2

Wallets and Smart Contracts

This chapter is focused on the specification and development of the i3M-Wallet, Auditable Accounting, Conflict Resolution, Explicit Consent, and Smart Contract Manager subsystems.

All the subsystem development is already public in the i3-MARKET GitHub and Gitlab repositories. For detailed information on every subsystem, one can jump to their specific sections in this book or check the documentation in the public repositories, which is constantly updated.

Table 2.1 summarizes the main technical contributions of the different building blocks addressed in this book: the i3M-Wallet, the Auditable Accounting, and the Smart Contract Manager.

2.1 i3-MARKET Wallet

There is a considerable amount of wallet applications. Some popular examples are MetaMask [6], TrustWallet [7], Exodus [8], or Electrum [9]. These applications use a dedicated app for iOS and Android, and browser extensions for desktop computers. Most of them are cryptocurrency wallets and are therefore targeted to operate with crypto tokens/currencies, showing balances, and allowing token transactions and swapping. However, there are not so many solutions facing the secure storage of W3C Verifiable Credentials and the selective disclosure of claims. Among them, the most common is to build the Wallet upon an SSI solution based on Sovrin [10] [11] or directly Hyperledger Aries [12] [13]. Fewer options have been found that use the Ethereum DLT, namely uPort [14], which has been discontinued, and Twala [15].

In i3-MARKET, the Wallet App has inherited some strong requirements:

- The technology must be open-source.
- It must work from the very beginning with Ethereum-like DLTs, as it is the case of Hyperledger BESU, the chosen DLT for i3-MARKET.

Table 2.1 Main technical contributions.

Building block	Main technical contributions
i3M-Wallet	High-level functionalities supporting the main i3-MARKET flows: • Authentication/authorization • Non-repudiation Protocol • Explicit Data-Owner Consent • Smart Contract Manager Complete SSI (DIDs, VCs, and selective disclosure) Wallet running on Ethereum-like DLTs with a complete open-source codebase and not locked in by any vendor infrastructure. Designed to also support other DLTs. Innovative, more secure, and privacy-preserving interface with the Wallet application, including a secure pairing protocol that does not require any external infrastructure. Designed to be able to integrate any crypto key wallet, including hardware wallets.[1] Nowadays, IDEMIA's hardware wallet is already integrated. Secure cloud vault allowing to completely operate (restore) the Wallet from any device without loss of context data.1
Auditable Accounting	Data is registered in a distributed high-availability database distributed storage. Use of a reliable, fast, scalable solution based on the use of DLTs and Merkle trees to reliably notarize the registered data.
Conflict Resolution/Non-repudiation Protocol	i3-MARKET is enforcing a fair cryptographically verifiable billing system with any kind of money, including fiat money. Reliable non-repudiable and cryptographically verifiable log of every data exchange. The logs are designed to not leak any sensitive data but to provide non-repudiable proof of a digital data exchange under the specification of a given data sharing agreement. These proofs can be used to support fair unfakeable billing with fiat or crypto money and also to support claims for eventual conflicts in the data exchange. In many cases, i3-MARKET Backplane can automatically solve conflicts based on these proofs.
Explicit Data-Owner Consent	i3-MARKET is, to the best of our knowledge, the only technology that enforces the existence of Explicit Data-Owner Consents when a provider is selling data. Data owners can at any time revoke the consent and their data will not be distributed any longer.

Table 2.1 *Continued.*

Building block	Main technical contributions
Smart Contract Manager	Data sharing agreements are modelled with coloured Petri nets, allowing their formal verification before they are translated to smart contracts. Smart contracts are developed using DAML, which make the development DLT agnostic and allows for translating our smart contracts to multiple DLTs, including i3-MARKET's Hyperledger BESU.

Obviously, it should be designed to be extendable for other DLTs in the future, with special focus on Hyperledger Aries.

- It must be able to integrate existing key wallets, such as IDEMIA's hardware wallet, for signing.
- It must support SSI flows, but also crypto tokens, as i3-MARKET is creating a custom one. Therefore, i3M-Wallet is going to be a hybrid wallet, supporting SSI and cryptocurrencies.
- Adoption of SSI technologies should be easy for the end-users:
    - The Wallet should be easy to backup and restore with no loss of information.
    - The end-user wallet should be universally accessible from any device (desktop computer, mobile phone, etc.).

