Integrating Digital Identity and Blockchain

Francesco Buccafurri[1], Gianluca Lax[1(✉)], Antonia Russo[1], and Guillaume Zunino[2]

[1] University of Reggio Calabria, Reggio Calabria, Italy
{bucca,lax,antonia.russo}@unirc.it
[2] ENSICAEN, Caen, France
guillaume.zunino@ecole.ensicaen.fr

Abstract. Blockchain is a recent technology whose importance is rapidly growing. One of its native features is pseudo-anonymity, since users are referred by (blockchain) addresses, which are hashed public keys with no link to real identities. However, when moving from the use of blockchain as simple platform for cryptocurrencies to applications in which we want to automatize trust and transparency, in general, there is not the need of anonymity. Indeed, there are situations in which secure accountability, trust and transparency should coexist (e.g., in supply-chain management) to accomplish the goal of the application to design. Blockchain may appear little suitable for these cases, due to its pseudo-anonymity feature, so that an important research problem is to understand how to overcome this drawback. In this paper, we address this problem by proposing a solution that mixes the mechanism of public digital identity with blockchain via Identity-Based-Encryption. We define the solution and show its application to a real-life case study.

Keywords: Digital identity · Blockchain · IBE

1 Introduction

Blockchain [34] is a recent technology used in many application contexts, such as financial services, industry 4.0, smart city, share trading. It was defined in [34] and allows us to replace a single centralized party managing a service with a distributed ledger of replicated, shared, and synchronized digital data spread across different servers. Data are saved in a growing list of records, called blocks, and each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. Blockchain can record transactions between two parties efficiently and in a verifiable and permanent way [27]: it is managed by a peer-to-peer network of nodes running a common protocol for validating blocks. Once saved, the data in a block cannot be modified without alteration of all previous blocks, which requires a too high power computation.

Blockchain has several features: it is completely decentralized, since there is no central authority regulating data; it guarantees irreversible transactions,

H. Panetto et al. (Eds.): OTM 2018 Conferences, LNCS 11229, pp. 568–585, 2018.
https://doi.org/10.1007/978-3-030-02610-3_32

because once a transaction is generated, there is no way to delete or modify it; it is a trustless system, since it allows the transfer of sensitive information on a non-trust network by trusting the system on the whole not the system participant; it shows a pseudo-anonymous nature, since anybody can create a blockchain address to be used for transactions and it is no way to trace back it to his/her identity if appropriate precautions are taken [33]. It is worth noting that anonymity, in the original notion of blockchain, is a fundamental feature, as blockchain is born with the cryptocurrencies in mind and, for many years, cryptocurrencies were the sole applications for blockchain.

However, in the last years, also thanks to the advent of new blockchains and smart contracts, we are witnessing the shift from the use of blockchain as simple platform for cryptocurrencies to complex applications in which we want to automatize trust and transparency, and to take advantage from the other features of blockchain. In these cases, in general, we do not need anonymity anymore. Indeed, there are situations in which accountability, trust and transparency should strictly coexist, and accountability should be implemented by allowing a secure association with real-life identities. This requirement may derive from many different needs: it might be just an opportune measure to prevent unresolvable disputes, or it could derive from compliance with the law. Observe that, an approach in which users simply auto-declare their identity by a Blockchain transaction is not enough if there is no certainly of such an identity, because a user could declare a fake identity.

For these cases, blockchain appears little suitable, especially when the domain of the involved actors is open and not confined inside a single organization, which is a prerequisite for the suitability of blockchain itself. Consider, for instance, the management of the flow of goods and services (supply chain) [25]: it involves the movement and storage of raw materials, of work-in-process inventory, and of finished goods from a point of origin to a point of consumption. Typically, a supply chain is managed by a platform, a sets of technologies and processes promoting information sharing and coordination. There exist platforms for same day e-commerce home delivery in which consumers use a smart phone to browse and shop a broad range of products aggregated from nearby retail stores. Then, customer orders are handled by nearby independent couriers for pick-up and delivery to the customer. However, the platform acts as a trusted third party, thus it has to be always online and trusted by all participants. If at least one of the two conditions does not hold, using a blockchain makes sense. In this case, it should be necessary that anybody generating a transaction can be identified, but the current version of blockchain allowing pseudo-anonymous transactions does not help us. For all the above reasons, an important research problem is to understand how to overcome the native pseudo-anonymity of blockchain in order to support identity-aware applications.

In this paper, we address this problem by proposing a solution that mixes the mechanism of public digital identity with blockchain via Identity-Based-Encryption. We found this way the most suitable and not explored (so far) approach, because it accomplishes all the aimed requirements. Identity-Based-

Encryption (IBE) gives a direct role to the notion of identity, so allowing a direct link between the pair of cryptographic keys used to sign and verify a transaction and the identity of the transaction signer. On the other hand, public digital identity allows us to give a concrete definition of the identity to be used in IBEs by solving one of the problems of the concrete solutions based on IBEs, which is the proof of identity to the party issuing private keys (i.e., the Private Keys Generator).

As public digital identity, we use the notion compliant with eIDAS [7], a recent European Union regulation on electronic identification fully effective from 2016. It establishes the principle of mutual recognition and reciprocal acceptance of interoperable electronic identification schemes among Member States, and we chose it because (1) it is expected that, in the next years, eIDAS will be used by the most of EU citizens, (2) it is based on robust cryptographic primitives so that it can be considered secure, and (3) it has full legal effect.

We observe that an attempt of direct integration of public digital identity with a blockchain-based application would not provide a good result in terms of trust. Indeed, we should require that some entity of the application (even a smart contract if we adopt a blockchain like Ethereum) should play as a Service Provider of the public digital identity system (like in [19]). This implicitly requires the trust in this node for the assessment of identity, and this does not reach the goal in a satisfactory way from the security point of view, because it requires that the service providers (internal to the application domain) are trusted third parties. In contrast, the use of IBEs requires that only Identity Providers (and this is an assumption accepted also in eIDAS) and the Private Keys Generator of IBEs are trusted parties, that are parties external to the application. Clearly, Identity Provider and Private Keys Generator might also coincide.

