the seller of an instrument has, in fact, the right to sell it.

Artwork:

The online art market is growing dramatically. In fact, according to Bloomberg[15], it is increasing at an annual rate of about 24%. Its market cap is expected to exceed $9.5 billion annually by 2020. At the auction house Sotheby's, internet buyers spent $155 million in 2016, up 20% from the previous year. Its competitor, Christies, saw a doubling of its online-only revenues in 2017.

While the growth and the potential of online sales are impressive, they have led to several chronic challenges for the global art market. The most obvious of these are counterfeiting and fraud.

Business
Case studies

In fact, Yan Walther, CEO of Geneva-based FAEI, says that an often-heard claim that half of the art circulating on the market is forged or misattributed is likely to be a conservative estimate[16]. A piece of art linked to an Arianee certificate would allow a buyer to confirm its provenance while guaranteeing the validity of a transaction. And as the art changed hands, the blockchain technology would confirm – forever – the identity of the artist and of the successive owners.

Wine:

In the fine wine industry, the counterfeit market makes up an estimated 20% of international sales if all types of fake wine are considered. Problems with document tampering and other fraudulent activities continue to affect the entire supply chain pipeline – from the grape to the glass – and every step in between.,[17/18]

To date, authenticators could identify an individual bottle as a counterfeit; however, they haven't found a way to certify a bottle as authentic because of the susceptibility of documents to tampering and the inability to ensure that a certificate would remain with a bottle of wine as it changed ownership and location.

An Arianee certificate would remain digitally connected to the bottle of wine to which it was originally linked, ensuring the provenance of the bottle and reducing the possibility of counterfeiting and the other fraudulent activities that have plagued the industry.

Antiques:

For centuries, people have been interested in art, furniture and other collectibles. This interest generates value, of course, and the value has led to a proliferation of fake antiques and forgeries. Not only would a digital certificate of authenticity linked to an antique eliminate a buyer's uncertainty in the purchase of a product, it would also trace its journey through time.

As is the case with any item of value, a buyer who purchases an antique online runs the risk of buying a fake or improperly described product or of being the victim of fraudulent behavior.

An antique linked to an Arianee certificate would allow a buyer to confirm its provenance while guaranteeing the validity of a transaction. And as the ownership of an antique changes, the blockchain technology would verify the authenticity of the item and add a layer of confidence in the transaction.

Other Markets

Arianee's protocol has the potential to benefit many fields, and will enhance trust and generate opportunities on a number of levels. Pharmaceuticals, weapons, pets and food products, for instance, present similar needs for traceability and authenticity. While the industrial and commercial processes mean that business architecture and user interface will need to be specifically crafted, the Arianee blockchain can be the foundation upon which solutions for these industries are built.

– 16 "Fine Arts Experts Institute: Lab Sleuths in Geneva Help Art World Uncover Fakes." September 19, 2014.
http://artdaily.com/index.asp?int_sec=11&int_new=73562#WqTx9pPFKuW.
– 17 "Everledger Secures the First Bottle of Wine on the Blockchain." Fintech Finance (blog), December 9, 2016.
http://www.fintech.finance/01-news/everledger-secures-the-first-bottle-of-wine-on-the-blockchain/
– 18 "How To Avoid Buying Fake Wine." Accessed March 13, 2018.
https://www.forbes.com/sites/jeanniecholee/2017/01/22/how-to-avoid-buying-fake-wine/#729690149daa.

Technical Implementation

Decentralized blockchains present significant undeniable benefits compared to traditional databases. They bring a level of distributed trust through consensus mechanisms that enable viable shared decentralized databases.

However, this architecture means that blockchains present some limitations. They are not efficient for storing vast amounts of data due to the network limitations. Today blockchains are also limited as to the number of transactions they can process at any given time. This is because the number of transactions that can be processed can never exceed the processing speed of any one node participating in the blockchain.

This leads to a key problem that currently affects blockchain, namely scalability. While innovative individuals and companies attempt to overcome the current limitations of purely blockchain-based databases, the current prevailing wisdom is to combine the strengths of a conventional database with that of a blockchain. We have adopted such a hybrid model to combine the advantages of both worlds. The blockchain will be used as the immutable shared repository for all valid assets registered on the Arianee platform. However, to prevent pollution of the Arianee blockchain by fake or irrelevant data, each asset entered by a user will be warehoused until it is certified by a verified brand or expert, at which point it will be recorded on the Arianee blockchain.

Below is a discussion on the choice made for the Arianee technical implementation.

Why Arianee chose to use a blockchain

In considering the best possible technological database for the Arianee platform, it was important to consider all of the existing options. We realized early in the process that a blockchain solution was ideally suited to our needs but the decision wasn't taken lightly and we'd like to talk about some of the factors that influenced not only our adoption of blockchain but more specifically, a consortium blockchain model.

Disintermediation:

This complicated sounding term means, simply, that a blockchain makes it possible to share a database across so-called boundaries of trust without an intermediary. Blockchain transactions have their own inherent proofs of validity and authorization and thus, don't require a central administrator to enforce them. Transactions can be verified, processed, and executed independently by multiple nodes (users) and the blockchain, acting as a consensus mechanism, ensures that those nodes stay in sync.

Compare this with a regular database: its contents are stored in the memory of a specific computer system, meaning that the data can be destroyed or corrupted by anyone with sufficient access to the system. Accordingly, the security of your data is only as reliable as the human-controlled system hosting the database.

Stability:

Thanks to their built-in redundancy, blockchain-powered databases are also highly fault-tolerant. Each transaction has to be processed by every node, so no individual node is essential to the database as a whole. Because the nodes are connected to each other in a dense peer-to-peer fashion, numerous communication links would have to fail for the system to malfunction. Thanks to the blockchain, a node that goes down is always able to catch up on any missed transactions.

When blockchain nodes are connected, they keep themselves in sync automatically. Two additional characteristics of blockchain-powered databases are particularly useful for Arianee. First, nodes can be easily added to or removed from the network. Second, external users can address transactions to an individual node or to multiple nodes, and the transactions are automatically shared with all the other nodes on the consensus blockchain.

Performance:

It should be pointed out that blockchains are, by their nature, slower than centralized databases for three significant reasons: each blockchain transaction has to be digitally signed and verified; energy has to be invested in ensuring that consensus is reached by the nodes in the network, a process which may involve back and forth communication; and finally, each transaction on a blockchain has to be processed independently by every node in the network. This redundancy means that the blockchain is doing an enormous amount of work to reach the same end result as its centralized counterpart. But these attributes – signature verification, consensus, and the redundant processing – ultimately combine to suit the platform ideally to Arianee's needs.

