The Legacy Project

Michel, Nicolas
nicolas@legacy.network

Almonacid, Vicente
vicente@legacy.network

September 5, 2017
v0.3

Abstract

Legacy is blockchain-based application allowing people to easily distribute assets upon their death or, in general, 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 to transfer digital assets, such as images, videos and text documents. The application core functionalities will be initially developed on the Ethereum blockchain. These include a Proof of Life engine responsible of 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. Exploiting the unique characteristics of blockchain platforms, Legacy is designed in order to ensure security, reliability and long-term availability. Typical use cases include transfer of sensible data (*e.g.*, personal meaningful data), cryptocurrency holdings and confidential data such as account credentials of digital services. In the long-term, Legacy expects to integrate smart property as well as to provide a platform for peer-to-peer legal and technical assistance, thus becoming a next-generation smart-will solution.

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 possessions 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, on the one hand, and the imminent mainstream adoption of the Internet of Things (IoT), on the other, we expect to see the emergence of a novel concept of property known as *smart property*; that is, a type of property that can be traded and transferred without the need for intermediaries. 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[1], a blockchain-based service that aims at becoming the first *smart will*. At a 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 or that hold non-monetary value. On the other hand, Legacy also considers the problem of securely managing cryptocurrency holdings in the event of the owner's death. In the long term, as smart property becomes a reality and law embraces the blockchain revolution, Legacy aims at positioning as the *de facto* smart will solution, progressively eliminating the need for trusted third parties and ensuring key attributes such as security, privacy and long-term operation.

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 (*i.e.*, the person who writes the will). An executor must be trustworthy.

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

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, however, these are not legally indispensable, 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 addressing this problem exist, 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 in general 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. The OpenLaw protocol recently proposed by Consensys [4] is an interesting innovation on this subject.

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.

Goals

Simplifying the process of transferring digital possessions in the event of death

Legacy is designed to be an easy-to-use application. Since Legacy points to a wide public, including seniors and baby boomers, its usability and accessibility properties are one of its most important aspects Users should be able to create and configure an account in a few 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 require to disable a large number of its nodes. A blockchain also allows to securely transfer digital assets without the need for intermediaries. User's data will be stored using a distributed file system, ensuring privacy and reliability. A design approach oriented towards decentralization 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 allow to simplify the process. In some cases, however, creating a will may be a complex process (for instance, for people holding a large variety of assets), and some legal assistance is necessary. We propose a solution to this problem based on 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 the long-term vision of the Legacy project 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—as we discuss in more detail later on.

Overview of Legacy and Use Cases

In the short to mid terms, Legacy plans to deliver two main releases: Legacy v1.0 *Memoirs* and Legacy v2.0 *Heritage*—the main differences between both being in the underlying software architecture. Further releases including enhanced capabilities—such as the ability to manage smart property—are also considered over the medium and long terms, as technological and legal issues are overcome. This document focuses mainly on Legacy versions *Memoirs* and *Heritage*, which we may refer indistinctly to as Legacy in the following.

Initially, Legacy will allow to securely transfer 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[2]. 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 with them special memories for important days of their lives such as graduation or marriage. A user can easily specify which are the events and conditions that trigger a capsule transfer.

An important function of the Legacy application is to determine precisely and timely whether the user is alive or not—ideally without involving interaction with family members. This is verified periodically through a mechanism called Proof of Life (PoL). 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.

Cryptocurrencies and Smart Property: The Legacy Vision

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 importance of the IoT in this context is in that it will allow smart property to seamlessly interact with the blockchain. In the same way as the Internet extended 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 to dispose any type of property are no longer technological, but mostly legal. Trading and transferring smart property will be easily achieved leveraging the benefits provided by the blockchain.

In the long term, it is highly likely that people as well as private and public institutions will hold important fractions of their assets in the form of cryptocurrencies. 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 disposition of blockchain-based assets after death will become a problem of significant importance in the near future. Legacy expects to

[2]By *verifiable* event we refer to any event or condition that can be automatically verified and signaled to the blockchain (for instance, using an Oracle) with some minimum amount of reliability

2 Implementation

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.