It is worth noting that the approach proposed in this paper has the ambition to mix state-of-the-art techniques and methodologies to meet concrete needs. As a matter of fact, this paper is developed within the project called "Id Service: Digital Identity and Service Accountability" [6] funded by the Ministry of Economic Development (MISE), whose aim is studying innovative methods and techniques for designing and developing infrastructures for the accountability of cooperative services, also based on blockchain infrastructures, and their validation in virtual environments.

The paper is structured as follow. In Sect. 2, we introduce the notion of digital identity and the related technologies. In Sect. 3, we present Identity-Based Encryption, which is used to binding a digital identity and a public key. In Sect. 4, we present the idea underlying our solution. In Sect. 5, we describe the concrete proposal aiming at associating a public digital identity with a blockchain transaction. In Sect. 6, we instantiate our proposal to a specific scenario and we provide the technical details about how our solution works. The related work is discussed in Sect. 7. Finally, in Sect. 8, we draw our conclusions.

2 Digital Identity

A digital identity is defined as information on an entity used by computer systems to represent an external agent that may be a person, organization, application, or device [5]. Another similar definition given by ISO/IEC 24760-1 reports digital identity as a set of attributes related to an entity [1]. In this section, we briefly survey the main technologies related to digital identity and describe that used in our proposal.

Open Authorization (OAuth) [10] is an open access delegation protocol used by users to provide a third party (typically a site or an application) with the ability to access their personal information registered on a site without providing them with credentials to access this site. This protocol is widely used, especially in social networks, by many big companies (examples are Facebook, Twitter, Google) to allow their users to share profile information with third parties. OAuth is designed to use the HTTPs protocol for communication and exploits the release to the third party of tokens by an authorization server, once the user approves the proxy. These tokens are used as credentials to access shared information.

OpenID is another decentralized authentication protocol promoted by the OpenID non-profit foundation. By this protocol, a site administrator is supported in managing the users' authentication procedure, because no credential for user's login has to be stored. By OpenID, user access different sites with the same digital identity and password. In this protocol, the third party that handles authentication is the OpenID identity provider, while a site compatible with OpenID is called a relying party. The protocol is distributed among the identity providers and there is no central entity that manages authentication or decides who can act as a provider or identity provider. The first version of OpenID was published in 2005 by Brad Fitzpatrick, creator of the LiveJournal community and with the name Yadis (yet another distributed identity system). In 2007, Symantec included OpenID as a supported standard. In 2008, the OpenID 2.0 release was published and carried out by several major providers (Yahoo, Google, IBM, Microsoft, VeriSign, MySpace). The third and latest version, called OpenID Connect, was released in 2014.

Windows CardSpace [16] is a Microsoft software for digital identity management released in 2007. Born with the purpose of providing an environment robust against phishing attacks, CardSpace stores digital identities and provides a graphical interface for their management. When an application or a site needs to obtain information about the user, it generates a request for that information. The request is intercepted by CardSpace, which starts a graphical interface that shows the information stored and associated with that application or site. At this point, CardSpace contacts the digital identity provider to obtain the information to be shared, which is returned as a signed XML file, to guarantee its authenticity and integrity. In 2011, Microsoft registered a development of CardSpace, due to the technological changes and feedback received from partners and users. At the same time, Microsoft has shifted interest towards the U-Prove project. U-Prove is an advanced cryptographic technology, combined with identity

solutions on existing standards, aimed to find a compromise to the eternal dilemma between identity and privacy guarantee with two important privacy-preserving features: (1) unlinkability and (2) selective disclosure of attributes.

In this paper we refer to a specific notion of digital identity, which is *public digital identity*, which means that it is recognized by law in a Country or at international level making the basis for non-repudiable accountable applications. There is a concrete instantiation of this notion in the European Union. It is based on the Regulation (EU) N. 910/2014 [7] on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), issued on 23 July 2014 and fully effective from 1 July 2016. It has the purpose of providing a normative basis at EU level for fiduciary services and providing the means of Member States' electronic identification to increase the security and effectiveness of e-business services and e-business and e-commerce transactions in the European Union. Thanks to the principle of mutual recognition and reciprocal acceptance of interoperable electronic identification schemes, eIDAS wants to simplify the use of electronic authentication against public administrations, both by companies and by citizens. Each Member State maintains it own electronic identification systems, which have to be accepted by all other member states. For example, Italy has notified to the EU Commission the institution of *SPID*, the Italian public system for the management of the digital identity of citizens and businesses [15]. Thanks to the eIDAS regulation, it is possible for Italian citizens to access the online services of other EU countries (university services, banking, public administration services, other online services) using SPID credentials, and at the same time, European citizens in possession of recognized national digital identities within the eIDAS framework will have access to the services of Italian public administrations. It is expected that in the next years, eIDAS will involve the most of EU people. This consideration, as well as the high security of this identification mechanism, suggested us to exploit eIDAs-compliant identification schemes as solution for the management of digital identity in our proposal.

3 Identity-Based Encryption

Asymmetric cryptography is based on the use of a public and private key for each user. Public keys are typically arranged by a Public Key Infrastructure, which binds public keys with the respective identities of entities (like people and organizations) through a process of registration and issuance of certificates by a certificate authority (CA). However, there are cases in which pre-distribution of keys is inconvenient or infeasible due to technical restraints: in these situation, Identity-based Encryption is a solution.

Identity-based Encryption (IBE) [9] allows any party to generate a public key from a known identity value (for example, an e-mail address). A trusted third party, called the Private Key Generator (PKG), generates the corresponding private key. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as master key). Given the master public key, any party can compute a public key corresponding to an

identity by suitably combining the master public key with the identity value. To obtain a corresponding private key, the party authorized to use the identity ID contacts the PKG, which uses the master private key to generate the private key for the identity ID. The operations carried out in an IBE scheme are summarized in Fig. 1.

