DISCLAIMER: This version of Legacy's whitepaper is now considered as deprecated, but is still publicly accessible for consultation purposes. Please note that Legacy is no longer considering a token sale.

The Legacy Project

Almonacid, Vicente
vicente@legacy.network

Michel, Nicolas
nicolas@legacy.network

November 14, 2018
v0.7.3

Abstract

Legacy is a blockchain-based application allowing people to easily distribute assets upon their death or upon any set of verifiable events. The application integrates a variety of services that will be developed progressively as blockchain technology consolidates. This paper mainly describes Legacy's initial releases, which allow the transfer of digital assets, such as images, videos and text documents. The application's core functionalities will be initially developed on the Ethereum blockchain. These include a Proof of Life engine responsible for determining whether the user is alive or not, and a smart contract that manages user assets and schedules their distribution according to a given set of triggering events. Leveraging the unique characteristics of blockchain platforms, Legacy is designed to ensure security, reliability and long-term availability. Typical use cases include transfer of sensitive data (*e.g.*, personal meaningful information), cryptocurrency holdings and confidential data such as online service credentials. In the long-term, Legacy expects to integrate smart property and other blockchain-based digital assets, as well as to provide a platform for peer-to-peer legal and technical assistance, thus becoming a next-generation smart-will solution.

Acknowledgements

The Legacy Project would not have been possible without the generous support and valuable feedback from many individuals. Directly or indirectly, they have also helped us to improve this document significantly. We would like to express our deep gratitude to (without any particular order): Laurent Hardy from Madrid's Ethereum Community, Marina Markežič from Cofoundit, Arturs Zelenkovecs, Scott Stevenson, Benoît Belin, Louis-Félix Nothias, reddit users FjorXD and rpr11; Aragon team members Jorge, Luis and tatu; Virginie Gretz, Sebastien Bourguignon, Roman Beyon from La Maison du Bitcoin and CTO of iExec Oleg Lodygensky.

Special thanks to our advisors Adrian Brink, Julien Bouteloup and Rafael Mery.

GENERAL DISCLAIMER

The White Paper shall be read together with the T&C and does not constitute an offer or an invitation to sell shares, securities or rights belonging to Legacy.

Legacy is not deemed providing any information which can be considered as a basis for an investment decision.

Legacy is not providing any investment recommendation nor investment advice.

The White Paper including the T&C does not constitute or form part of, and should not be construed as, an offer for a sale or subscription, or an invitation to buy or subscribe securities or financial instruments. It does not constitute the basis for, or should not be used as a basis for, or in connection with, a contract for the sale of securities or financial instruments or a commitment to sell securities or financial instruments of any kind.

Legacy expressly disclaims any liability for any direct or indirect loss or damage of any kind arising directly or indirectly from:

i. any reliance on the information contained in this document,

ii. any error, omission or inaccuracy in said information, or

iii. any resulting action that may be brought.

Regulatory Uncertainties of Tokens

The regulatory status of tokens and distributed ledger technology is unclear. It is difficult to predict how or whether regulatory authorities may apply existing regulation with respect to such technology and tokens platform. It is difficult to predict how or whether the regulator may implement changes to the law and regulation affecting distributed ledger technology and its applications, including the LEG Tokens and the platform. Regulatory actions could negatively impact the platform in various ways, including, for purposes of illustration only, though a determination that the purchases, sale and delivery of the LEG Tokens constitutes unlawful activity or that LEG Tokens is a regulated instrument that requires registration of the platform itself, or the licensing of some or all of the parties involved in the purchase, sale and delivery thereof. The platform may cease operations in a jurisdiction in the event where that regulatory actions, or changes to low or regulation, make it illegal to operate in such jurisdiction, or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction.

A LEG Token is not a financial instrument. A LEG Token does not represent an investment in a security or a financial instrument within the meaning of EU Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 relating to markets in financial instruments: the LEG Token confers no direct or indirect right to the Legacy's capital or income, nor does it confer any governance right within Legacy.

A LEG Token is not proof of ownership or a right of control. It does not confer any right on any asset or share in Legacy. A LEG Token does not grant any right to participate in control over Legacy's management or decision-making set-up.

A LEG Token is not an electronic currency within the meaning of EU Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 relating to access to and pursuit of the business of electronic currency institutions: LEG Tokens are not accepted outside the platform and a LEG Token does not have a fixed exchange value equal to the amount delivered at the time of its issue.

A LEG Token does not qualify as a payment service within the meaning of EU Directive (2007/64/EC) of 13 November 2007 relating to payment services in the internal market, nor within the meaning of the (EU) Directive relating to payment services 2 (DSP 2) N° 2015/2366 of the European Parliament and of the Council of 25 November 2015: the ICO does not involve the purchase/sale of LEG Token and the Legacy's business does not consist in receiving currencies against the delivery of LEG tokens; as such, a LEG Token is not a means of payment either.

A LEG Token is a cryptographic token used by the platform. A LEG Token is a crypto-currency, i.e. an unregulated, digital asset, issued and controlled by its developers, and used and accepted only by the members of a given community.