In the beginning, as a short-term solution for implementing SSI, we adopted the uPort Wallet [14] since it was already working with Ethereum, supports the disclosure of verifiable claims, its codebase is open-source, and was mature enough and well-tested. Twala [15] and other Ethereum-based SSI solutions were in a very early stage in the beginning of i3-MARKET, with little to no support for implementing the issuance of Verifiable Credentials and the server part of a selective disclosure.

The uPort solution has now been split into two different projects, Serto [16] and Veramo [17], being just the second in the libraries for creating and managing DIDs and Verifiable Credentials without worrying about interop and vendor lock-in. Veramo is at the very core of i3M-Wallet and the identity solution of i3-MARKET.

In any case, it was clear that i3-MARKET success would need a custom Wallet App supporting at the same time:

- Ethereum-based DLTs such as Hyperledger BESU, and potentially others (currently analysing Hyperledger Aries).

- Management of digital identities and Verifiable Credentials, including selective disclosure of claims, as well as cryptocurrencies.
- Complete open-source codebase with a technological solution not locked in by any vendor infrastructure.
- Enhanced usability in the sense of being universally accessible/recoverable from any device.
- The integration of any key wallet into the App, including hardware wallets.

Besides all the above features, the current version of i3M-Walllet is innovative in terms of the following:

- The desktop application has been built with privacy and security as a main design goal. For that reason, i3M-Wallet is not a browser extension and runs as a multi-platform application that is securely paired to local applications (such as JavaScript running in a browser). Not sharing a process with the browser, as extensions do, prevents a bunch of potential "speculative execution" attacks and minimizes the exposure of the app to attacks performed by malicious websites. Moreover, running the wallet as an external application is more privacy-respecting for the end-user since the Wallet will not have any access to the data exchanged with a visited page, as it is partially the case with extensions, especially when using Firefox, which has got a more limited sandbox for extensions than Chrome.
- Even though there are complete and mature implementations of the selective disclosure of verifiable claims running on Hyperledger Aries and Sovrin, the solutions using Ethereum-like DLTs do not currently implement a complete selective disclosure flow. The closest solution was the popular but now abandoned uPort [14], which implemented a selective disclosure where users could agree or not to disclose a set of claims, but not to deal individually with each of them. The Serto [16] solution (derived from uPort) is aimed at providing that, but it is still not available for public testing. Twala [15] is more dedicated to digital signatures, with a somehow limited selective disclosure of identities' claims that, in any case, relies on the Twala ecosystem and closed infrastructure. The selective disclosure flows of i3-MARKET identity system, including the i3M-Wallet, is to the best of our knowledge the first complete selective disclosure flow on Ethereum-like DLTs that is completely open-source and not locked in by any vendor.

- The Wallet integrates a secure backup system (currently in testing phase) designed to not be tied to any vendor infrastructure. The backup is complete not only in terms of restoring cryptographic material but also to restore high-level i3-MARKET data, including identities, Verifiable Credentials, and non-repudiation proofs of data exchanges.

2.2 Auditable Accounting

Marketplaces need to record, audit, and provide availability and non-repudiation for data involved in exchanges. The auditing tasks in these systems are typically performed by a trusted third-party auditor (TTPA) who is responsible for checking the integrity of the content and thus for increasing stakeholders' trust in data exchanges. It is a centralized model where all the power and responsibility fall on the TTPA, which is a single point of failure and cannot be disputed by users. Decentralized architectures and protocols appear as an alternative to avoid those risks while providing the same quality of service (QoS).

The challenges of designing a feasible storage auditing framework emanate from the security challenges of decentralized solutions and the performance overhead due to on-chain operations. In this context, the work in [18] presents a solution based on a Merkle hash tree for Auditable Accounting. Their approach is similar to ours and the project is also open-source. However, the implementation is made for the Bitcoin network while our project uses an Ethereum-based network built with the Hyperledger BESU client. In other works, polynomial commitment schemes are used to create succinct proofs of data possession and guarantee data availability [19] [20] [21] [22]. However, i3-MARKET's Auditable Accounting system is faster and more scalable but with less complexity than the mentioned alternatives. This is made possible thanks to the following:

- the usage of Merkle trees for aggregating notarization proofs of the data to register;
- the use of a smart contract for storing just the roots of those Merkle trees on the blockchain, which allows for reliable verification while heavily reducing the needs of storage in the blockchain.

The storage of the registered data with their corresponding Merkle proofs (needed for verifying against the Merkle roots) is available and ready to use as a fully distributed database provided in the i3-MARKET ecosystem.