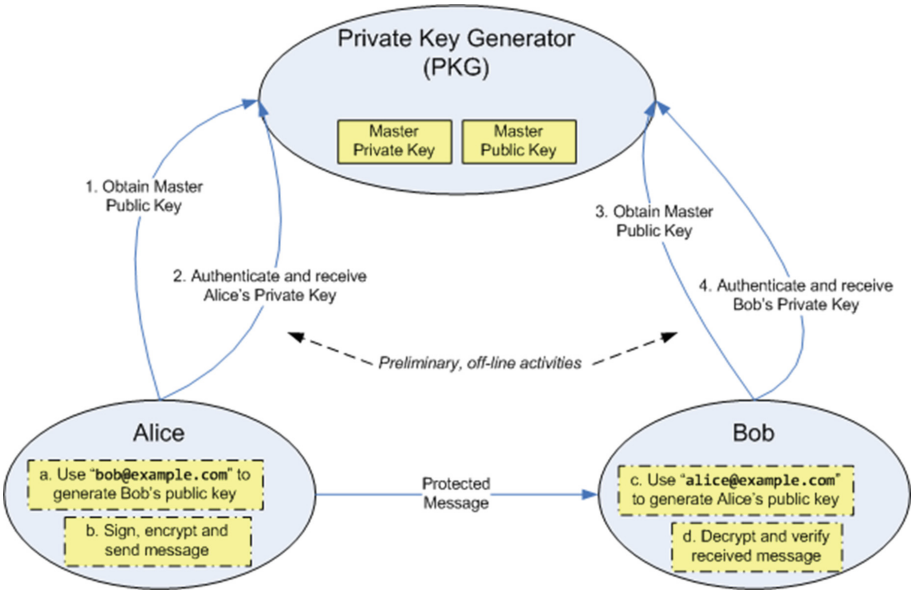

Fig. 1. Operations carried out in an IBE scheme.

As a result, parties may encrypt messages (or verify signatures) with no prior distribution of keys between individual participants, once their identity is known and well-defined. However, to decrypt or sign messages, the authorized user must obtain the appropriate private key from the PKG, by proving the possession of the proper identity. The most used IBE systems have been proposed by Boneh-Franklin [22] and by Sakai-Kasahara [36].

4 The Ideal Solution

We recall that the basic goal of this paper is to integrate blockchain and public digital identity. In this section, we sketch what we identify as the ideal solution of the problem above, in the sense that it implements the above integration in the most direct and strong way.

Suppose we have an IBE system with Private Key Generator PKG (see Sect. 3) and a public identity digital system with identity provider IP (assumed unique, w.l.o.g.). For simplicity, we assume we are not considering blockchains

allowing smart contracts (i.e., Blockchain 2.0), even though the generalization to every kind of blockchain is straightforward. Therefore, we focus our attention just on the elements related to our problem, which are the blockchain addresses and, consequently, the form of transactions. Obviously, the organization of blocks, the consensus protocol, the mining process, and the other aspects of the blockchain are outside the scope of our problem.

Specifically, the elements of the blockchain we are considering in this section are:

1. the blockchain address, denoted by A_u, of a user u and obtained as $A_u = h_1(h_2(P_u))$, where h_1 and h_2 are two proper cryptographic hash functions (as typically done in blockchains), and P_u is a public key of u in the cryptosystem used in the blockchain;
2. the transaction, which we schematically denote as a tuple $\langle P_{u_s}, i, A_{u_r}, c\rangle$, where P_{u_s} is the public key associated with the user *sender*, i denotes the input transactions, A_{u_r} denotes the blockchain address of the user *recipient* (assumed unique for simplicity) and c is the payload of the transaction (e.g., in Bitcoin, it represents the amount of money transferred by this transaction). The transaction is signed by using the secret key S_{u_s}.

Our idea is the following. We assume that u is equipped with a public digital identity granted by IP and let UID be the universal identity number of the user in the public digital identity system (recall that such an identification number exists in real-life public digital identity systems and it is independent of the identity provider, in case of multiple identity providers). Let denoted by IBE^P_{UID} and IBE^S_{UID} the IBE public key and secret key derived by the identity UID, respectively. Recall that, on the basis of the master key, IBE^P_{UID} can be obtained by any party with no need of further information. On the contrary, IBE^S_{UID} is released by PKG through a secure channel to any party able to demonstrate to be the owner of the identity UID. What we require is that PKG becomes a service provider in the public digital identity system, which means that it recognizes in a secure way the identity of people by leveraging the federated authentication protocol involving IP and a (strong) authentication session of the user at IP. Therefore, in order to release secret keys, PKG will require a secure authentication session done according to the protocol of the public digital identity system.

This allows us to design a blockchain in which the address of the user u, recognized in the public digital identity system by the identifier UID, is obtained as: $A_u = h_1(h_2(IBE^P_{UID}))$ (we recall that h_1 and h_2 are two cryptographic hash functions). Therefore, the sources and the recipients of a transaction are derived directly from UIDs, thus from public digital identities, and impersonation is not possible provided that it is not possible in the public digital identity system. Specifically, a transaction $\langle P_{u_s}, i, A_{u_r}, c\rangle$ done by the user u_s with identity UID_s and having as recipient the user u_r with identity UID_r, is signed by the IBE secret key $IBE^S_{UID_s}$ and verified by the IBE public key $IBE^P_{UID_s}$, which everyone can compute on the basis of the IBE public master key, once the identity UID_s is known. This allows us also to represent the transaction as: $\langle UID_s, i, UID_r, c\rangle$.

This representation reflects a nice feature of our solution, in which blockchain addresses are intensionally always existing in the blockchain domain, even though they are not materialized, provided that the corresponding identities exist in the public digital identity system. As a consequence, a given transaction moving a token (or money) to a user u may exist in the blockchain without requiring any action from u on the blockchain (the creation of a key-pair), as identities are implicitly blockchain addresses.