Intellectual property belonging to Legacy. The User acknowledges that Legacy retains sole and exclusive ownership of all intellectual, industrial and expertise rights relating to the LEG Tokens, documents, data, etc. The technical and technological resources and expertise used to design both LEG Tokens, and documents of any nature, shall remain the exclusive property of Legacy regardless of whether they are protected under an intellectual property clause. Therefore, any document, listing, database, etc., in its entirety, is given to the User in return for payment or free of charge solely as a loan for use that exclusively enables them to use the platform, under or not a separate availability and/or non-disclosure agreement that forms an integral part of these T&C, and may not be used by the User for any other purpose without incurring their liability

Protection of Personal Data. The processing of personal data performed under the platform will be declared in France to the National Commission for Data Protection and Liberties. In accordance with Article 32 of French law N° 78-17 of 6 January 1978 relating to Information Technology, Files and Civil Liberties, Legacy, which is responsible for processing the said data, will inform the User that it is processing their personal data. The details entered by the User on the forms available on the website are intended for authorized Legacy personnel for administrative and business management purposes. These data are processed to allow Users to access and use the services under the platform.

- The User is entitled to access, question, modify, rectify and delete their own personal data,
- the User is also entitled to object to the processing of their personal data for legitimate reasons, as well as to object to the use of such data for the purposes of prospecting activities.

To exercise their rights, the User shall notify their request to Legacy, attaching a copy of their signed ID document. . The User shall comply with the provisions of French law N° 78-17 of 6 January 1978 relating to Information Technology, Files and Civil Liberties, amended, any breach of which is deemed a criminal offence. In particular, they shall not collect or misuse data and, in general, perform any act likely to infringe the privacy or reputation of individuals

Regulatory uncertainties. The User acknowledges and accepts that the ICO launched by the Legacy is taking place within a French legal environment that is still under development. New laws or rules may subsequently frame, modify or clarify the practice of such ICO. Where necessary, should legislative changes conflict with all or part of these terms and conditions, Legacy reserves the right to amend the terms of the ICO as appropriate, retroactively if necessary, in order to ensure that the ICO remains legal and compliant with the various French regulatory bodies.

Legacy will respond to any request issued via regular legal process aimed at obtaining specific information about the Users, particularly in terms of the fight against money laundering.

Applicable law and jurisdiction. These T&C and any contract relationship relating to the services offered by Legacy are governed exclusively by French law, the Legacy's commitment being subject to this clause. Translations of the White Paper including the T&C herein, made available to the User, are purely informative and are not legally binding. The French version of these terms and conditions has sole legal force. If an English version is provided to Users, it is for information purpose only. Legacy and the Users agree to seek an amicable settlement prior to bringing any legal action. Failing this, any dispute, of any nature whatsoever, will be brought expressly before the court with jurisdiction over the Legacy's registered headquarters, as no document can affect a novation or waiver of this jurisdiction clause.

Contents

"While agreements are no longer memorialized in clay, lawyers have failed to take advantage of advances in computing to streamline and simplify their work."

Aaron Wright and David Roon

1 Executive Summary

Wills have a history that goes back to Ancient Greece. While their utility and legal implications vary through cultures and ages, their underlying mechanisms are the same. As we move into a digital economy and society, analog forms of value—both sentimental and monetary—are replaced, stored and transmitted in digital formats. Printed documents, books, pictures and even money are examples of things that are now handled digitally. In this context, distributing valuable digital assets securely after death cannot be easily achieved through the traditional system of writing a legal document (*i.e.*, a will or testament) and naming an executor. In particular, this approach usually requires the intervention of several trusted third parties (eventually, an executor, a lawyer and a public notary) and does not guarantee security, reliability nor privacy—the latter especially important with regards to transferring meaningful personal data. Furthermore, with the introduction of blockchain platforms and smart contracts and the imminent mainstream adoption of the Internet of Things (IoT), we expect to see the emergence of a novel concept of property known as *smart property*[1]. Like cryptocurrencies, smart property will require a different technological solution, as well as a novel legal framework, in order to be securely transferred according to a decedent's last will. This paper introduces Legacy[2], a blockchain-based service that aims at becoming the first *smart will*. In its first stage, Legacy allows distribution of what we refer to as *memories*; *i.e.*, digital items such as images, video recordings, manuscripts or other forms of digital data that capture valuable life experiences. The issue of securely managing digital assets of higher monetary value (such as cryptocurrency holdings) in the event of the owner's death is considered afterwards. Legacy will evolve gradually into a more decentralized, self-sustainable architecture based on a reward system. In the long term, as smart property becomes a reality and law embraces blockchain technology, Legacy aims at positioning as the *de facto* smart will solution, progressively eliminating the need for trusted third parties (including the Legacy organization) and ensuring key attributes such as security, privacy and long-term operation.

[1] By smart property we mean a type of property that can be traded and transferred through the blockchain. See also [9]

[2] Here we only discuss technical aspects of the project. Additional relevant information, such as business plan, team information and development roadmap, can be found in `https://legacy.network`.

1.1 Problem Statement

The traditional process of transferring property—whether in the form of real estate, money or ordinary valuable objects—through a will and testament involves several issues.

In general, the process depends entirely on an executor, who is in charge of administrating the legacy and is appointed by the testator. An executor must be trustworthy. Depending on the legal framework, writing a conventional will might require the intervention of additional intermediaries, such as a lawyer and a notary. In many cases, these are not legally necessary, which suggests that the process can be systematized in order to be easily self-completed by the testators.

Wills are written as ordinary documents, and can get lost or destroyed. Since they must be easily accessible by the executors when the moment arrives, wills are usually not stored securely.This compromises the content's integrity and confidentiality. As a consequence, conventional wills are inherently unreliable.