Immutability:

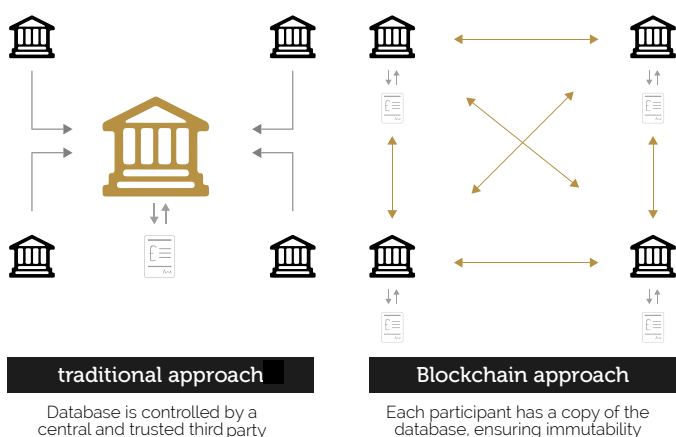Immutability is a core feature of blockchain technology. When the participating nodes have agreed to a transaction and shared it on the distributed network, it cannot be undone. This means that a provider of data can prove that his/her data hasn't been altered and conversely (and logically), the recipients of that data can be confident that the data hasn't been altered. Centralized databases can't offer the same assurances.

Technical Implementation

Summary:

In conclusion, it should be noted that blockchain technology is not intended as a universal across-the-board replacement for traditional databases, which will always be especially well-suited for the recording of some types of information. Blockchain is, however, ideal for Arianee and its ambitious vision.

As we have reported, one of the great benefits of blockchain is its decentralized nature. It should be clear at this point that data stored in a centralized database can be corrupted or compromised by anyone who might have access to it. We pointed out that the security of a centralized database can only be as reliable as its administrator's infrastructure. Because the data storage that characterizes blockchain technology is decentralized, security is an inherent part of its structure and thus, perfectly suited to Arianee and its needs.

traditional approach	Blockchain approach
Database is controlled by a central and trusted third party	Each participant has a copy of the database, ensuring immutability

Which blockchain?

A ǀ A consortium blockchain

There are three major blockchain models – public, private and consortium (federated) – each of which has its own advantages and liabilities. The public blockchain model is the most widely known because its use is so prevalent in cryptocurrency applications like Bitcoin and Ethereum. Public blockchains are particularly attractive because they offer the greatest degree of decentralization. However, public blockchains are expensive and their transaction speed is are less than optimal. Private and consortium blockchain platforms offer the same level of user control and privacy for users as public blockchains. They do, however, cede some of the decentralization of public blockchains for higher efficiency, faster speed and lower costs of operations.

The Arianee Foundation has opted for a consortium blockchain platform and to help you understand the reasons for that decision, it is worth reviewing the three major models briefly.

Public Blockchain:

Blockchain technology was designed to eliminate intermediaries in any situation involving the exchange of assets. Simply expressed, it sets up block of peer-to-peer transactions, each of which is verified and synchronized with every node (user) before it is written to the system.

Only after these transactions have been verified and synced can the next transaction be executed. Anyone with a computer connected to the internet can set him-/herself up as a node, which is then synchronized to the entire blockchain history.

The need for each transaction to be verified and synced with every node makes a public blockchain extremely secure but also slow and costly. With each new node that joins the public blockchain, the amount of electricity required to run a transaction increases.

The advantages are that each transaction is public, users can maintain anonymity, and the network is fully decentralized.

Private Blockchain:

Private blockchains, to a certain extent, allow intermediaries back in. 'Write permissions' are centralized to a single authority. 'Read permissions' can be public or restricted to an extent determined by the organization, depending on the needs of a specific application. Private blockchains allow users to take advantage of blockchain technology by setting up groups whose participants can verify transactions in the context of the organizing entity.

Private blockchains are more susceptible to security breaches than public blockchains but they are particularly well suited to situations that require compliance with data privacy rules and regulatory issues.

Consortium Blockchain:

A consortium blockchain is partly private and the distinction between consortium and fully private systems can be confusing. Ethereum co-founder Vitalik Buterin has succinctly defined the differences, saying, **"So far there has been little emphasis on the distinction between consortium blockchains and fully private blockchains, although it is important: the former provides a hybrid between the 'low-trust' provided by public blockchains and the 'single highly-trusted entity' model of private blockchains, whereas the latter can be more accurately described as a traditional centralized system with a degree of cryptographic auditability attached."**[19]

– 19 -The Music Trades," n.d.
https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Technical Implementation

In short, with a consortium blockchain model, rather than allowing anyone with an internet connection to participate in the verification of transaction processes or vesting full control in only one company, some selected nodes are predetermined.

Accordingly, the consortium platform model offers many of the advantages associated with a private blockchain, including enhanced efficiency and transaction privacy, but it doesn't consolidate the power within a single company.

And it was these advantages, along with transaction speed and relative economy, that helped the Arianee founders determine that it was the clear choice for Arianee.

	Public No centralised management	Consortium Multiple organizations	Private Single organization

Participants
(nodes)
	Permissionless
	
	• Anonymous
	• Could be
	  malicious
	• Free entry for
	  miners
		Permissioned
		
		• Identified
		• Trusted
		• Miners selection
		  process
			Permissioned
			
			• Identified
			• Trusted
			• Closed mining,
			  one central miner

Consensus Mechanisms	Proof of Work, Proof of stake, etc.
	
	• Large energy
	  consumption
	• No finality
	• 51% attack
		Voting or multi-party consensus algorithm
		
		• Lighter
		• Faster
		• Lower energy
		  consumption
		• Enables finality
			Voting or multi-party consensus algorithm
			
			• Lightest
			• Fastest
			• Lowest energy
			  consumption
			• Enables finality

Transaction Approval Freq.	Long Bitcoin: 10 min or more	Short 100x msec	Short 100x msec

Conclusion:

Public and fully private blockchain technologies do not meet Arianee's protocol needs and expectations. A consortium blockchain is more specifically aligned with our needs, particularly because it offers many of the same advantages of a private blockchain, but operates under the management of a group instead of a single entity. This is how we envisage the operation of the Arianee network.

Technical Implementation

B | A proof of authority consensus

As stated previously, we believe that a consortium blockchain is the best compromise between technical performance and decentralization. We still need to define how consortium nodes are selected.

Let's first define the two kinds of nodes that are necessary to sustain such a blockchain infrastructure.

Validation nodes:

A validation node is a node which validates information, makes sure it's true, and passes the information along to other nodes, thus enabling the transfer of value from location A to location B. Anybody who wishes to run a validation node can run one; there is no restriction.

The absence of barriers to entry to run a validation node is essential as it ensures transparency and auditability of the blockchain. In extreme cases, it also means that the blockchain can be forked to maintain the infrastructure.