2.3 Conflict Resolution/Non-Repudiation Protocol

One of the main issues with digital data trading is related to the legal support if either the consumer or the provider does not adhere to the signed agreement. If not under the umbrella of a big player that assumes the risks, this situation diminishes the confidence in the data exchange and prevents the ignition of an ecosystem of digital data trading.

i3-MARKET provides a technology that relies on the use of a blockchain/DLT to build confidence in digital data trading. Contrarily to other approaches that also use a DLT for that purpose [23] [24] [25], i3-MARKET does not want to force its stakeholders to use specific crypto currencies/tokens (although it provides one if desired), which can be used to automatize payments when certain conditions are met; *i3-MARKET wants to build confidence on data exchanges with any payment system*, including the most common one: fiat money. As a result, i3-MARKET is, to the best of our knowledge, the first technology that uses a DLT just as a reliable ledger of the data exchange with the goal of supporting a *fair billing system* (also with fiat money) and to be able to *solve eventual disputes*.

The i3-MARKET innovative approach generates proofs of every data exchange that can be later used to prove what was exchanged, when it was exchanged, and under which data sharing agreement. i3-MARKET does not define per-se a payment system (although it provides a crypto token if desired) but generates cryptographically verifiable and reliable data that can be used to properly invoice, and to support eventual future disputes, since both the consumer and the provider, and any third party they allowed as well, can verify them.

Besides those disputes based on subjective opinions (for instance, a consumer not liking the acquired dataset), i3-MARKET can automatically solve disputes and even enforce penalties if it were part of the agreement.

2.4 Explicit Consent

i3-MARKET's architecture has been designed to allow all the stakeholders – namely providers, consumers, data owners, and marketplace operators – to meet the strictest policies in terms of privacy and data protection, which in fact leads to meet the GDPR requirements with little effort.

Article 4 of the GDPR [26] defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. Data controllers shall be able to demonstrate that they hold the Explicit Consent of the data subjects to process (Article 7) and/or trade their data. To the best of our knowledge, no technology is enforcing user consent to the point of preventing trading without it.

It is a remarkably innovative feature of the i3-MARKET project that the Explicit Consent of the data subjects is absolutely required for trading users’ data.

2.5 Smart Contract Manager

There is noticeable interest in the literature related to automating service-level agreements, specifically data sharing agreements, by leveraging a distributed ledger technology (DLT), such as the blockchain. DLTs, and in particular smart contracts, help provide potential decentralized markets that furnish a peer-to-peer interaction between the different parties without third-party interference. Hence, this contributes to empowering the shared economy applications.

A framework that enforces the parameters of the legal data-sharing agreements with the use of smart contracts is proposed in [23]. As they describe, these parameters are automatically enforced. Moreover, they have a voting-based system. This voting system is external and acts as Conflict Resolution in case of any breaches to the agreement terms. However, these smart contracts are written in Solidity, which need to be formally verified and prove that they are error prone.

The authors of [24] present an approach based on blockchain and smart contracts to enable dynamic payments during the entire SLA lifetime (compensation value). A smart contract is implemented to detect and record any violations on the blockchain. Once the violation is detected via the “monitoring”-smart contract, the compensation value will automatically be transferred to the customer. In their work, they also use Solidity contracts.

Ocean Protocol, presented in [25], has proposed a new approach called service execution agreement (SEA), which brings the idea of SLAs to the blockchain. An SEA represents the service-level specification of an SLA, which can be translated into a smart contract. SEAs are implemented as smart contracts running on the blockchain. They have a modular design consisting of three parts: service identifier, conditions and fulfilment, and reward logic. Nevertheless, Ocean Protocol uses Solidity smart contracts running on Ethereum. Moreover, Ocean Protocol has integrated a reward logic into SEA components to reward a network of verifiers for their work. According to Ocean Protocol, the role of verifiers is to maintain data integrity and availability. However, this would require the interference of a third party (representing the network of verifiers).

In this work, we have modelled all the possible execution paths of the data sharing agreement (service-level agreement for the data market domain) using coloured Petri nets [27], a modelling method that allows describing a variety of resource types and execution logic in a way that can be formally verified. As a result, we can formally verify the modelled agreement's behavioural properties and then, with a clear understanding of how these contractual agreements are executed, translate them to smart contracts retaining the correctness and completeness of the modelled agreement. On top of that, unlike many of the presented work that relies on Solidity and Ethereum blockchain, we use the digital asset modelling language (DAML) [28], an open-source smart contracts programming language inspired by Haskell, which helps make our approach more general and focus more on the business logic and the design of our approach. DAML allows platform-independence and can be later integrated into several DLTs, including i3-MARKET's Hyperledger BESU.