Wills are in general limited to the distribution of monetary valuable possessions and are not suitable for managing personal digital data. Nowadays, most of our important life experiences and memories are captured in emails, digital images, videos, and other digital items. These are also part of our legacy and require attention. But conventional wills are not meant for this. While some software solutions address this problem, they are based on centralized architectures that provide limited guarantees in terms of reliability and long-term operation.

A conventional will is defined and executed once. Making further modifications after it has been signed is generally not possible and requires rewriting the entire document. A will is also inherently static; it cannot be automatically adapted according to changes in future conditions or unpredictable events. In addition, the process of executing a will may take significant time. Much of the process can be accelerated and systematized by taking advantage of simple software solutions.

Finally, there is the problem of securely transferring cryptocurrencies. Currently, cryptocurrencies are stored in wallets that can be accessed through a private key or password-protected encrypted files. If an individual holding cryptocurrencies dies without having communicated his/her wallet credentials to third persons, then the entire wallet balances are irrevocably lost.

1.2 Goals

Simplifying the process of transferring digital assets in the event of the owner's death

Legacy is specially designed to be an easy-to-use application. Oriented to serve a wide public, with a focus on young parents, while also including seniors and baby boomers, its usability and accessibility properties are one of its most important aspects. Users will be able to create and configure an account in a few simple steps, without the need for setting up external services (*e.g.*, a third-party storage service).

A service that ensures security, reliability, privacy and long-term operation

Legacy's core logic will reside in the Ethereum blockchain, which guarantees its integrity and availability in the future. A large blockchain network such as Ethereum guarantees long-term operation because it does not rely on a single organization. Shutting it down would require the disabling of a large number of its nodes. A blockchain also allows to securely transfer digital assets without the need for intermediaries. Users' data will be stored using a distributed file system, ensuring privacy

and reliability. A design approach oriented toward decentralization and self-sustainability is also essential to further meet these properties.

Reducing the need for trusted third parties for creating and executing a will

The need for trusted third parties for transferring property usually has more to do with legal issues rather than with technical aspects. From a technical standpoint, advanced algorithms combined with smart contracts allows to simplify the process. In some cases, however, creating a will may be a complex process (*e.g.*, for people holding a large variety of assets), and some legal assistance is necessary. We propose a solution to this problem based on a decentralized platform, in which lawyers and accountants may offer assistance.

An enhanced, smart will allowing to transfer cryptocurrency and smart property

Our ultimate goal is to integrate a wide variety of transferable items, including cryptocurrencies and other virtual assets, as well as smart property. This is Legacy's long-term vision and represents the main problems that we aim to tackle. This goal, however, involves a number of technical challenges and legal issues that need to be overcome and will be discussed in more detail later on.

1.3 Overview of Legacy and Use Cases

Initially, Legacy will allow a secure transfer of any form of digital data, such as pictures, videos, audio files and text documents. Files will be stored using a decentralized, encrypted system. Each individual file belonging to a given user represents a *memory*. Memories can be bundled into *capsules* that a user may schedule for transfer to one or more recipients upon death and/or upon a specific set of verifiable events[3]. This way, a capsule can be programmed in many different ways, forming a *smart will*. For instance, a user might want to send an email to his/her children once they turn eighteen years old or share special memories on important days of their lives such as their graduation or wedding. A user can easily specify which events and conditions trigger a capsule transfer.

An important function of the Legacy application is its ability to determine precisely and efficiently whether the user is alive or not—ideally without involving intermediaries. This is verified periodically through a mechanism called the Proof of Life (PoL) engine. The PoL engine uses different criteria in order to make a reliable decision, and its operation can be completely customized by the user. For instance, PoL can be based on social network activity patterns—which has the advantage of not requiring explicit signaling from the user—or on periodic email notifications asking the user to simply click on a link. Different PoL mechanisms can be combined in order to achieve a desired level of reliability and user experience. Once the PoL engine determines that the user has died, the capsules are scheduled for further distribution.

1.4 Upcoming Trends: Cryptocurrencies and Smart Property

With the introduction of blockchain technologies and smart contracts, as well as with the global deployment of the IoT, a new generation of smart property will rapidly become a reality. The

[3]By *verifiable events* we refer to any event or condition that can be automatically verified and signaled to the blockchain using an oracle interface and with some minimum amount of reliability.

importance of the IoT in this context is in that it will allow smart property to seamlessly interact with the blockchain. Just as the Internet extends to *things*, blockchains will integrate them as well, opening a variety of new applications. At this stage, the challenges involved in implementing smart wills allowing for the disposal of any type of property are no longer technological, but more likely legal. Trading and transferring smart property will be easily achieved leveraging the benefits provided by the blockchain. In fact, recent projects such as REAL [6] already provide a link between real estate and the crypto space, allowing to easily transfer property shares using blockchain technology.

In the long term, it is highly likely that people, as well as private and public institutions, will hold important fractions of their wealth in the form of cryptocurrencies, cryptosecurities or other types of blockchain-based assets. Indeed, a recent report by the World Economic Forum predicts that 10% of the global GDP will be stored on the blockchain within a decade [7]. Enabling the disposition of blockchain-based assets after death will become a problem of significant importance in the near future.