One could argue that a similar solution makes us lose the full decentralization of the blockchain paradigm. This is necessarily true if we want to rely on the current notion of public digital identity system, which is inherently centralized. However, a different notion of digital identity could be applied, also fully decentralized and based on blockchain itself like [8] or [30].

It is worth noting that the ideal solution here presented implicitly requires that blockchain (public and private) keys are compliant with the adopted IBE scheme (for example, RSA [35]). Unfortunately, this is not the case of existing blockchains: for an instance, Bitcoin blockchain adopts the elliptic curve `secp256k1` [32], which is not compliant with any IBE scheme and a definition of an IBE scheme on this cryptographic scheme is not feasible.

For this reason, to give a more practical value (also for the industrial nature of the research project in which this paper is located) to this paper, we implement in the next section a workaround that allows us to basically obtain the same result by leveraging any existing blockchain. Specifically, we chosen Bitcoin blockchain because it is one of the most used, but any other blockchain could be considered, also by extending the approach toward smart-contract-supporting blockchains like Ethereum. Consider that, in this case, any solution (like [19]) that implements the integration between the public digital identity system and the blockchain by directly giving the role of service provider to smart contracts, does not reach the goal in a satisfactory way from the security point of view, because it requires that the service providers (internal to the application domain) are trusted third parties (TTPs). Conversely, in our solution, TTPs are only TTPs of the external systems (i.e., the identity provider of the public digital identity system and the Private Key Generator of the IBE system).

5 A Practical Solution

Starting from the considerations done in the previous section, in this section we provide a practical solution that does not relax any security feature w.r.t. the ideal one. It is practical in the sense that it does not require changes of blockchain formats and protocol, thus operating on the exiting ones. For the sake of presentation, we describe the solution on the Bitcoin blockchain, which is widely used.

The actors in our scenario are:

- *Users*, physical or legal people using a public digital identity for authentication.
- *Identity Providers*, which create and manage public digital identities.

- *IBE Services*, public or private organizations providing the mapping between a public digital identity and a pair of asymmetric encryption keys (called IBE keys).
- a *Blockchain*, a Distributed Ledger.

In our proposal, we can identify the following operations.

1. *Digital Identity Issuing.* First, a user creates his/her public digital identity. To do this, he/she must be registered to one of the *Identity Providers*, which is responsible for the verification of the user identity before issuing the public digital identity and the security credentials.
   A public digital identity is identified by the pair $\langle username, IP \rangle$, where IP is the identifier of the identity provider that issued the public digital identity and *username* is a string. Moreover, there exists a string *UID* (Universal ID), which identifies a public digital identity. For example, the user X registered by the Identity Provider Y is identified by the UID X@Y. It is worth noting that UIDs are supported by the Public Digital Identity Systems.
2. *IBE private key gathering.* To obtain the IBE private key, a user contacts the Private Key Generator (PKG) of the IBE service to receive the master public key, if it is not already known. Then, the Private Key Generator, by acting as a service provider of the public digital identity system, authenticates the user by an eIDAS-compliant scheme, as illustrated in Fig. 2.
   First, the user using a browser (`User Agent`) sends to PKG a request for gathering the IBE private key (Step 1). Then, PKG replies with an authentication request to be forwarded to *Identity Provider* (Step 2). If the received request is valid, *Identity Provider* performs a challenge-response authentication with the user (Steps 3 and 4). In case of successful user authentication, *Identity Provider* prepares the statement of user authentication, which is forwarded to PKG (Step 6). Finally, PKG provides the user with the IBE private key (Step 7).
3. *Blockchain Registration.* First, the user generates a pair of private and public blockchain keys, and, starting from the public one, the blockchain address A is computed. Then, the user generates on the blockchain a transaction from A to A, having as payload $\langle UID, E(A) \rangle$, where UID is the universal ID of the public digital identity of the user, and $E(A)$ is the encryption of the user's blockchain address by the user's IBE secret key. By this transaction, the user links her/his public digital identity to the blockchain address A: indeed, by computing $E(A)$, the user proves the knowledge of the IBE secret key associated with this UID.
4. *Transaction.* When a user S (sender) wants to carry out a transaction with a user R (receiver), the following operations are done:
   (a) S obtains the universal ID of R, say IUD_r.
   (b) S searches for the transaction having IUD_r in the payload: this is the transaction done by R in the blockchain Registration step.
   (c) S extracts from this transaction the blockchain address of R, say A_r.

(d) S generates a blockchain transaction from her/his blockchain address A_s to A_r (the value of the payload depends on the application).

Now, it should be easy to understand how to know the public digital identity of a user involved in a blockchain transaction. Consider a blockchain transaction from the (blockchain) address A_s to the (blockchain) address A_r, and assume we are interested in knowing the identity of the user associated with A_r[1].

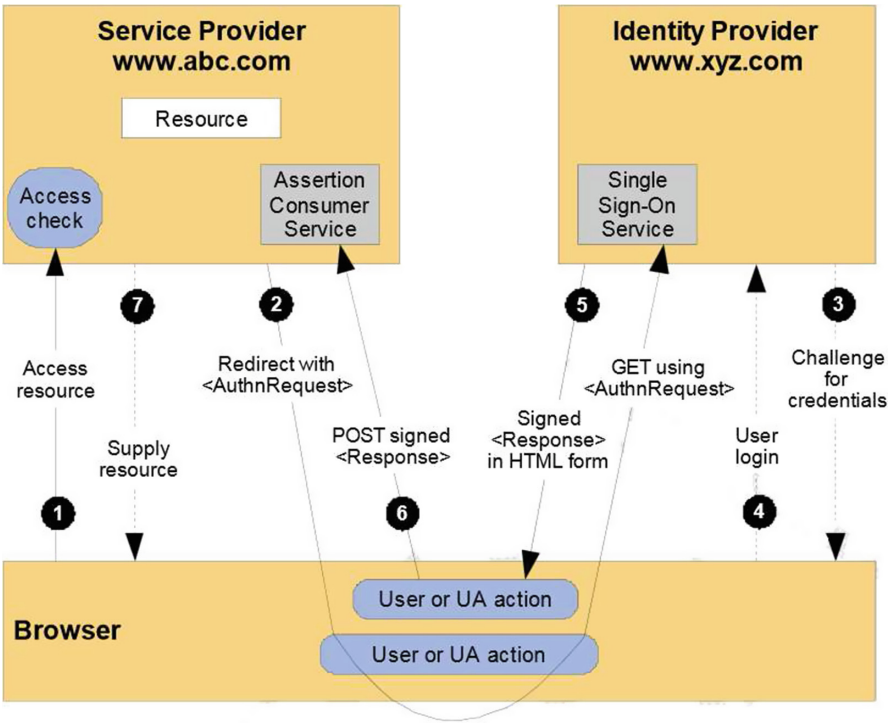

Fig. 2. Data flow in an authentication process.