Why Blockchain?

The essential role of a blockchain consists on 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 allows to fully guarantee that all its content was actually 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 consists 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.

Technical Aspects

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 himself). 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 [3, Appendix G]. Hence, 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 by the Legacy team. 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 partiular, blockchain-based file storage provides high reliability, DDOS resistance, 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 (Centralized). Combining proven and experimental storage methods will allow Legacy to be confident in its longevity promise.

Another approach for data storage consists on deploying a decentralized network of nodes running the IPFS protocol [5]. Such a network would be composed by any individual or organization interested in offering storage services. The LEG token (see Section 4) can be used for paying storage fees. 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 based on a third parties.

Proof of Life

The set of functions by which Legacy determines if a user has died is referred to as Proof of Life (PoL). The PoL engine is implemented at different parts of the application. It is configured by the user through the web interface and, internally, it is commanded by the user smart contract instance. Several different sources of data can be used for PoL purposes, among which we may mention:

- Online user activity: simple plugins can be implemented in order to directly signal online user activity. To that end, each user is assigned a personal wallet that serves as interface with the user smart contract. In this way, when a user logs-in in a given web app, a simple empty transaction can be generated through a web app plugin to the user smart contract. Plugins can be integrated in social networks (e.g. Facebook and Twitter) and on the Legacy web interface as well.

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

- A dedicated mobile app: Legacy may receive direct signalling using a mobile app in which users can simply press a button or answer some personal question.
- Email notifications: users can signal activity by clicking on a link sent periodically from Legacy's servers.
- Official data: Some governments offer official obituary databases that can be freely consulted through an API.
- Human-assisted mechanisms: as an additional PoL layer, Legacy may directly contact one or more persons previously designated by the user. This mechanism is referred to as "Layer-3 PoL" in the simplified diagram shown in Figure A.1. While this may go against the spirit of Legacy in that it involves intermediaries, it is also a valid alternative that may be required in some cases (for instance, users may require to have third persons to validate and supervise the whole process).

The different PoL signalling channels are shown in Figure 3.1. Using this set of input data sources, a weighted algorithm determines the user state (alive/dead) with a given periodicity. The main input parameters, plugins and periodicity are fully configurable by the user, and can be adapted on-the-fly. The options available for PoL also vary according to the user's subscription package because using additional mechanisms also results in increased transactions between the blockchain and external services, which in turn involves additional costs.

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 has an impact on the user experience. A simple way to tackle this problem 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 provide an additional degree of certainty. AI-based PoL can be implemented as a first, default layer, transparent to the user, exploiting the same data sources mentioned above.

AI-aided Search for Beneficiaries

Transferring digital assets from testators to beneficiaries involves also 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 they contact information or even die. AI technology can also help to mitigate this problem, for instance, by monitoring interaction between the user and his/her beneficiaries.

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 hold an account in the network (*i.e.*, a blockchain address to receive the assets) and hence it is not currently feasible. However, it is highly likely that blockchains will be massively adopted by individuals in the future—specially if its usage is encouraged by governments—which would greatly simplify the problem. In the meanwhile, a solution involving Legacy as a trusted third party is unavoidable. Security also means that Legacy must be robust against attacks. Measures to enforce Legacy's security include a more rigorous code development methodology and including regular code audits. Code audits by independent third parties are also considered.

Privacy

Protecting user's privacy involves some issues. By definition, public blockchains like Ethereum do not offer privacy, which compromises user-related information stored. This is a problem of active research and several solutions have been already proposed [6]. Most of user's data however will not be stored directly on Ethereum and will be encrypted. Legacy is also monitoring current research on zero-party privacy, which offers significant advantages. With zero-party privacy, transferring sensible data would achieved without involving trusted third parties (including the Legacy organization).