2

Technical and Implementation Aspects

This chapter focuses on software implementation aspects and related issues. We identify key attributes that Legacy must exhibit and describe the adopted approaches to tackle them. Overall, Legacy's underlying implementation aims at building a robust application that inspires confidence from both users and investors.

As mentionned, Legacy's core functionalities reside in the Ethereum blockchain platform [1]. This aspect is perhaps the main competitive advantage of Legacy with respect to similar solutions, and also enables additional functionalities that have not been addressed by other services.

2.1 Why Blockchain?

The essential role of a blockchain consists of removing the dependency on trusted third parties in networks where nodes are non-reliable. In this way, any pair of nodes may exchange and process data securely without the intervention of intermediaries. In this way, Bitcoin eliminated the requirement for banks as validators of money transactions. The introduction of smart contracts has paved the way for many novel blockchain applications. Basically, smart contracts not only allow to securely perform peer-to-peer money transactions, but virtually any type of operation. In addition, smart contracts can be executed programmatically and in response to real world events (*i.e.*, events outside of the blockchain). In our context, a blockchain platform supporting smart contracts also allows us to guarantee the main following properties:

- Authenticity: a will stored in the form of a smart contract fully guarantees that all its content was dictated by its original author.
- Immutability: once a smart contract has been signed and uploaded to the blockchain, it cannot be modified nor deleted by attackers.
- Reliability: most blockchains consist of a large number of nodes that jointly validate the current system state. Smart contract data and transaction records are safely stored, validated and replicated at each network node. Hence, it is very difficult for an attacker to disrupt the network or corrupt the data.

2.2 Data Storage

Using Ethereum smart contracts guarantees that the code is reliably stored and that user's dispositions, as specified in the contract, remain immutable in the long term (unless, of course, they are modified by the user). However, storing data directly on the blockchain is currently prohibitively expensive. For instance, an SSTORE operation, which stores a 256-bit word on the Ethereum blockchain, costs 20000 gas [11, Appendix G]. Storing 1 Gigabyte of data on the Ethereum blockchain would cost around 13000 ETH, or, equivalently, about 4 million USD[1]. In fact, due to the amount of overhead involved, blockchains are not designed for data storage, which is why it is disincentivized by imposing fees.

As a consequence, data storage requires a different approach. Currently, several alternatives are being discussed and investigated. Among some identified third-party providers we may mention:

- Swarm
- Usenet
- Storj
- Sia
- Filecoin

These are all based on decentralized architectures and have been considered as candidate solutions for Legacy. In particular, blockchain-based file storage provides advantages in terms of reliability, DDOS resistance and fault tolerance, among other desirable attributes.

To further improve storage reliability, more "traditional" services can be also considered, as for instance local storage (*i.e.*, using Legacy's infrastructure), Glacier by Amazon, hubiC by OVH and Drive by Google.

Another approach for data storage consists of deploying a decentralized network of nodes running the IPFS protocol [3]. Such a network would be composed by any individual or organization interested in offering storage services. In this case, the LEG token (see Section 4) can be used to reward nodes offering storage services. While this approach is essentially the same approach used by some of the blockchain-based storage services cited above, it provides the advantage of not being dependent on third parties.

2.3 Proof of Life

The set of functions by which the system determines if a user is alive is referred to as Proof of Life (PoL). The PoL engine can be implemented at different levels of the application (see for instance Figure 3.1). It is configured by the user through the web or mobile interface and, internally, is commanded by the user smart contract instance. Several different sources of data can be used for PoL purposes, among which we may mention:

- Contract activity: first, it is desirable to provide a simple PoL mechanism that does not require off-chain entities. A user can provide PoL data by simply sending an empty transaction to his/her wallet. Note that this can be achieved by a user without going through Legacy's interfaces.

[1] At the time of writing, the gas price is 21 Gwei and 1 ETH $\equiv$ 250 EUR.

- Online user activity: simple web plugins can be implemented in order to signal online user activity. To that end, each user is assigned a personal wallet (internally) that serves as an interface with his or her smart contract. In this way, when a user logs-in to a given web application, a simple, empty transaction originated by the web plugin is sent from the user wallet to the user smart contract. Plugins can be integrated in social networks (*e.g.*, Facebook and Twitter) and in Legacy's web interface as well.

- Using a mobile application: Legacy may obtain direct and indirect PoL signalling through a mobile application. For direct signalling, users can simply receive periodic notifications that can be acknowledged involving minimal interaction. Alternatively, upon users' consent, indirect PoL signalling can be obtained using a background process, able to read whatever metadata is provided by the users. First-order PoL information can be readily obtained by simply verifying that the mobile phone is active.

- Email notifications: users can signal activity by clicking on a link sent periodically from Legacy's servers. This option is less practical but may be adopted whenever the above methods are not available or provide few information.

- Official Death Registries: Some governments and other public institutions offer databases that can be freely fetched through an API.

- Human-assisted mechanisms: as an additional PoL layer, Legacy may directly contact one or more persons previously designated by the user. While this option may go against the idea of reducing the need for intermediaries, it is also a valid alternative that may be preferred by the users in some cases (for instance, the user may prefer to have third persons to validate and supervise the process, acting as the executors in the traditional system).

The different PoL signalling channels considered in Legacy's initial release are shown in Figure 3.1. Using this set of input data sources, a weighted algorithm determines the user's state (alive/dead) with a given periodicity. The main input parameters, plugins and periodicity can be fully configurable by the user, and can also be adapted dynamically (*i.e.*, after the user smart contract has been created). The options available for PoL may also vary according to users' subscription packages because using additional mechanisms also results in increased transactions between the blockchain and external services, which in turn involves additional costs.