The first operation to do is to search for the transaction having A_r as sender and receiver (i.e., the transaction done in the Blockchain Registration step). If it is not found, this means that A_s did not execute the protocol correctly, because she/he generated a transaction to an unregistered user (clearly, it is not possible that the registration transaction of A_r has been deleted because blockchain transactions are immutable). Thus, we assume that this registration transaction, say T, is found.

[1] For the sake of presentation and to avoid to introduce new notations, in the following, with a little abuse of notation, we use the address A_u also to refer to the user u, thus meaning "the user associated with the address A_u".

Now, after verifying the authenticity and integrity of T (i.e., that it has been signed by the blockchain public key associated with the address A_r), the payload $\langle p_1, p_2 \rangle$ is extracted.

Next, the IBE public key $IBE^K_{p_1}$ derived from the string p_1 is computed, as described in Sect. 3 and used as public key to decipher p_2. If the decryption of p_2 corresponds to A_r, then we are sure that the receiver (i.e., A_r) of the transaction T is associated with the public digital identity p_1.

Clearly, by repeating the same procedure starting from A_s instead of A_r, we can identify also the user associated with A_s, who generated the transaction.

6 Case Study and Implementation Details

In this section, we instantiate the general approach presented in the previous section to a specific scenario and we show the generated data both to better explain how our proposal works and to demonstrate its compliance with the Bitcoin blockchain.

Among the numerous applications that can benefit from our solution, we selected crowdshipping, which is very timely (as remarked in Sect. 7).

Crowdshipping refers to the phenomenon of recruiting citizens to serve as couriers: a person already traveling from point A to point B takes a package with him and, making a stop along the way, delivers the package to another person in exchange for a reward. The objective is reducing pollution and road traffic using, as a delivery carrier, a person who is already on the move.

Zipments [17], active in New York since 2014, and PiggyBee [11], online since 2012, are probably the most known crowdshipping platforms. Also DHL launched the MyWays platform to facilitate last-mile deliveries throughout Stockholm by involving the city's residents [2]. Being a centralized approach, the platform has to be a trusted party because it is in charge of receiving and storing log activity: clearly, an attack on the system or a malicious behavior of the platform provider could compromise accountability.

To address this problem, the use of blockchain is a solution: all the information needed to guarantee accountability, especially the delivery of a package between two users, is stored in the blockchain. In particular, we considered the basic step of a crowdshipping system, which occurs when a user, say Alice, delivers a package to another user, say Bob. Alice needs both: (1) to be sure that the person receiving the package is Bob and (2) to have a proof of delivery. Our solution guarantees both the goals without using a centralized crowdshipping platform.

We implemented a Java prototype to test our solution in a crowdshipping scenario: it is composed of a module implementing the IBE system and a module implementing the access to the blockchain. We did not need to implement the identification scheme compliant with eIDAS, because it is a service used by our prototype. We show all the operations carried out by the two users and the generated data.

1. *Digital Identity Issuing.* Both Alice and Bob have a public digital identity: thus, they have been identified by an identity provider, say `example.com`, which gave each of them a public digital identity and a credential for authentication (typically, a password). Now, assume that the username of Alice is `alice` and the username of Bob is `bob`. Thus, the UIDs of Alice and Bob are `alice@example.com` and `bob@example.com`, respectively. Observe that, for the sake of presentation, we used the same identity provider (i.e., `example.com`) for both the users: however, no problem arises in case the public digital identities are issued by different identity providers, because the solution does not depend on the particular UID of the user.
2. *IBE private key gathering.* To obtain the IBE private key, a user connects to the site of the IBE system by the browser (i.e., the user agent) and sends a request for accessing the service. Observe that the IBE system acts as a service provider in this step, because it needs to authenticate the user before issuing the private key. Then, the IBE system replies to the user agent with an authentication request to be forwarded to the identity provider. The identity provider is selected according to the user's UID.
   If the received request is valid, the identity provider performs a challenge-response authentication with the user. In case of successful user authentication, the identity provider prepares the *assertion* containing the statement of the user authentication for the IBE service provider. The assertion contains the reference to the request message, the authenticated user, the identity provider, the personal information about the authenticated user, the temporal range of validity, and the description of the authentications context. The assertion is signed by the identity provider to guarantee integrity and authenticity.
   Now, the assertion returned to the user agent is forwarded via `http POST` Binding to the IBE service provider. The IBE system verifies the assertion and provides the user with her/his IBE private key. We denote by IBE_U^S the IBE private key of the user U.
   Concerning the user's IBE public key, they are computed starting from the master public key and the user's UID. We denote by IBE_U^P the IBE public key of the user U.
   In Table 1, the IBE public and private keys of Alice and Bob are reported: they are represented by Base58Check encoding [3], which is used for blockchain addresses (see later).
3. *Blockchain Registration.* Each user needs to have a private and a public blockchain key. The private key is a randomly generated 256-bit string. The public key is generated by the private one by means of a cryptographic function named *elliptic curve point multiplication*. In particular, the used algorithm is Curve Digital Signature Algorithm (ECDSA) and the elliptic curve is `secp256k1` [32]. The use of these functions is necessary to guarantee the compatibility of our solution with blockchain.
   We denote by BKC_U^S and BKC_U^P the blockchain private key and public key of the user U. In Table 1, the blockchain public and private keys of Alice and Bob are reported.