Long-term Service Availability

Clearly, Legacy must provide guarantees of sustainability in time. In many cases, in fact, user's capsules are 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 of Legacy and requires taking multiple measures.

From the point of view of the application architecture, the code must be able to evolve in time and be easily adaptable according to major technological changes. This is another reason why dependence on specific third-party services must be minimized, in particular on 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 eventuality that the former shows critical signs of scalability or stability issues. A blockchain-agnostic model also offers the possibility of setting up capsules into two parallel blockchains, if this option appears to be economically viable.

Ensuring long-term service operation also requires to minimize the dependence on the Legacy organization itself. Indeed, users expect that their assets will be effectively distributed even in the eventuality that the Legacy organization is dissolved. This will be one of the fundamental roles of the Legacy Foundation. Among the measures foreseen in this case, Legacy is committed to publish an open source application allowing users to keep paying operational costs (*i.e.*, fees required for blockchain transactions and storage) in order to ensure continuous operation. The Legacy foundation will be in charge of maintaining the code and guaranteeing its functionality.

3 Architecture

Legacy's architecture is composed by several entities: the blockchain platform, Legacy's own infrastructure, an Oracle—which serves as interface between the smart contracts and the outside world—and other third-party services. In an ideal scenario, third-party services would only be required for providing input data to the PoL engine, whereas most of the application logic would reside in the Blockchain. However, given the current state of maturity of blockchain technologies and related services, some functionalities must be initially implemented using a custom backend as well as third-party infrastructure. As a consequence, Legacy's architecture is expected to evolve in time, starting from a hybrid architecture and converging towards a fully decentralized architecture.

Legacy v1.0 (Memoirs): A Hybrid Architecture

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 sensitive data on more traditional technologies. A high-level representation of Legacy Memoirs' architecture is given in Figure 3.1. Legacy's own infrastructure and frontends are shown in blue, third-party services in green and the blockchain in red. There are two main frontends: a web application, which is the main interface between the user and the core infrastructure, and a mobile application, which has more limited capabilities and is mainly used for providing user PoL data (see Section 2.2.2). Legacy's backend 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 backend is in charge of running periodic calls in order to execute the code. And third, it also gathers PoL data from external web services and plugins. The user smart contract implements the PoL algorithm that determines if a user is still alive or not, schedules subsequent calls from the backend and triggers the distribution of capsules once the PoL engine determines that the user has died. Memories and capsules will be initially stored using third-party services. Further details are given in Section 2.2.1. To allow our smart contracts to query the outside world (for instance, for PoL signalling), an Oracle interface is required. Legacy Memoirs will employ a third-party, Ethereum-compatible Oracle (such us Oraclize[1]).