Taking into account the mechanisms described above, a layered model of the PoL engine has been considered in Legacy's design and is shown in Table 2.1.

PoL Layer 0	Smart Contract Activity
PoL Layer 1	Notifications, Web and Mobile Plugins
PoL Layer 2	AI engine
PoL Layer 3	Official Death Registries
PoL Layer 4	Human assisted

Table 2.1 – Simplified layered model of the PoL engine.

Proof of Death vs Proof of Life

Strictly speaking, the mechanisms in PoL layers 0–2 can only prove that a user is alive. With this information, the user's state can be derived as explained above. The main advantage of this approach is that a decision can be drawn without relying on a centralised entity and without the intervention of third parties. PoL layers 3 and 4 are semantically different—they provide direct *proof of death*, though they do rely on centralised entities and third parties. We note that, while PoL layers 0–2 might be enough to implement a robust algorithm, official proofs may be required by law in some cases.

2.4 AI-aided Functionalities

AI-aided PoL

While providing a large number of options to configure the PoL engine brings flexibility and a higher degree of certainty, it also has an impact on the user experience. A simple way to address this issue is to offer a default configuration set-up with a few options. Alternatively, the use of artificial intelligence (AI) technology could greatly simplify the PoL interface, thus improving the user experience and providing an additional degree of certainty. AI-based PoL can be implemented as a default, background process, transparent to the user, exploiting the same data sources mentioned above.

AI-aided Search for Beneficiaries

Transferring digital assets from testators to beneficiaries also involves the problem of finding the right beneficiaries. Since contracts can be executed a long time after being configured and committed to the blockchain, beneficiaries may change their contact information or be deceased. AI technology can also help to mitigate this problem, for instance, by monitoring interaction between the user and his/her beneficiaries.

2.5 Security

Security is one of the key attributes that Legacy must exhibit in order to build confidence among the community. In particular, it is desirable to securely transfer digital assets without requiring the intervention of a trusted third party. While this can be easily achieved through the blockchain, this solution requires every beneficiary to maintain an account in the network (*i.e.*, a blockchain address allowing to send and receive digital assets) and consequently is not currently feasible. However, it is highly likely that blockchains will be widely adopted in the future—especially if their usage is encouraged by governments—which would greatly simplify the problem. Meanwhile, a solution involving Legacy as a trusted third party is critial. Security also means that Legacy must be robust against attacks. As mentioned, keeping essential functionalities in the blockchain already provides advantages on this issue. Measures to enforce Legacy's security include a more rigorous code development methodology and scheduling regular code audits. Code audits by independent third parties are also considered.

2.6 Privacy

Protecting user's privacy involves several issues. By definition, public blockchains like Ethereum do not offer privacy, which compromises user-related information stored. This is a problem currently undergoing active research and several solutions have already been proposed [5, 4].

In Legacy's initial releases, most user data will not be stored directly on the blockchain (see Section 2.2 above). In this way, data can be encrypted using robust algorithms without involving high complexity costs. Data integrity can be ensured by storing in the blockchain a hash of the data contained in each capsule. Legacy is also monitoring current research on zero-party privacy, which offers significant advantages. With zero-party privacy, transferring sensitive data can be achieved without requiring trusted third parties—including the Legacy organization—to have access to the actual data involved in the transactions.

2.7 Long-term Service Availability

Clearly, Legacy must provide guarantees of sustainability. In many cases, in fact, user's capsules should be transferred within a time span of at least several decades. Ensuring service operation for such large time spans is one of the most important challenges for Legacy and requires taking multiple measures.

From the point of view of the application architecture, there must be some mechanism allowing the code to evolve over time and to adapt to major technological changes. This is another reason why dependence on specific third-party services must be minimized, in particular by those who are based on centralized architectures. Instead, core functions of Legacy should be flexible and provide support for alternative solutions. In the long term, Legacy expects to be agnostic regarding its main dependencies (*i.e.* blockchain platform, storage and oracle interface). This would allow, for instance, to migrate user's smart contracts from one blockchain to another, in the event that the former shows critical signs of scalability or stability issues.

Ensuring long-term service operation also requires minimizing dependence on the Legacy organization itself. Indeed, users expect that their assets will be effectively distributed even in the event that the Legacy organization is dissolved.

The approach envisioned to resolve these issues is one of the major features of Legacy and is introduced next.

A Reward and Incentive Platform to Reinforce Long-term Service Availability

The methodology envisioned by Legacy to meet long-term sustainability requirements can be summarized in three main ideas:

- decentralization;
- community building;
- an incentive and reward system.

Decentralization, in both terms of architecture and governance, is required in order to minimize and even remove any critical dependence on the Legacy Organization. Regarding the architecture, this means that the infrastructure provided by the Legacy Organization must be fully decentralized

in the long term. To that end, all the code included in Legacy's back and front ends should be hosted in a decentralized service. In terms of governance, Legacy also considers to implement a decentralized model allowing users and members of the community to be part of all major decisions related to the application development, upgrades, etc.

Community building is essential. Without a strong, active community supporting Legacy there are few chances to build an autonomous system independent of any central entity. In particular, this community not only needs to attract regular customers, but also more advanced users and developers.