The blockchain address A of a user is computed from the public key K as $A = \text{RIPEMD160}(\text{SHA256}(K))$, where SHA256 [14] is a cryptographic hash developed by National Security Agency (NSA) and returns a 256-bit digest, whereas RIPEMD160 [13] is a cryptographic hash designed in the open academic community and returns a 160-bit digest.
We denoted by A_U the blockchain address of the user U. In Table 1, the blockchain addresses of Alice and Bob are reported. Observe that blockchain addresses are usually represented by Base58Check, an encoding similar to Base64 but modified to remove non-alphanumeric characters and letters which might look ambiguous when printed. It is therefore designed for human users who manually enter the data by copying from some visual source.
Finally, each user generates on the blockchain a transaction with her/his address as both sender and receiver, having as payload $\langle UID, E(A)\rangle$, where UID is the universal ID of the public digital identity of the user, and $E(A)$ is the encryption of the user's blockchain address done by the user's IBE private key.

4. *Transaction.* Now, both Alice and Bob have their public digital identity associated with a blockchain address. Suppose that Alice has to deliver a package with $ID = AB123$ to Bob and, consequently, she needs a proof of delivery from Bob. In a real-life situation, we can image that carriers run a mobile app on their smartphones to manage transaction generations. We can suppose also that the package ID is a QRcode [12] printed on the box, so it can be easily read by the mobile app running on carrier's smartphone. Moreover, the same mobile app can show another QRcode reporting the UID of the owner, in such a way that when Alice has to deliver the package to Bob, Bob can show his UID by his mobile smartphone and vice versa.
Once the package ID and the UID of Alice have been collected, Bob's mobile app generates a transaction to A_{Alice} (i.e., the Alice's blockchain address) including in the payload the type of operation carried out (i.e., package receiving) and the id of the product. This transaction is signed by Bob with the blockchain private key and stored on the blockchain.
Alice can read on the blockchain this transaction and checks its correctness: clearly, this is done by the app mobile. This transaction represents the proof of delivery of the package from Alice to Bob.

Observe that in some context it could be necessary also an additional proof: in this case, Alice can generate a transaction to Bob having, in the payload, "package sending" as the type of operation and the id of the product, in such a way that Bob can proof the reception of the package from the correct user (i.e., Alice).

7 Related Work

In this section, we survey the most important proposals of the state of the art related to our approach.

Table 1. Value of the data generated in our running example.

Symbol	Value
IBE^{S}_{Alice}	2UBUArXzNjLYArGyk46pn6yJVrik5x5sFRne1H2ACznMeBeAfvJyMdbdY 5aDofJ2NxjTQHwCUdpRiPMfKo4Y7CNhrwVq4KDFTiA3KavkyX7b7dE U1CVB1SwEZkMQL2KoD5erHSVsCwcKiqm6yPESsZMPWhEUkWio47D SETVP672AYrnw4E8zMH18gvrnPaERiLd9KL8Z9ZhYui7NL7NWA4oJ8kq GXSsJX85gTheFyswfSXya4HrwfXtQYotrpq7uuS7rKgGGsAhazE7Ceg6mY cMUSdbPg9drR21EUx3LrD3z3sp8QhFvDBpLkdhEZMGsngjDgdu24rZZh M5beQUCC56WVWefRE
IBE^{P}_{Alice}	C9vPE,185xNAn8quf9s4vrechMHXj6PDZakHJ532JYvGbQt7obcLqyyeLub 7VTXcY8qPg3FJj3TvPgEV3CAEx4K9U8diTkGj1xe2dZFicQLWk68KnGy eDZimALtNHm2hEvjFJSDinMtBEQAZrZUXGBrqN7QFT5imVLV821kEJ b1sMh3HMfnhEmucXsn1MDKgCymhkrXHKsFfFRyta9wzQvQKRmdNhT 5FruGXTV8VbA6XG1VaszpUco7EiUzLfayZdA8YWw3umeZDr5bi3AenxM WHXw6ptZFPg7rkf2YgmbHKqFnBCEyDT2gsF8XF9S1rkWjiqsKxef1ZC63 czWiRvfAZ3A5xfo7R9QAsk
IBE^{S}_{Bob}	18NxP33Ub9UwGTA1SRVT5ih4Ji7oq5mFmowxqUHAxQKYgzcUtR5aECK c2sgf6Xmwxo1jzQnPkq1D4LfZp5egDFBCQ2mhUNtL5mwqrkGUaR3qgkDf Dgpu57WntwmyXo8KVoNvHRgcwRSEUzBdMgnGA1JDTaxbCeyf98ebh4D tDxCoygjumt3khenAwnkytiwxiXXnjgXtBxaTPwhBYr1ZVtCmJmR9yoLTn msCQevuL57DtpQc492jwymgMi957FQwe1bDB1WDENgogBX87bTQjqRk mYyK74EFuN1bFPFjbZJ3WAMPWnRCVBawic9eumHWPfwmSfg38jFgP 9f2tJrNKWVX7msGFWQ
IBE^{P}_{Bob}	Meip8,185xNAn8quf9s4vrechMHXj6PDZakHJ532JYvGbQt7obcLqyyeLub7 VTXcY8qPg3FJj3TvPgEV3CAEx4K9U8diTkGj1xe2dZFicQLWk68KnGye DZimALtNHm2hEvjFJSDinMtBEQAZrZUXGBrqN7QFT5imVLV821kEJb 1sMh3HMfnhEmucXsn1MDKgCymhkrXHKsFfFRyta9wzQvQKRmdNhT5 FruGXTV8VbA6XG1VaszpUco7EiUzLfayZdA8YWw3umeZDr5bi3AenxM WHXw6ptZFPg7rkf2YgmbHKqFnBCEyDT2gsF8XF9S1rkWjiqsKxef1ZC6 3czWiRvfAZ3A5xfo7R9QAsk
BKC^{S}_{Alice}	z4KNrFydhCHUt15g9N3MDX4Di2WfuE1JzMMZHRFtVCWkpx6DTH1H VTqBCtdwCL1ERwVfeto3A5pU8G8Fgkv8V2G
BKC^{P}_{Alice}	2f6eQs8MtzDWd1dj95LncxAfEseGNvn7LhbUYrg8kPSUNp5gYKN9zwkvwm ZtPFoFpjPrqdEgeYj3jzbvzKvComRQ7iF9JSE3JGY6UfNBYshkZzXG8qkJ WM93MDDSz6rJzYfAZ8rVU6n9xLLH2CeSSfhv5QZW9MqjcT3v7Mpsahh HtYHUK7
BKC^{S}_{Bob}	22PMoQ4VMGhGwep4KxxqHLB4JtPZFJ5AvLWar5ndP3fvGHaRbsEW2H yw55qAZR9TMyG9Z49P3tApibixFZo2SwXV
BKC^{P}_{Bob}	2f6e6iHZ4yg6h5oTaNj5tvTpgbhbjGJ63DUrA7Zi9n8aut1wtWQ9ELNt3iMeZ 7taavtwv55bZUY2MQdNFmAhoozstxUt6km8j791bWwDtaZGmkxv7vb5bzy sLtnDre8fgQ8GfLuv3F5yEmzweGv69S
A_{Alice}	1QCw797xQbc7UjbpeMeCcdxyj9SpbVnvN4
A_{Bob}	1JCn8rVTLTKf8H1hJQc9Jx2s9FTEwPNUDk