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

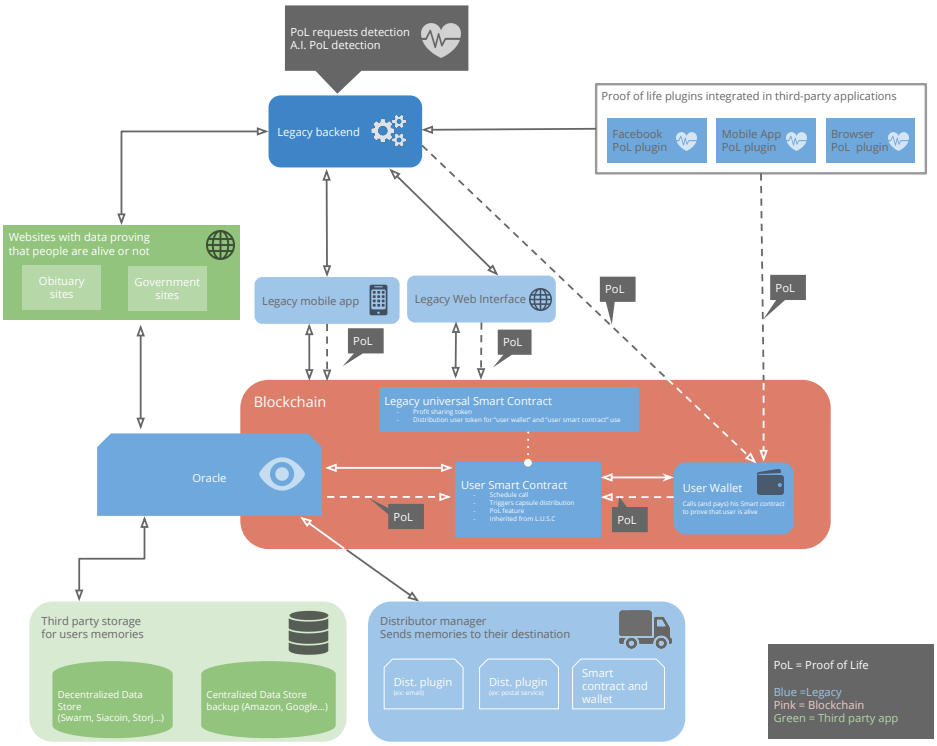

Figure 3.1 – Legacy Mémoires architecture.

Legacy v2.0 (Heritage): Towards a Fully Decentralized Architecture

Legacy v2.0 Heritage will be Legacy's second stable release. It main differences with respect to Legacy Memoirs are in the underlying architecture. This version intends to take maximum advantage of blockchain features offering, in particular, on-chain storage services and improved privacy. Release of this version is estimated for 2020, though it is subject to the technological advances in the blockchain ecosystem.

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 100.000.000 LEG can be created. Table 4.1 provides some details regarding the token and its supply distribution. Additional details regarding the token sale process and how to participate in it will be provided in Legacy's official website [8].

Total Supply	100 000 000 [LEG]
Auction Model	Ascending-price auction
Percentage of supply available for investors	75%
Percentage of supply for Legacy founders	6%
Percentage of supply for Legacy Organization	15%
Percentage of supply for advisors, partners and consultants	4%

Table 4.1 – Token sale summary.

The Legacy token serves several different purposes.

First, they allow to create a shared economy on top of Legacy's platform. In this way, once Legacy is ready to handle a large variety of assets, experts (*e.g.*, lawyers, accountants) in the community may provide technical assistance to users with 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 payments in the platform.

Second, the tokens can be used to encourage constant development of the platform. Users may propose novel functionalities (for instant, a specific PoL plug in) which can be implemented by developers in the community. To further encourage platform development, a special reserve of tokens can be exclusively use for this purpose.

Third, LEG tokens can be used by users to gain access to commercial advantages. Paying for the service directly in LEG gives access to reduced service costs and other type of commercial incentives. This is a standard strategy to encourage token demand and can also allows to implement fiscal policies regarding the token economics [2].

Finally, LEGs allow for profit sharing. As a means for encouraging participation in the token sale, future token holders may benefit from Legacy's profits by depositing LEGs in a custom wallet or contract.

A simplified diagram showing how the token is employed in the application, including the profit sharing mechanism, is presented in Appendix B (note that this diagram does not include the use of the token for peer-to-peer transactions, which is a feature considered for future releases).

5 Legal Considerations

[WIP]

It is clear that Legacy may involve several legal implications that go beyond the team expertise—at least in its current form. Some legal issues identified so far include:

- *[list possible issues]*

The Legacy Foundation

Even when all technical aspects are working perfectly, finding people to deliver memories entrusted to Legacy may be difficult. Recipients may move, change their phone numbers, their email addresses, etc. These edge cases can be handled by a separate, non-profit foundation. The foundation will take care of correctly transmitting user's assets if and only if purely automated means fail. The second mission of the foundation will be to advocate for change in the legislative process of transmitting properties. In addition, the foundation may also run storage nodes to improve service reliability.

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's smart contracts once the service is paid.