To guarantee the success of the community building process, an *incentive and reward system* is proposed. Initially, The Legacy Organization will boost community building by means of bounty programs. In this way, users can be rewarded for contributing with bug reports and providing feedback related to their overall experience using the application. Similarly, developers can be attracted by giving them access to a software development kit (SDK) allowing them to fix bugs, propose novel functionalities and integrate additional services.

A decentralized platform supporting an incentive and reward system can be easily implemented by taking advantage of the functionalities provided by the Ethereum blockchain. In fact, several decentralized Applications (dApps) are currently being built following this philosophy.

Gradually, the main role in the community building process will be transferred to The Legacy Foundation (see Section 5.1). Eventually, major software improvements and upgrades will be decided by the community, and implemented by third parties using the reward and incentive system.

3 Architecture

Legacy's architecture is composed of several entities: the blockchain platform, Legacy's own infrastructure, an oracle and other third-party services. The essential logic of the application is kept inside the blockchain: it is here where the smart contracts that manage user assets are stored and executed. Legacy's infrastructure includes the application front ends, as well as a back end to interact with the blockchain, perform heavier computation (*e.g.*, to run the AI engine) and gather additional PoL data. The oracle is required to provide an interface between the smart contracts and the outside world. Finally, third-party services can be used for data storage and also to implement plugins for PoL data gathering.

3.1 Legacy v1.0 (Memoirs)

Legacy v1.0, named *Memoirs*, will be the first stable release of the Legacy Project. This initial version enables secure distribution of memories in the form of digital data, such as pictures, videos, text documents, etc. Since blockchain technologies supporting privacy requirements are still evolving, Legacy Memoirs is based on a hybrid architecture, taking advantage of smart contracts but keeping sensible user data outside of the blockchain. In particular, encryption keys will be stored using more traditional systems. A high-level representation of Legacy Memoirs' architecture is given in Figure 3.1. Legacy's own infrastructure and front ends are shown in blue, third-party services in green and the blockchain in red.

There are two main front ends: a web and a mobile application. These are the main interfaces between the user and the core infrastructure, and provide similar functionalities so that the service can be fully accessed and configured from either. The web and mobile applications are also employed by the system to obtain PoL data based on user interactions with the service (see also Section 2.3).

Legacy's back end plays different roles. First, it creates smart-contract instances after a user initiates the service and commits a capsule. Second, once a user smart contract is uploaded to the blockchain, the back end sets up an oracle instances that runs periodic calls in order to execute the contract code. And third, it gathers PoL data from external web services and plugins. The user smart contract implements the PoL algorithm that determines if a user is alive or not, schedules subsequent calls from the back end and triggers the distribution of capsules once the PoL engine

determines that the user has died. Legacy's Memories will implement PoL layers 0 and 1 described in Section 2.3. Memories and capsules will be initially stored using a decentralized, encrypted, blockchain-based, third-party service, which will be backed up using traditional infrastructure. To allow our smart contracts to query the outside world (for instance, for PoL signalling), an Oracle interface is required. Legacy Memoirs will employ an Ethereum-compatible oracle (such us Oraclize[1]).