Authority nodes:

Authority nodes are a subset of validation nodes because every authority node is also a validation node. authority nodes are needed to maintain the global Arianee infrastructure. authority nodes are the only nodes capable of confirming transactions and sealing blocks on the Arianee blockchain and receive a remuneration for this work. Because of their crucial role in a consortium blockchain and their number limited by design, authority nodes need to be selected according to a clear process. To make sure a malicious authority node cannot inflict damage on the network, any authority node can sign, at most, one of a number of consecutive blocks.

Authority node selection method:

In consortium blockchains, methods to choose these nodes can be classified in two main categories:

- selection by vote,
- selection by procedure.

Selection of authority nodes by vote is usually done by staking tokens to select your "delegate". In other words, every token holder who wishes to participate in the selection of authority nodes receives as many votes as tokens they are holding. The nodes receiving the most votes during a given period are responsible for sealing blocks during this period. While this system has its merits, it has been criticized for its vulnerability

to manipulation[20]. In certain conditions, an ill-intentioned operator could gain control of all the validator nodes and compromise the blockchain.

Selection by procedure is also called "Proof of Authority". To be effective, a Proof of Authority consensus system needs to respect these two conditions:

- Identity of the validating nodes must be true and verified,
- The procedure which candidates must follow to become an authority node needs to be clear and the same for all so that everybody can trust its integrity.

The Arianee protocol is designed to respect these two conditions.

Candidates to become an authority node must go through a strict identity verification process. Verified brands and experts are automatically eligible as they have already completed a strict identity confirmation process. It is however, important for the integrity of the Arianee blockchain that some nodes are completely independent from brands and experts. Therefore any interested party can go through a similar identity process to become eligible to become an authority node. There is no limit on the total number of authority nodes; therefore, any eligible node can become an authority node if it notify the Network Onboarding Circle. The Network Onboarding Circle will then move forward with the onboarding process.

At the launch of the Arianee blockchain, the Network Onboarding Circle will deploy a number of pre-selected independent authority nodes, distributed around the world. The importance of these pre-selected authority nodes will diminish as additional authority nodes join the network.

Shared **Transaction nodes** / Member 1 / Member 4 / Member 2 / Member 3 / **Mining nodes**
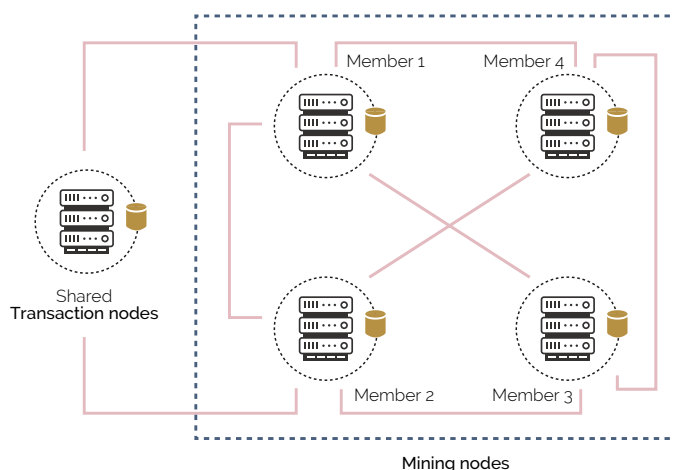
– 20 Governance, Part 2: Plutocracy Is Still Bad, Vitalik Buterin
https://vitalik.ca/general/2018/03/28/plutocracy.html?utm_campaign=Market%20Report&utm_source=hs_email&utm_medium=email&utm_content=61785122&_hsenc=p2ANqtz-9r-aR7DD6kvBShjeV1dAKKJ2k8NZuPlVHgQiG1bCEBQ2WKlvRKGozZU8MqkMfI412MOPYtsraizF_qWinODygaFisiTw&_hsmi=61785122

Technical Implementation

C | Blockchain platform

Smart contracts are necessary for the deployment of the Arianee Network. We have looked carefully at both Ethereum and Tezos blockchain technology and would like to offer a summary to our readers.

For obvious reasons, no one can describe Ethereum better than Ethereum can and for a detailed look at its blockchain technology, Arianee would like to share an excerpt from the organization's website:

"Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference. These apps run on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property. This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past and many other things that have not been invented yet, all without a middle man or counterparty risk. Ethereum was the first technology to implement the concept of smart contracts. The community is very strong and most of the actual projects work on the Ethereum blockchain.[21]"

	ETHEREUM	TEZOS
CONCEPT	smart contract platform	smart contracts platform + built-in governance + facilitates formal verification
CONSENSUS	proof of work → proof of stake	delegated proof of stake
NATIVE CURRENCY	ether (ETH)	tezzies (XTZ)
RELEASE DATE	July 2015	expected late 2017
RELEASE METHOD	presale in July 2014 raised $18M in bitcoin	presale in July 2017 raised $232M in bitcoin and ether

Linda Xie published an excellent piece that we recommend on *medium.com*, which provided a concise and accurate introduction to Tezos[22]. Xie points out that Tezos, like Ethereum, is a a smart contracts platform but that it incorporates a process for upgrading the protocol over time through an on-chain governance system that allows for a smooth evolution of the

blockchain rather than having to hard fork, where a blockchain is split into two separate versions.

While Arianee believes that, given the different purposes they serve, multiple smart contract platforms will coexist well into the future. For the time being, Arianee has opted for the Ethereum platform because it is more mature in every respect. We do, however, admire the ambition and energy Tezos has demonstrated and we reserve the right to switch to its technology when it has demonstrated that it has sufficient maturity to support the Arianee protocol.

D | Smart contract standards

Smart contracts on the Arianee protocol respect the standard established by the following ERC.

ERC-20 Token Standard (or ERC-777)

This standard provides basic functionality to transfer tokens, and also allows tokens to be approved so they can be spent by another on-chain third party.

ERC-20 defines six differents functions for the benefit of other tokens within the Ethereum system. These are generally basic functionality issues, including how tokens are transferred and how users can access data about a token. ERC-20 also prescribes two differents signals that each token takes on and which other tokens are attuned to.

Put together, this set of functions and signals ensures that Ethereum tokens of different types will typically work in the same way in any place within the Ethereum system. This means that almost all of the wallets that support the ether currency also support ERC-20 compliant tokens.

https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md

This ERC will be used by the Arianee token utility. It forms the basis of the Arianee network and economic model.

Every paid feature on the Arianee network requires Arianee token utility, and will be divided among the Consortium, facilitators, and users.

ERC-721: Non-fungible Token Standard

This standard allows for the implementation of a standard API for non-fungible tokens (henceforth referred to as "NFTs") within smart contracts. This standard provides basic functionality to track and transfer ownership of NFTs.

https://github.com/ethereum/eips/issues/721

Certificates are comparable to non-fungible tokens. ERC721 is completely related to this use case and the Arianee network will use it to emit new certificates and let users transfer and prove ownership.