A
Flow Chart

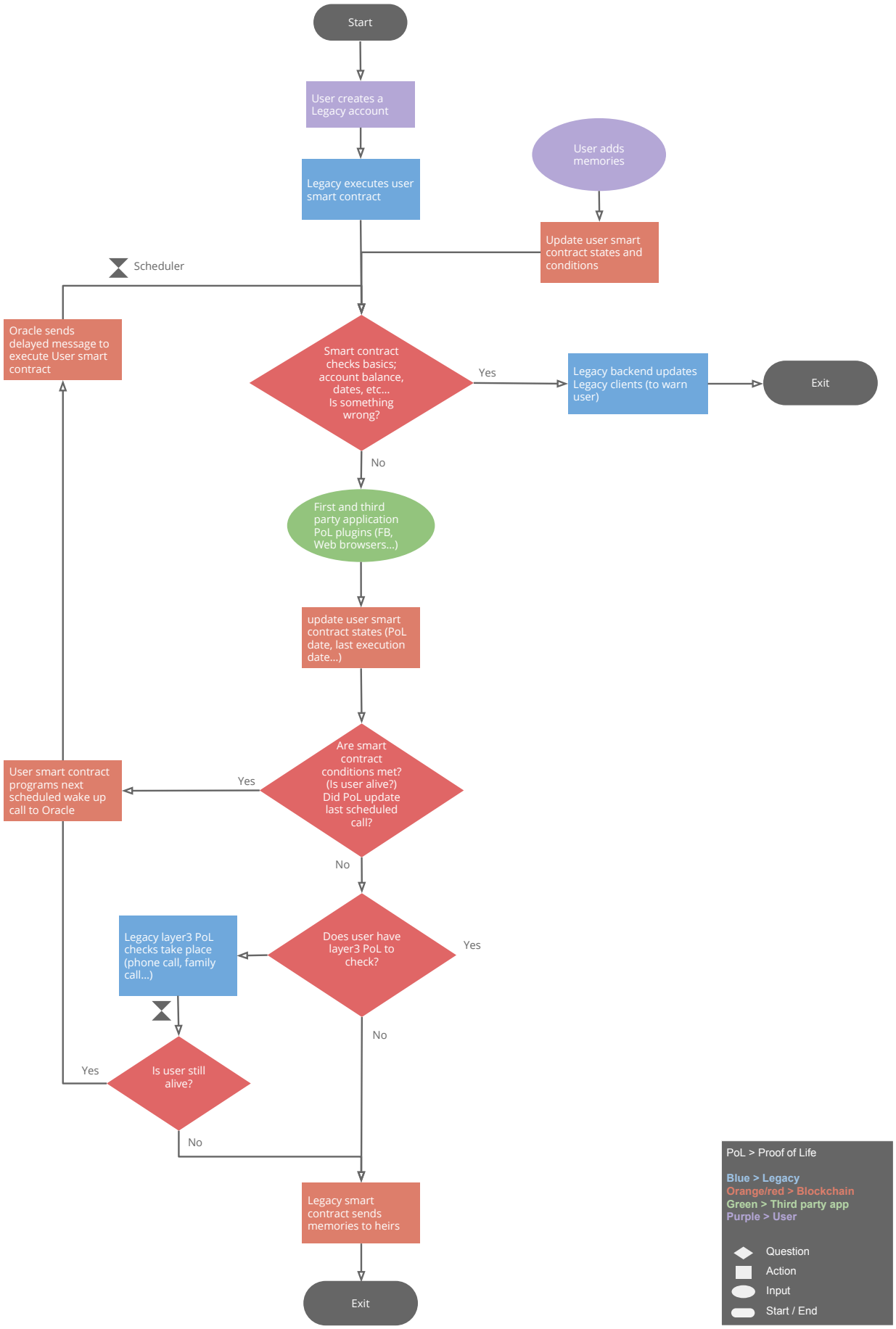

Figure A.1 – Application flow chart.