In [18], the authors review applications relying on blockchain. They highlight the potential benefit of such technology in manufacturing supply chain and a vision for the future blockchain ready manufacturing supply chain is proposed. The paper [20] provides a high level understanding of how blockchain technology

will be a powerful tool to improve supply chain operations. It illustrates theoretical and conceptual models for use of open and permissioned blockchain in different supply chain applications with real life practical use cases as is being developed and deployed in various industries and business functions. The paper [29] states that digital supply chain integration is becoming increasingly dynamic. Access to customer demand needs to be shared effectively, and product and service deliveries must be tracked to provide visibility in the supply chain. Business process integration is based on standards and reference architectures, which should offer end-to-end integration of product data. The authors of this study investigate the requirements and functionalities of supply chain integration, concluding that cloud integration can be expected to offer a cost-effective business model for interoperable digital supply chains. Moreover, they explain how supply chain integration through the blockchain technology can achieve disruptive transformation in digital supply chains and networks. In [28], the authors highlight that the need for blockchain-based identity management is particularly noticeable in the Internet age, as we have faced identity management challenges since the dawn of the Internet. They observe that blockchain technology may offer a way to circumvent this problem by delivering a secure solution without the need for a trusted, central authority. It can be used for creating an identity on the blockchain, making it easier to manage for individuals, giving them greater control over who has their personal information and how they access it. The proposed solution stores users' encrypted identity, allowing them to share their data with companies and manage it on their own terms.

Bitnation [4] is the world's first Decentralised Borderless Voluntary Nation (DBVN). Bitnation started in July 2014 and hosted the first blockchain for refugee emergency ID, marriage, birth certificate, World Citizenship and more. The website proof-of-concept, including the blockchain ID and Public Notary, is used by tens of thousands of Bitnation Citizens and Embassies around the world. In [24], the authors focus on Public Digital Identity System (SPID), the Italian government framework compliant with the eIDAS regulatory environment. They observe that a drawback limiting the real diffusion of this framework is that, despite the fact that identity and service providers might be competitor private companies, SPID authentication results in the information leakage about the customers of identity providers. To overcome this potential limitation, they propose a modification of SPID to allow user authentication by preserving the anonymity of the identity provider that grants the authentication credentials. This way, information leakage about the customers of identity providers is fully prevented. The paper [37] focuses on pseudonymisation, a concept that was only recently formally introduced in the EU regulatory landscape. In particular, it attempts to derive the effects of the introduction of pseudonyms (or pseudonymous credentials) as part of the eIDAS Regulation on electronic identification and trust services and, ultimately, to compare them with the effects of pseudonymisation within the meaning of the General Data Protection Regulation (the GDPR). The paper examines how eIDAS conceives pseudonymisation and explains how this interpretation would translate in practical uses in the

context of a pan-European interoperability framework. In [23], an advanced electronic signature protocol that relies on a public system for the management of the digital identity is proposed. This proposal aims at implementing an effective synergy to provide the citizen with a unique, uniform, portable, and effective tool applicable to both authentication and document signature. In [21], the authors propose a security framework that integrates the blockchain technology with smart devices to provide a secure communication platform in a smart city. The authors observe that, despite a number of potential benefits, digital disruption poses many challenges related to information security and privacy. In [26], the authors explore an environment in which in-store customers supplement company drivers can take on the task of delivering online orders on their way home. The results of their computational study provide insights into the benefits for same-day delivery of this form of crowdshipping, and demonstrate the value of incorporating and exploiting probabilistic information about the future.

The study carried out in [31] highlights that passengers and freight mobility in urban areas represents an increasingly relevant component of modern city life. On one side, it fosters economic growth, but, on the other, it also generates high social costs. Congestion and pollution are two problems policy-makers want to curb adopting appropriate measures. In this context, this paper analyses the feasibility and behavioral levers that might facilitate the diffusion of crowdshipping in urban areas. Two are the main objectives the paper. The first is to investigate under which conditions passengers would be willing to act as crowdshippers. The second is to find out under which conditions people would be willing to receive their goods via a crowdshipping service. Crowdshipping can generate positive impacts, such as the reduction of total and ad-hoc trips, by optimizing, through sharing, the use of resources and infrastructures.

From the brief review of the state of the art here reported it clearly emerges both the importance of securely identifying the entities operating in real-life applications that can also benefit from blockchain, and the originality of our proposal that, to the best of our knowledge, is the first combining IBEs and blockchain.