Technical Implementation

ERC-725/735 : Identity & Claim Order

The following describes standard functions for a unique identity for humans, groups, objects, and machines.

This identity can hold keys to sign actions (transactions, documents, logins, access, etc), and claims, which are attested from third parties (issuers) and self-attested, as well as a proxy function to act directly on the blockchain.

We will use this standard to define people, companies, and others entities to ensure liability over time.

E | ARIA: a utility token

The Arianee blockchain uses a token called ARIA. The ARIA is a token used by brands and third parties to pay for premium features that leverage the blockchain. This fits the definition of a utility token as outlined by the growing body of blockchain token guidelines being established around the world[23].

Arianee's fuel:

The ARIA token is essential to sustaining a blockchain. ARIA spent by brands on premium features will be split among facilitators who help execute the transactions, the Arianee entity, authority nodes and a reserve with a new vesting period. One portion will be used to compensate authority nodes each period. Another portion will be assigned to the Arianee fund for platform maintenance and to seed fund promising third-party ecosystem projects providing exceptional value to the Arianee platform. The rest will go to the third party which facilitated the transaction.

The ARIA is also a solution to prevent communication spam and pollution of the blockchain with falsified certificates. It guarantees - by its nature - spamless communication, and trust in the certification and expertise.

Adjustable fees for predictability:

We wish to ensure that paid feature costs are predictable and stable for companies using them. Because the ARIA/USD exchange rate is free floating, the Arianee platform will include a mechanism to adjust paid feature fees. Fees for paid features will be regularly adjusted to maintain a stable cost in fiat currency. The value of fees in ARIA will be adjusted based on the weighted current average ARIA market rate across exchanges.

F | Zero-knowledge proofs

Privacy and auditability are very important for Arianee. As you may already be aware, the Ethereum Metropolis (Byzantium) upgrade adds a new cryptographic tool (zk-SNARKs) that was pioneered by Zcash. The zk-SNARKs, meaning *zero-knowledge Succinct Non-interactive Argument of Knowledge*, is a very important new tool in the Ethereum box that we will be using.

The addition of zk-SNARK technology into Ethereum is another factor that draws us to this technology. Arianee will implement zk-SNARKs as soon as it will be efficient to do so.

G | Data storage

So far, to store all external data we have opted for IPFS *(https://ipfs.io)* solution regarding media content storage, such as user images/photos and video information. IPFS provides resilient access to data, independent of low latency or connectivity to the backbone. IPFS and Blockchain are a perfect match. Large amounts of data can be addressed with IPFS, and it is possible to place the immutable, permanent IPFS links into a blockchain transaction. This timestamps and secures content, without having to put the data on the chain itself. We are also paying attention to the Ethereum roadmap with decentralized storage project called Swarm. We will choose the best option available at the time of deployment of the Arianee protocol.

H | Open source

Open source software development is essential to building trust and safety into blockchain networks. Here's why it matters from a governance perspective for the Arianee project.

Arianee's role is to define, build and maintain the Arianee protocol. We want to build a decentralized network that allows participants to trust each other, align their incentives, and punish fraud. It is developed in the open, free for the world to use and modify – wholly independent of one or even a handful of corporate interests – and used by hundreds of passionate users.

The Arianee protocol will be available for free use and modification under a permissive copyright license, and the full history of that development is visible within a public software repository like Github. All code is released under the LGPL-3, a copyleft license that requires all future derivative works to be released under the same non-proprietary licensing. If needed, developers will be able to freely fork the Arianee Core Github repository to build a purpose-specific Arianee-compatible blockchain.

●

....

– 21 https://www.ethereum.org/

– 22 https://medium.com/@linda.xie/a-beginners-guide-to-tezos-cg618240183f

– 23 -We reference here the definition of a utility token as established by the Swiss FINMA in Guidance 04/2017: "Utility tokens are tokens which are intended to provide access digitally to an application or service by means of a blockchain-based infrastructure."

08
Technical Architecture

··· .

T he technical architecture of the Arianee platform will be articulated as follows. The Arianee blockchain is a Proof of Authority (POA) blockchain, Ethereum-based with a collection of smart contracts to define the backbone of our protocol. A collection of proxy servers connected to the blockchain will be deployed that will enable the scaling of the platform in read-only mode.

A similar process will be applied for storage nodes in order to store certificate data. The exact architecture will depend on the distributed data storage solution chosen. IPFS and Swarm are the most likely solutions but the decision will depend on the maturity of each solution at time of deployment. End-user applications such as the owner app, the brand terminal or third-party ecosystem developed apps will connect to the platform using web3js connector.

Overall Architecture

Blockchain
Infra & code

Business
smart contracts

Identity
ERC 725/735

Certificates
ERC721

Unity token ERC223
Split value between partners

Smartcontracts

Ethereum state machine

Public blockchain with proof of authority consensus
Maintained by Arianee & partners

Proxy servers for scaling	IPFS Nodes / Swarm Static asst (pictures / metadata)	
Mobile wallet for users	Mobile wallet for experts	BackOffice app for brands
Other app built by the ecosystem	Other app built by the ecosystem	

Technical Architecture

Information hierarchy and data encryption

Information hierarchy and data encryption are key for a successful blockchain architecture. To store different kinds of information, Arianee will implement a payload format with security checks to validate origin. All users will have the choice to encrypt this information to avoid storing any plain text.

```
{
'payload': {
'type': 'PRODUCT_TOKEN_V1', 'ean': '...',
'brand': '...',
'description': '...',
'material': [ '...',
],
'size': '...', 'color': '...', 'photos': [
'(uri_photo_1)',
... ],
'issuer': '...',
},
'sig': { 'v': '...',
'r': '...',
's': '...' }
}
```

HASH(): Cryptographic hash function SERIALIZE(): Serialization function

pt : Product Token

signature = HASH(SERIALIZE(pt.payload)) PUBHASH(pt) = HASH(SERIALIZE(pt))

PubKey officially identifying the brand (or a well-known expert)

Signature of the payload with the PrivKey associated to the issuer (PubKey)

```
{
'payload': {
'type': 'PRIVATE_PROPERTY_TITLE_V1',
'asset': {...},
'beneficiary': '...'
'issuer': '...',
}, 'sig': {
'v': '...', 'r': '...', 's': '...'
} }
```

Chain of nested Private Property Titles rooted by a ProductToken

PubKey of the new owner

Owner's pubkey
(pubkeys are used only once)

Signature of the payload with the PrivKey associated to the owner's PubKey

HASH() : Cryptographic hash function SERIALIZE(): Serialization function ppt : Private Property Title

signature = HASH(SERIALIZE(ppt.payload)) PUBHASH(ppt) = HASH(SERIALIZE(ppt))