B

Economic Flow Model

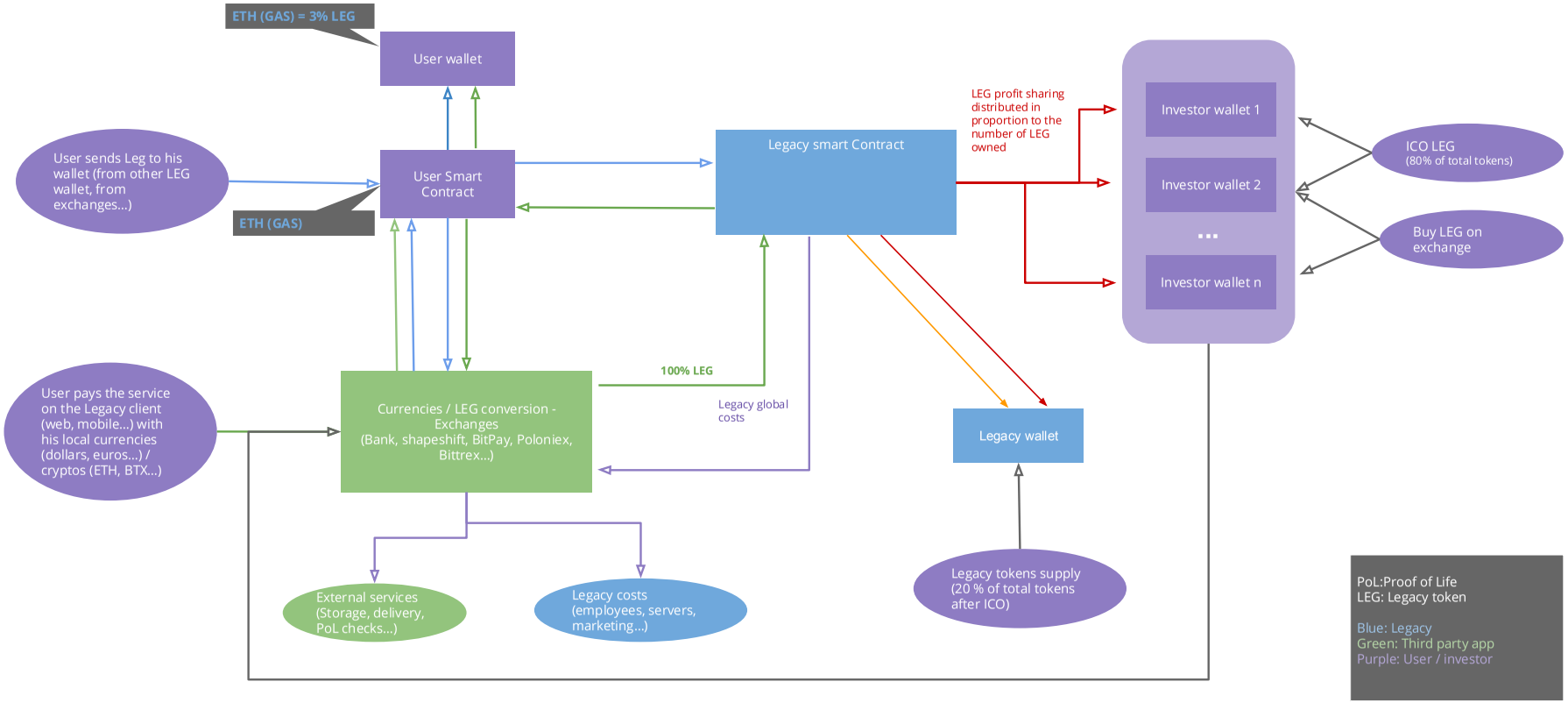

Figure B.1 – Legacy's economic flow model.

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] *Economics of Initial Coin Offerings.* 2017. URL: http://www.allenovery.com/SiteCollectionDocuments/ICO-Article-Nivaura-20170822-0951%20%20-%20Final%20Draft.pdf (visited on 09/02/2017).

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

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

[5] *IPFS - Content Addressed, Versioned, P2P File System.* URL: {https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a ipfs.draft3.pdf} (visited on 09/02/2017).

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

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