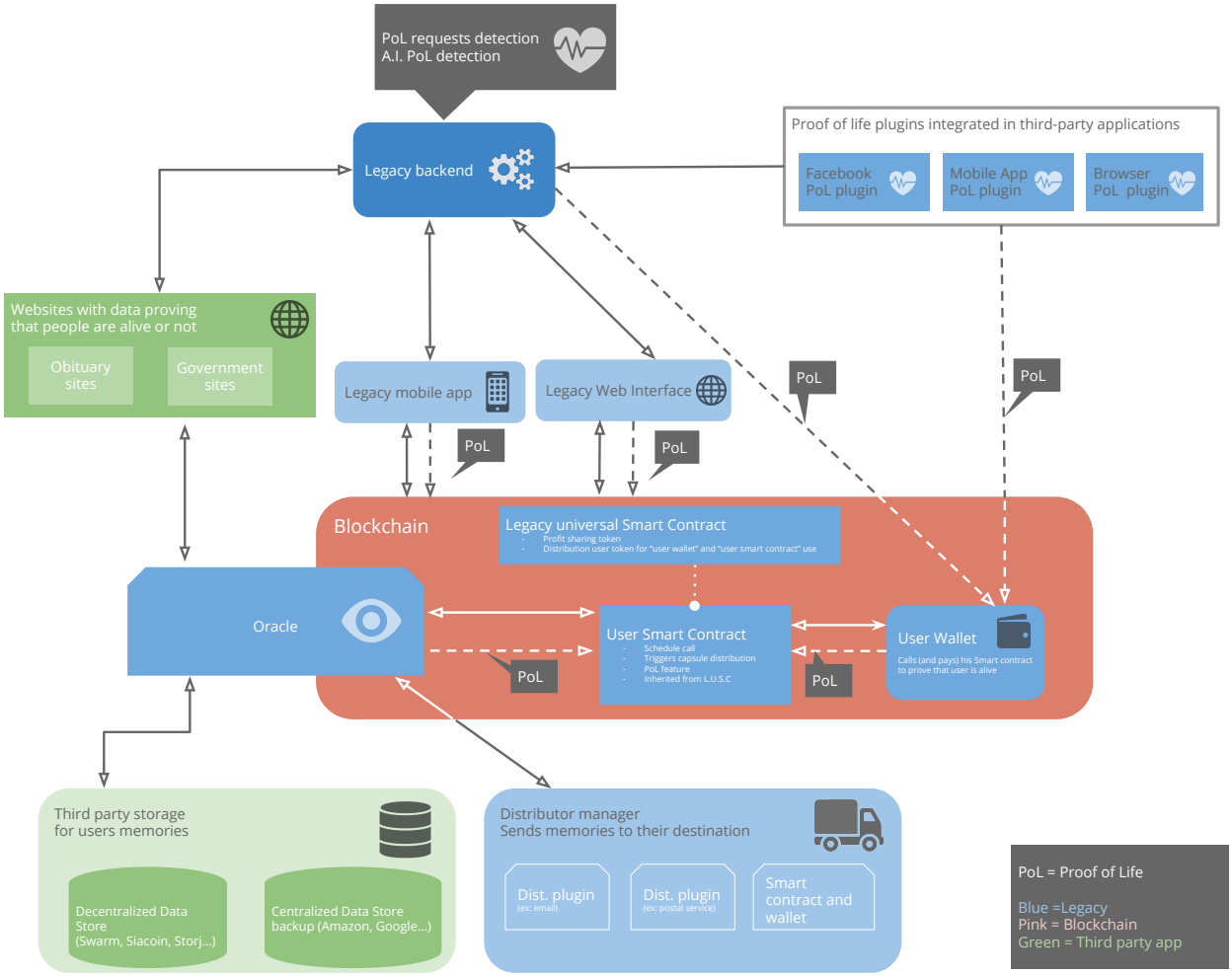

Figure 3.1 – Legacy Memoirs architecture.

3.2 Legacy v2.0 (Heritage)

Legacy v2.0 *Heritage* will be Legacy's second stable release. One of the key aspects in this version is related to privacy. Heritage will implement blockchain privacy features currently under research and development status (see for instance [4]). The main idea is to minimize trust on Legacy's infrastructure and therefore to store secrets (*e.g.*, users' private keys) securely over the blockchain. Heritage will also offer the possibility to create legally-bound wills using smart contracts. In order to facilitate the process of creating valid, legal wills, Heritage also integrates a set of software tools allowing automation of the process, in line with novel advances such as the OpenLaw protocol proposed by

[1] http://www.oraclize.it/

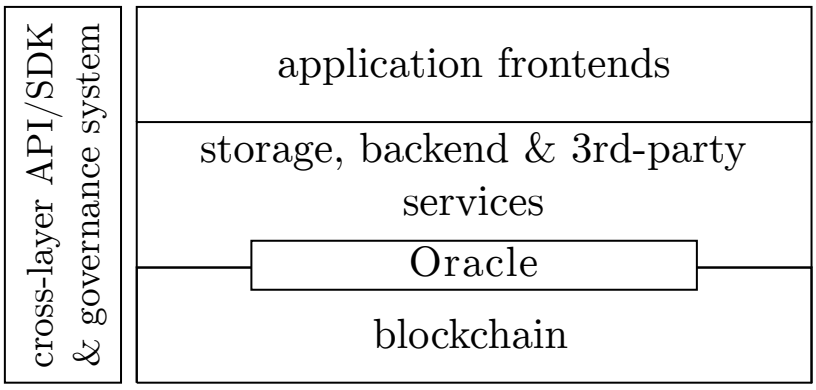

Figure 3.2 – Legacy's platform model

Consensys [2]. A major improvement in Legacy's Heritage is the capability to transfer smart property, cryptocurrencies and other blockchain-based assets (though this feature will be subject to the dispositions given by each jurisdiction). Advancements in blockchain oracle design will also be taken into account in order to further improve and decentralize Legacy's architecture. Depending on the level of funding available, we expect to implement a first release of Legacy's AI engine, as well as PoL layers 3 and 4.

3.3 Legacy v3.0 (Future): A Decentralized, Autonomous Platform

Legacy v3.0 *Future* will pave the way for guaranteeing a long-lasting service capable of evolving over time. Legacy's Future will notably implement the reward and incentive system described in Section 2.7. A simplified platform model is shown in Figure 3.2, where in addition to the basic elements included in previous releases, a cross-layer API/SDK module as well as a decentralized governance system is considered. By leveraging the capabilities provided by the platform, Legacy is expected to become blockchain-agnostic in the long term. Finally, significant enhancements in both PoL and AI engines are considered to be included.

Table 3.1 summarizes the main features included in each release.

version	**backend architecture**	**storage**	**supported assets**	**comments**
α/β	centralized	centralized	*memories*	PoL layers 0–1
v1.0	centralized	decentralized	*memories*	Oracle, PoL layers 0–1 ++
v2.0	decentralized	decentralized	*memories*, smart property, cryptocurrencies.	PoL layers 2 (AI), 3 and 4. Legally-bound SC
v3.0	decentralized, enhanced redundancy	decentralized, enhanced redundancy	*memories*, smart property, cryptocurrencies	PoL layers 2–4 ++, AI++, blockchain-agnostic.

Table 3.1 – Summary of Legacy's main releases

4
The Legacy Token

The Legacy Token, called LEG, will be created during a token sale event organized to fund the project. The token sale process will follow standard modalities established in the blockchain community. Once the token sale period is finished, no additional tokens will be generated. A maximum of 100000000 LEG can be created. Table 4.1 provides some preliminary[1] details regarding the token and its supply distribution. Additional details regarding the token sale process and how to participate in it will be provided on Legacy's official website [10].