Technical Architecture

```
'payload': {
...,
'issuer': '...'
},
'sig': {...}
```

Product token

Brand transfers property to User1

```
'payload': {
'type': '...,
'asset': { },
'issuer': $P_b$,
'beneficiary': $P_{u1}$
},
'sig': {...}
```

Property Title USER1

User1 transfers property to User2

```
'payload': {
'type': '...,
'asset': { },
'issuer': $P_{u1}$,
'beneficiary': $P_{u2}$
},
'sig': {...}
```

Property Title USER2

Pb: Brand's PubKey
Pu1: User1's PubKey
Pu2 User2's PubKey

```
{
  'payload': {
  'type': 'PROPERTY_TITLE_V1',
  'asset': {
      'payload': {
      'type': 'PROPERTY_TITLE_V1',
       'asset': {
          'payload': {
          'type': 'PRODUCT_TOKEN_V1',
      'ean': '...',
          ...,
          'pubkey': $P_b$
          },
      'signature': ...
        },
      'from': $P_b$,,
       'to': $P_{u1}$
        },
       'signature': {...}
      },
    'from': Pu1,
     'to': $P_{u2}$
    },
    'signature': {...}
}
```

Property Title

Transfer from User1 to User2

Transfer from Brand to User1

· Users can audit the chain of ownership up to the root (Product Token issued by the brand) **Brands' public keys must be published and verifiable**

· Users' privacy is protected by one-time-use public keys (pseudonymous system)

Technical Architecture

Workflows

A | Gas and Aria coordination

All operations on the blockchain require the use of Gas to efficiently allocate blockchain computation power. Gas is a necessary but costless unit complementary to ARIA. Only paid transactions (authenticity certification and messaging) require ARIA in addition to Gas to be expended. While Aria can be acquired on the Arianee platform or on e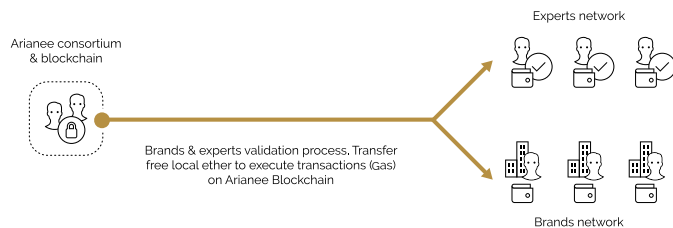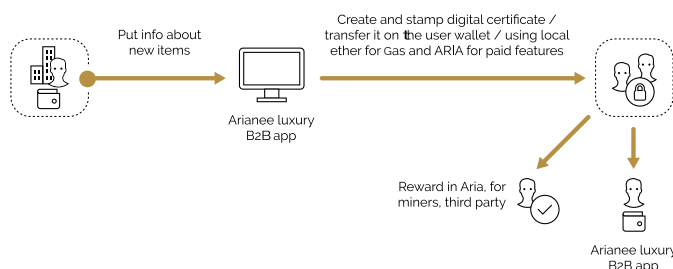xchanges, Gas is distributed to verified brands, verified experts and owners with at least one certified Smart-Asset at no cost according to need. Each one of these users receives a Gas allotment which can be replenished once depleted.

Arianee consortium
& blockchain

Experts network

Brands & experts validation process. Transfer free local ether to execute transactions (Gas) on Arianee Blockchain

Brands network
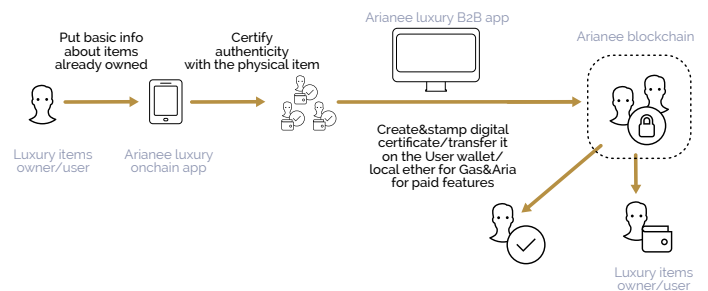
B | Smart-Asset creation for new items

Verified brands can elect to register their products on the Arianee blockchain before the sale to a customer. For each new item, a Smart-Asset must be recorded to the Arianee blockchain. When a verified brand adds a Smart-Asset this way, it is automatically certified and registered in the brand's Vault. While the creation of the Smart-Asset only requires Gas, the authenticity certification requires both Gas and Aria to be expended.

At the time of purchase, the owner will transfer the Smart-Asset to their Vault by simply scanning with the owner's app a single-use QR code provided by the brand.

Put info about new items

Create and stamp digital certificate / transfer it on the user wallet / using local ether for Gas and ARIA for paid features

Arianee luxury B2B app

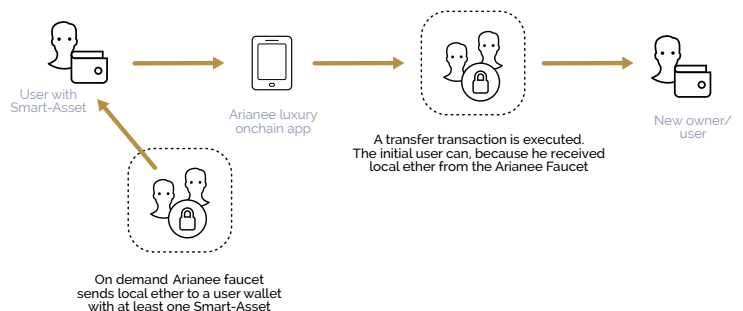Reward in Aria, for miners, third party

Arianee luxury B2B app

C | Smart-Asset creation for existing items

A user can transfer a certified Smart-Asset to another user's Vault. This transfer is recorded on the blockchain and the Gas expended is taken out of the sender's Gas allotment. To be finalized, the transfer needs to be accepted by the receiver.

Put basic info about items already owned

Certify authenticity with the physical item

Arianee luxury B2B app

Arianee blockchain

Luxury items owner/user

Arianee luxury onchain app

Create&stamp digital certificate/transfer it on the User wallet/ local ether for Gas&Aria for paid features

Luxury items owner/user

D | A Smart-Asset transfer from a user

A user can transfer a certified Smart-Asset to another user's Vault. This transfer is recorded on the blockchain and the Gas expended is taken out of the sender's Gas allotment. To be finalized, the transfer needs to be accepted by the receiver.

User with Smart-Asset

Arianee luxury onchain app

A transfer transaction is executed. The initial user can, because he received local ether from the Arianee Faucet

New owner/ user

On demand Arianee faucet sends local ether to a user wallet with at least one Smart-Asset

Technical Architecture

E | Token issuance

Arianee will operate with a token model ERC20/777 on the Arianee blockchain. The ARIA token is the token listed on cryptocurrency exchanges. Between the ICO and the release of the Arianee blockchain, tradeable AriaOption tokens will be released as an ERC20 token on the Ethereum main network.