8 Conclusion

In this paper, we discussed about the benefits deriving from the possibility of binding the sender or the receiver of a blockchain transaction to a public digital identity. We proposed an architecture to do this, which exploits eIDAS-compliant identification schemes for handling public digital identities and Identity-based Encryption for associating a digital identity with a public key. This architecture has been implemented by a Java prototype and used to validate the proposal in a crowdshipping scenario. To the best of our knowledge, this is the first attempt to create a non-anonymous blockchain, which can be used in all cases in which the author of a transaction has to be identified with certainty and legal effect.

As future work, we plan to investigate the possibility to use blockchain 2.0 to solve the accountability problem by a smart contract, for example, to allow

the inclusion of new rules and conditions in the product delivery process. Moreover, we need to evaluate the dependence of our solution on the regulation and technological changes or advances in the use of available mechanisms for a more explicit and transparent digital identification.

Acknowledgment. This paper has been partially supported by the project "Id Service - Digital Identity and Service Accountability" funded by the Ministry of Economic Development (MISE), project code number F/050238/03/X32 and by INdAM – GNCS Project 2018 "Processing and analysis of Big Data modeled as graphs in different application contexts".

References

1. ISO/IEC 24760–1:2011: Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts (2011). http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
2. DHL crowd sources deliveries in Stockholm with MyWays (2013). http://www.dhl.com/en/press/releases/releases_2013/logistics/dhl_crowd_sources_deliveries_in_stockholm_with_myways.html
3. Base58Check (2018). https://en.bitcoin.it/wiki/Base58Check_encoding
4. Bitnation Pangea—Your Blockchain Jurisdiction (2018). https://tse.bitnation.co/
5. Digital identity (2018). https://en.wikipedia.org/wiki/Digital_identity/
6. Digital Identity and Service Accountability (2018). http://www.okt-srl.com/ricerca-pon-mise-idservice.html
7. eIDAS - Interoperability Architecture (2018). https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014
8. IBM Blockchain (2018). https://www.ibm.com/blockchain/solutions/identity
9. ID-based Encryption (2018). https://en.wikipedia.org/wiki/ID-based_encryption
10. OAuth Community Site (2018). https://oauth.net/
11. PiggyBee: CrowdShipping - Crowdsourced delivery (2018). https://www.piggybee.com/
12. QR code (2018). https://en.wikipedia.org/wiki/QR_code
13. RIPEMD (2018). https://en.wikipedia.org/wiki/RIPEMD
14. SHA-2 (2018). https://en.wikipedia.org/wiki/SHA-2
15. SPID Sistema Pubblico di Identità Digitale (2018). https://www.spid.gov.it/
16. Windows CardSpace (2018). https://en.wikipedia.org/wiki/Windows_CardSpace
17. Zipments: Same Day Delivery Service (2018). https://zipments.com/
18. Abeyratne, S.A., Monfared, R.P.: Blockchain ready manufacturing supply chain using distributed ledger (2016)
19. Angiulli, F., Fassetti, F., Furfaro, A., Piccolo, A., Saccà, D.: Achieving service accountability through blockchain and digital identity. In: Mendling, J., Mouratidis, H. (eds.) CAiSE 2018. LNBIP, vol. 317, pp. 16–23. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-92901-9_2
20. Banerjee, A.: Blockchain technology: supply chain insights from ERP. Adv. Comput. **111**, 69–98 (2018)
21. Biswas, K., Muthukkumarasamy, V.: Securing smart cities using blockchain technology. In: 2016 IEEE 18th International Conference on High Performance Computing and Communications, IEEE 14th International Conference on Smart City, IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 1392–1393. IEEE (2016)

22. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_13
23. Buccafurri, F., Fotia, L., Lax, G.: Implementing advanced electronic signature by public digital identity system (SPID). In: Kő, A., Francesconi, E. (eds.) EGOVIS 2016. LNCS, vol. 9831, pp. 289–303. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-44159-7_21
24. Buccafurri, F., Fotia, L., Lax, G., Mammoliti, R.: Enhancing public digital identity system (SPID) to prevent information leakage. In: Kő, A., Francesconi, E. (eds.) EGOVIS 2015. LNCS, vol. 9265, pp. 57–70. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-22389-6_5
25. Christopher, M.: Logistics & Supply Chain Management. Pearson, London (2016)
26. Dayarian, I., Savelsbergh, M.: Crowdshipping and same-day delivery: employing in-store customers to deliver online orders. Optimization Online (2017)
27. Iansiti, M., Lakhani, K.R.: The truth about blockchain. Harv. Bus. Rev. **95**(1), 118–127 (2017)
28. Jacobovitz, O.: Blockchain for identity management (2016)
29. Korpela, K., Hallikas, J., Dahlberg, T.: Digital supply chain transformation toward blockchain integration. In: Proceedings of the 50th Hawaii International Conference on System Sciences (2017)
30. Lewko, A., Waters, B.: Decentralizing attribute-based encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 568–588. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4_31
31. Marcucci, E., Le Pira, M., Carrocci, C.S., Gatta, V., Pieralice, E.: Connected shared mobility for passengers and freight: investigating the potential of crowdshipping in urban areas. In: 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), pp. 839–843. IEEE (2017)
32. Mayer, H.: ECDSA security in bitcoin and ethereum: a research survey. CoinFaabrik, 28 June 2016
33. Moreno, F., Trivedi, S.: Staying Anonymous on the Blockchain: Concerns and Techniques (2017). https://securingtomorrow.mcafee.com/mcafee-labs/staying-anonymous-on-the-blockchain-concerns-and-techniques/
34. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)
35. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
36. Sakai, R., Kasahara, M.: ID based cryptosystems with pairing on elliptic curve. IACR Cryptology ePrint Archive, p. 54 (2003)
37. Tsakalakis, N., Stalla-Bourdillon, S., O'hara, K.: What's in a name: the conflicting views of pseudonymisation under eIDAS and the general data protection regulation (2016)