Total Supply	100 000 000 [LEG]
Auction Model	fixed-price auction[2]
Percentage of supply available for crowdsale	60%
Percentage of supply for Legacy founders	6%
Percentage of supply for Legacy Organization	15%
Percentage of supply for advisors, partners and consultants	12%
Percentage of supply for Legacy Foundation	7%

Table 4.1 – Token sale summary.

The Legacy Token serves three main purposes:

1. It allows to create a shared economy on top of Legacy's platform. In this way, once Legacy is able to handle digital assets holding monetary value, experts and professionals such as lawyers, accountants or notaries may provide technical assistance to users managing complex holdings or in case specific legal requirements must be met according to local regulations related to property disposition through wills. In this context, the legacy token can be used to enable peer-to-peer transfer of value on the platform.

[1] The details regarding token supply distribution are subject to further changes as the exact crowdsale modality is not yet defined.

[2] To be confirmed.

2. In line with the previous idea, tokens can be used to implement a reward and incentive system to encourage continuous platform development. Users may propose novel functionalities (*e.g.*, a specific PoL plugin or a novel storage system) which can be implemented by developers in the community. Once a novel functionality is added to the platform, a fraction of the service fees are sent to its authors. This idea is further discussed in Section 2.7.

3. Finally, LEG tokens can be used by users to gain access to commercial advantages. Paying for the service directly in LEG may give access to reduced service costs and other types of commercial incentives. This is a standard strategy to spur token demand and also allows implementation of fiscal policies regarding the token economy [8].

5 Legal Considerations

[work in progress]

It is clear that Legacy may involve several legal issues, among which we may mention:

- Legally binding smart contracts according to each local jurisdiction, wherein Legacy expects to operate. The process of transferring assets through smart contracts must strictly comply with local regulations in order to be legally valid.
- Conflict resolution in cases where the smart contract alone executes unexpectedly.
- Legal disagreements in cases where testators and beneficiaries belong to different countries or jurisdictions.
- Ensuring that Legacy's smart contract is in fact the *last* will created by the testator, which otherwise would invalidate the contract in some jurisdictions.
- Taxation of estates: wills created and executed through Legacy may also be subject to taxes under certain jurisdictions. Those cases must be clearly identified in order to avoid tax evasion.

5.1 The Legacy Foundation

There are several scenarios in which software alone cannot provide fully satisfactory solutions and therefore some arbitrage mechanism is required. On the other hand, finding people to deliver assets entrusted to Legacy may prove difficult. Beneficiaries may move, change their phone numbers, email addresses, etc. In order to handle these cases, a separate, non-profit entity will be created: The Legacy Foundation. This entity will be completely autonomous and independent from the Legacy Organization.

In order to ensure correct operation, the Legacy Foundation will receive a percentage of the service operation fees, which will be automatically transferred from user smart contracts once the service is paid. In addition, a percentage of the funds obtained during the crowdsale will be also allocated to The Foundation.

In the long term, besides playing its mediator role, the Foundation will also intervene to encourage constant platform development (*e.g.*, by proposing bounty programs) and will assist in major software upgrades. At this stage, the structure as well as the policies adopted by The Foundation will be decided by the community following a decentralized governance system.

Other functions envisaged for The Foundation include: taking care of correctly transmitting user assets when automated means fail and monitoring the Legislative process of transmitting properties. Finally, the foundation may also run storage nodes to improve redundancy and service reliability.

Bibliography

[1] *A Next-Generation Smart Contract and Decentralized Application Platform.* URL: https://github.com/ethereum/wiki/wiki/White-Paper#a-next-generation-smart-contract-and-decentralized-application-platform (visited on 06/15/2017).

[2] *Introducing OpenLaw.* URL: https://media.consensys.net/introducing-openlaw-7a2ea410138b (visited on 07/25/2017).

[3] *IPFS - Content Addressed, Versioned, P2P File System.* URL: {https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf} (visited on 09/02/2017).

[4] Matt Luongo and Corbin Pon. *The Keep Network: A Privacy Layer for Public Blockchains.* Tech. rep. URL: https://keep.network/whitepaper.

[5] *Privacy on the Blockchain.* URL: https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/ (visited on 08/10/2017).

[6] *Real Estate Crowdfunding with Cryptocurrency.* Tech. rep. URL: https://www.real.markets/static/wp/en/REAL_Whitepaper.pdf.

[7] *Realizing the Potential of Blockchain: A multistakeholder Approach to Stwardship of Blockchain and Cryptocurrencies.* URL: http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf (visited on 09/02/2017).

[8] Avtar Sehra, Phillip Smith, and Phil Gomes. *Economics of Initial Coin Offerings.* Tech. rep. 2017. URL: {http://www.allenovery.com/SiteCollectionDocuments/ICO-Article-Nivaura-20170822-0951%20%20-%20Final%20Draft.pdf} (visited on 09/02/2017).

[9] *Smart property. Bitcoin wiki.* URL: https://en.bitcoin.it/wiki/Smart_Property (visited on 10/31/2017).

[10] *The Legacy Project, official website.* URL: http://legacy.network (visited on 09/02/2017).

[11] Gavin Wood. *Ethereum: A secure decentralised generalised transaction ledger.* Tech. rep. EIP-150 REVISION. URL: http://gavwood.com/paper.pdf.