Once the Arianee blockchain is released, a double smart contract (one on the Ethereum main network and one on the Arianee blockchain) will allow investors to convert their AriaOption tokens to Aria tokens on the Arianee blockchain.
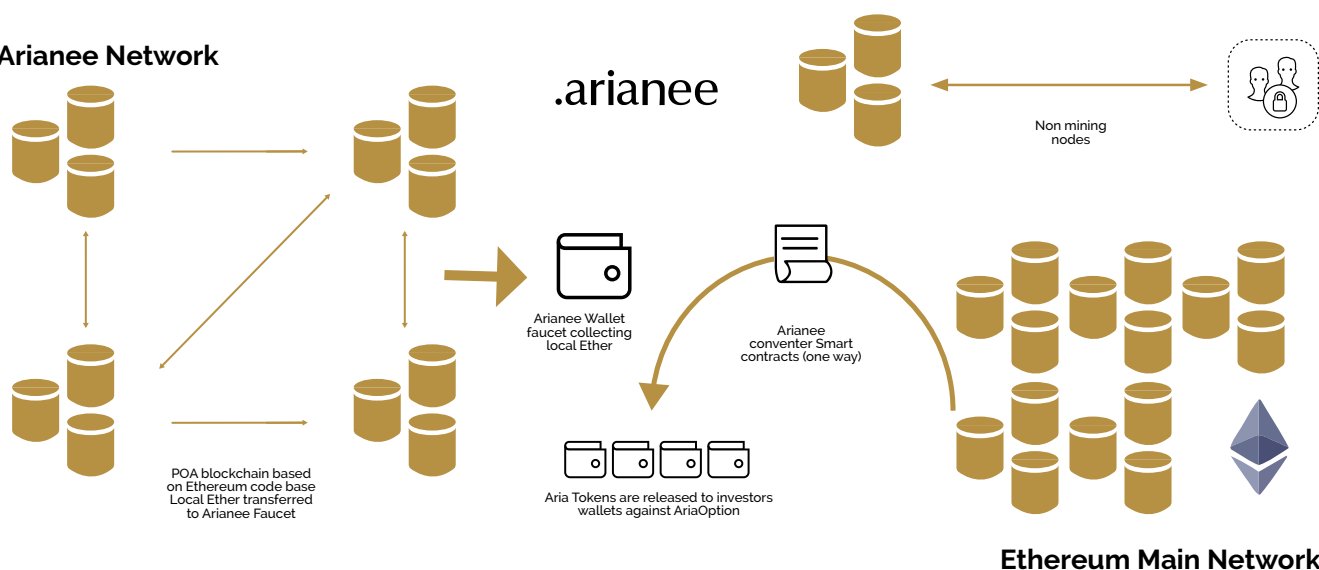
Ethereum Main Network

Arianee ICO
Smart contract

Aria Tokens are released
to investors wallets
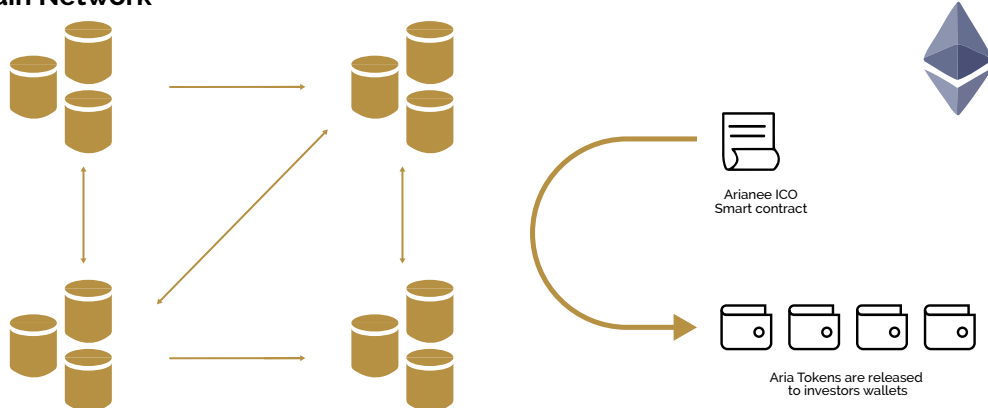
F | System overview

The Arianee blockchain is an Ethereum-based Proof of Authority (PoA) network. authority nodes are validated by the Arianee Network Board. All generated local ether for Gas goes to Arianee's faucet wallet. Authority nodes are paid in Aria from fees for premium features. Validation nodes can sync the blockchain (exchanges, third party, etc.). ICO investors convert AriaOption to Aria. Exchanges can connect to the Arianee blockchain to exchange and list Aria Tokens.

Arianee Network

.arianee

Non mining
nodes

Arianee Wallet
faucet collecting
local Ether

Arianee
conventer Smart
contracts (one way)

POA blockchain based
on Ethereum code base
Local Ether transferred
to Arianee Faucet

Aria Tokens are released to investors
wallets against AriaOption

Ethereum Main Network

Stakeholder incentives and Governance

Stakeholder incentives

Free to the owner:

The usage of the Arianee platform is completely free for an owner. The Arianee Vault is the most convenient solution to digitize and share the history of an owner's products. Owners can register their products in a Smart-Asset on the owner's app for free. Once the Smart-Asset is recorded on the Arianee blockchain, it is freely tradable between owners. All such transactions are recorded on the blockchain and Gas costs are covered by an allowance from the Arianee Faucet Wallet.

Owners, like every other user, whether registered or not, can run a validation node to verify the integrity of the blockchain.

Brands:

Verified brands use both free and paid features on the Arianee Network. Paid features offer a truly innovative service that allows brands to fight against counterfeiting and keep a link open with the actual owner of a product much more effectively. Paid features require ARIA. When they are used, utility tokens are split between Arianee, the facilitator, and authority nodes. This redistribution model ensures that all stakeholders in the Arianee platform are incentivized to contribute. While verified brands have a special role on the Arianee platform, they can also act as facilitators if they have the ability to build software leveraging the Arianee network.

Expert third parties:

For certain industries, such as fine art, expert third parties are required because there are no brands to certify the authenticity. Moreover, in certain conditions brands do not wish to take care of certifying the authenticity of their product after purchase. In these cases, verified expert third parties can be the sole sources capable of certifying the authenticity of a product. This is why verified expert third parties are necessary to the Arianee network and have access to similar authentication certification and smart messaging premium features paid for with ARIA.

Expert third parties are incentivized to participate in the Arianee platform as a it is a funnel for new clients in need for authenticity certification. Moreover, expert third parties can monetize their reach with product owners.

Enriched third-party ecosystem:

Arianee's potential can only be fully realized if a dedicated and diverse ecosystem of developers and partners are incentivized to build on the platform. Arianee will focus on delivering its open source main protocol in a manner that will foster business and non-profit opportunities for freelancers, companies, and NGOs. Arianee will provide technical guidance, APIs, and middleware tools to create smart contracts that will enhance the Arianee protocol or build software and interfaces using the main Arianee protocol. Enriched third party will always be free to build, deploy and give or sell their applications to sot users and brands using both free and paid features on the Arianee platform.

Participants in the enriched third-party ecosystem are remunerated thanks to the shared value smart contract. Every ARIA collected is distributed between the miners, the third party involved in facilitating the transaction and the Arianee Fund.

The Arianee fund will finance innovative projects leveraging the Arianee blockchain or updating it. Project selection for financial support will be the responsibility of the Executive Board.

In this way, we believe that we will encourage the rise of a fully resilient ecosystem.
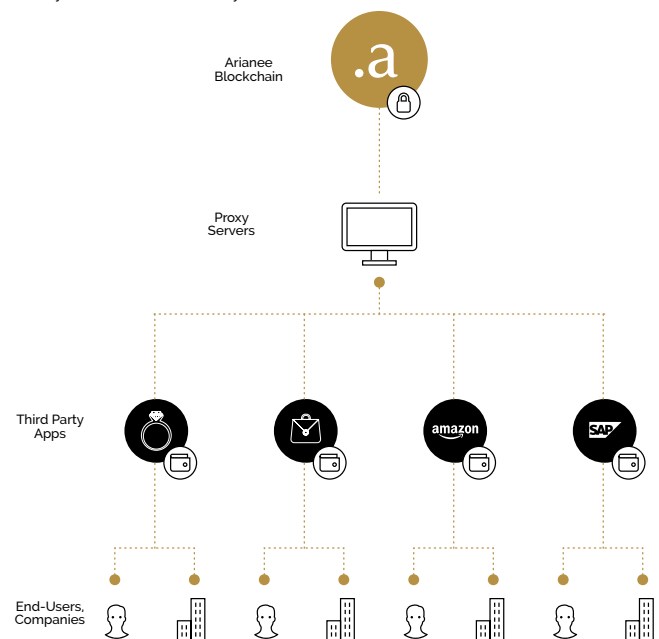
Governance

Blockchain governance is a consequential factor that can determine whether or not a blockchain is beneficial to the public interest. Governance is a process. It involves players who participate in that process to produce decisions that affect the governed resources. These decisions can have a lasting impact on many stakeholders.

One of the core value propositions of Ethereum and Bitcoin is that they are "unstoppable" by governments and regulators. This has played a key role in the growth

Stakeholder incentives and Governance

of the crypto world in recent years. To achieve this goal, the concept of a fully-decentralized network is necessary, which leads to a high level of complexity and risk in terms of governance. This being said, by its nature and considering its features, Arianee does not have the same constraints.

Governance principles:

Blockchain technology is hailed as a trustless, distributed self-governance system. However, while the high degree of decentralization that permissionless projects such as Bitcoin or Ethereum provides great fairness, it also leads to serious inefficiencies. Therefore, in order to improve the efficiency of the project, Arianee wishes to incorporate some concepts of centralized governance.

Permissionless blockchain enables decentralization and therefore censorship resistance. However this decentralization comes at the cost of efficiency and can lead to the stagnation of network development when the community cannot decide on a path forward. The recent split in the bitcoin core team around the question of block size, which led to the Bitcoin Cash (BCH) fork is a perfect example of such problems. Centralized organizations on the other hand offer the clearest decision making system at the expense of decentralization and censorship resistance, which makes it unattractive for blockchain projects.

The Arianee governance aims to find an equilibrium between the interests of individual owners, brands and the third-party community. We are convinced that we can find a governance model that will sufficiently satisfy the stability and predictability that large businesses seek and the protections that individuals and the third-party community demand. While governance based on direct voting or staking is popular today, we have come to the conclusion that the DAO failure or recent controversies around DPoS show the limits of such systems. We therefore believe that a deliberative architecture will result in a more robust governance system. In light of our previous experiences in blockchain projects, we aim to strike a balance between representativity and efficiency. We believe that this balance can be reached more easily with a transparent governance led by councils, and clear and simple processes to join them.

Governance architecture:

While the Proof of Authority protocol should be seen as the machine-based consensus mechanism certifying the integrity of the blockchain, the governance architecture should be seen as the social consensus mechanism.

The Arianee governance architecture should therefore operate with the same principles of transparency and clarity which underlie our Proof of Authority protocol.

• *The Executive Board*

The Executive Board manages the resources of Arianee

structure. It is in charge of allocating ICO funds and selecting the most qualified individuals, team or organization to build and maintain the Arianee platform. The Executive Board is also in charge of managing the Arianee fund. The Arianee fund distributes grants to promising projects developed by the third-party ecosystem and to individuals or teams contributing to the development and maintenance of the Arianee platform.

The Executive Board is composed of three Arianee team representatives, three advisors and the president of the Protocol Board, who will represent the voice of Arianee stakeholders.

• *Protocol Board*

The Protocol Board defines policies and enacts decisions pertaining to the development and maintenance of the Arianee protocol. The Protocol Board's mandate is to ensure the independence of the network and should preserve the balance of power between authority nodes.

The Protocol Board is composed of the president of each Enterprise Committee, three members of the Executive Board and an elected representative of the Network Onboarding Circle.

• *Enterprise Committees*

Enterprise Committees are the voice of the businesses using the Arianee protocol. Each committee shall represent a particular business sector involved in the Arianee ecosystem. Each Enterprise Committee shall surface the needs of its particular users, both internal and external. Each committee shall elect a representative who will participate to in meetings of the Protocol Board.

• *Network Onboarding Circle*

The Network Onboarding Circle is in charge of assisting brands, Experts and independent third parties who wish to run an authority node and who have successfully gone through the verification process.

The Network Onboarding Circle is composed of Arianee's Technical lead, one Technical Advisor and three independent authority nodes. They elect a representative of the Network Onboarding Circle who will participate in the Protocol Board.

• *Verification Process*

The verification process is a Know Your Business (KYB) process through which each brand, expert, and independent authority node operator has to go. Verified companies have access to paid features and are eligible to run an authority node if they wish to. The verification process is designed by the Network Onboarding Circle and approved by the Protocol Board.

Arianee team

Τhe team is composed of entrepreneurs, investors and software engineers who have worked, co-founded and exited companies together in the past.

Emmanuelle Collet

Marketing

Emmanuelle is an experienced communication and marketing professional with over 10 years of experience. Most recently, she was in charge of the global media strategy for the Swiss watch brand Omega. She earned her MBA from Paris La Sorbonne

Julien Romanetto

Product

For 20 years Julien has been a successful entrepreneur and an investor with an eye for the technical side. With Frédéric Montagnon, he co-founded and exited Secret Media, OverBlog, Teads and Nomao for a total value of more than USD 400 million. Julien has been involved in cryptocurrencies, mining and user cases for blockchain technology for the last three years.

Alexandre Cognard

Technical

Alexandre started coding by himself in late 90s. He then graduated from ESIEA with a masters in engineering and completed his education with an MBA. A serial entrepreneur, he started building companies when he was 18 years old thanks to his powerful framework EZBO. His first company, FDM, us still leader in shareholder relationship management solution. Following two main service companies specialized in custom e-commerce, he co-founded Vestiaire Collective, and worked as CTO for eight years. Vestiaire Collective is one of the world's leaders in the second-hand luxury marketplaces with €118m funding, close to €200m business, with a presence in Paris, NYC, London, Berlin, Milan and Hong Kong.

Christian Jorge

Operations

Christian founded his first start-up Néocité, a city-guide, in 1998 during his during his study of Economics at University. He then founded a digital marketing web-agency, IDEO Concept, which merged with Alexandre Cognard's company in 2003. Before co-founding Vestiaire Collective in 2009, he took part in the creation of some e-commerce companies as operational partner. Along with his role as comex chair at Vestiaire Collective, Christian worked as CPO for four years and VP Operations for another four years. He's now a business angel, advisor and mentor in the French Tech ecosystem (Numa, Ashoka).

Arianee team

Frederic Montagnon
Chairman, Board member

An accomplished entrepreneur and investor with 20 years of experience, Frédéric has founded and exited 4 companies for a total value of more than USD 400 million. He is ranked as the 7th largest start-up investor in France, and has been involved in the field of cryptocurrency as an investor since 2013. He is a well-known blockchain influencer and his commentaries have been published multiple times.

Jean-Marc Bellaiche
Business Development

Jean-Marc was previously Senior Vice President of Strategy and Business development for Tiffany & Co. He joined Tiffany in 2014 and brings with him over 20 years of experience in the luxury sector. Previously, he was Senior Partner at the Boston Consulting Group, where he led the global Luxury, Fashion, Beauty and Department Stores practice and implemented competitive business strategies for global clients in these sectors. Jean-Marc has a degree in econometry engineering from École Centrale Paris and an MBA from the global business school INSEAD.

Luc Jodet
Business Architecture

Luc started his career as a Business Analyst in a Fortune 500 company. He then co-founded BUYECO, a Renewable Energy Marketplace in Switzerland, which sources electricity for large corporate customers. This is where he discovered blockchain technology while working on energy traceability solutions.

Gregory Pouy
Brand Evangelist

Grégory is globally recognized speaker and marketing consultant specialized in the beauty, fashion and luxury industries. He also teaches digital marketing in major European business schools such as HEC, Essec or Dauphine.

Arianee team

Julien Abriel
Product manager

Julien has 10 years of experience in complex digital products and technical team management. He honed his skills in a wide range of organization from startups (Vestiaire Collective, Better Collective, Onepark) to large corporations (Le Monde, AFPA) and public institutions (the European Parliament, Centre Pompidou). He has a passion for innovation and is a performance focused Agile methods professional.

Fabrice Ezzine
Lead back end

Passionate about the internet, Fabrice has been able to deepen this knowledge in fullstack development during his 12 years of experience with Cairn as lead developer and then in Vestiaire collective as scrum master. During these years he was able to manage development teams and teach them new ways of working and more particularly on switching to agile mode. He then became a freelance and consultant specializing in architecture and payment method

Stephen Ferron
Editor

Stephen is an award-winning copywriter. He grew up in Colorado but is now based in Switzerland, where he has created and edited texts for global clients in a number of industries. Stephen holds an MA's in Mass Communications (Leicester), and World Music Studies (Sheffield), and an MSt in Creative Writing (Cambridge).

Julien Sechaud
Lead tech Mobile

Julien started his career as a Project Manager for major telecommunication firms. His taste for design and IT made him quickly a mobile enthusiast. Startup fan and early-stage lover, he brings his expertise to mobile-centric businesses for both technological and product challenges. His first discovery of blockchain technology was through democratic autonomous organization.

Kurban Atabinen
Lead front end

Multi-Skills Developer. Years of experience in web and mobile applications development. Creator of Backside Development platform.

Arianee roadmap

2016
Idea

2017 Q3
Founding
Team

2017 Q4
AlphaNet, mobile
wallet POC / Brands
enrollment to shape
the protocol

2018 Q1
Extended
Team

2018 Q2
Roadshow to build
the community
and spark awareness
of Arianee

2018 Q3
Token Generation
Event

2018 Q4
Launch of Arianee
TestNet, brands
workshops

2019 Q1
Arianee
Protocol Beta

2019 Q2
Launch of Arianee
MainNet + Arianee
suite Beta

End 2019
Official release of
Arianee Suite V1, Arianee
Protocol, Launch of
Experts Network

2020
and beyond
Expand the
ecosystem

2021
and beyond
Nurture other
markets

Arianee structure

Origin of the name

The legend of Arianee – Ariadne in English – has had countless interpretations in the more than 2000 years since it was first recorded. And while the details of the story vary depending on the narrator, one part of it is consistent: with a thread of glittering jewels, Ariadne helped the Athenian hero Theseus escape the Labyrinth after he slew the Minotaur.

It's fitting that the heroine's name survives in the expression "Ariadne's thread", which describes finding a solution to a problem through the exhaustive application of logic to all possible options.

There could be no better name for a structure committed to helping companies and individuals negotiate the internet – a labyrinth whose challenges far exceed those faced by Theseus – than Arianee. And there could be no greater privilege than to be your thread through this maze.

Independence

Arianee sustains, maintains, and upholds the reference **protocol** for each party: the **creation and management of digital ownership** for end **users and the issuance of certificates of authenticity** for property.

Arianee technology is based on a **blockchain,** which by its nature guarantees transparency, security and **data integrity.** Unlike centralized platforms, Arianee's users, whether individuals, brands, third parties or resellers, retain **ownership of their data**. They are the only ones who control it and who can decide how it is used.

Arianee is a **company** that both serves and is governed by its users. Its structure guarantees its **independence** and its **durability.**

Arianee aims to **create an ecosystem around its protocol** by delivering a free tool, and by financially supporting those who bring new customers and innovations.

> The ancient Greek poet Ovid wrote in his epic poem Metamorphosis: «The door [of the Labyrinth], so difficult, which none of those before could find again, by Ariadne's aid was found, the thread that traced the way rewound."

•

.a