An SSI Based System for Incentivized and Self-determined Customer-to-Business Data Sharing in a Local Economy Context

Kevin Wittek
Blockchain Research Lab
Institute for Internet Security
Gelsenkirchen, Germany
https://orcid.org/0000-0003-1245-9970

Laura Lazzati
Blockchain Research Lab
Institute for Internet Security
Gelsenkirchen, Germany
lazzati@internet-sicherheit.de

David Bothe
Data Research Lab
Institute for Internet Security
Gelsenkirchen, Germany
bothe@internet-sicherheit.de

Ann-Julie Sinnaeve
Data Research Lab
Institute for Internet Security
Gelsenkirchen, Germany
sinnaeve@internet-sicherheit.de

Norbert Pohlmann
Managing Director
Institute for Internet Security
Gelsenkirchen, Germany
pohlmann@internet-sicherheit.de

***Abstract*—With ongoing developments in the field of smart cities and digitalization in general, data is becoming a driving factor and value stream for new and existing economies alike. However, there exists an increasing centralization and monopolization of data holders and service providers, especially in the form of the big US-based technology companies in the western world and central technology providers with close ties to the government in the Asian regions. Self Sovereign Identity (SSI) provides the technical building blocks to create decentralized data-driven systems, which bring data autonomy back to the users. In this paper we propose a system in which the combination of SSI and token economy based incentivisation strategies makes it possible to unlock the potential value of data-pools without compromising the data autonomy of the users.**

***Index Terms*—ssi, token economy, blockchain, local economies, customer to business, gdpr, dlt**

I. Introduction

Personal data is an increasingly important asset class for organizations in our current society [1]. In this way, collecting personal data on a system of participants results in valuable insights of the overall behavior of the system and can help to accomplish personal goals of an organization. With incentivised tokens, it is possible to transcend the behavior of a community to a collective goal by providing tokens in exchange of specific actions [2]. Normally, when presenting incentives for data sharing in the context of a market economy, the customer is not able to choose which parts of their data is shared with which authority. They have to accept the terms and conditions because otherwise they cannot use the system. This is seen in the state of the art, demonstrating that there are systems in existence worldwide in which consumers are rewarded by their consuming behavior. For example, the mobile payment market in China is dominated by Alipay and Tenpay [3]. Both are connected to social-credit like systems, which results in perks being granted by the commercial sector and punishments being managed by government authorities [4]. We can observe a similarly centralized situation in Germany with regards to Payback and DeutschlandCard, the first being used by 75% German customers and the second one by 40% respectively [5]. In addition, there is a rising interest in systems specifically targeting the small scale regional economy, such as the CityBonusCard in Rheda-Wiedenbrück [6] and the Bonuspunkt Wittgenstein card [7]. Both are implemented using the proprietary meinbonus.cash system which allows local retailers to gather insights about the consumer behavior in their local market while the consumers get incentivized to share their data by different discounts and special offers [8].

SSI, as defined by the German Blockchain Association (GBA), is "a model of digital identity where individuals and entities alike are in full control over central aspects of their digital identity [...] and over how their Credentials and related personal data is shared and used." [9]. Christopher Allen defined the "Ten Principles of SSI" [10], where he proposes, among others, that users must agree to the use of their identity and that the identity must be widely available, crossing international boundaries.

In this paper we propose a system similar to the ones above mentioned, in which customers are encouraged with rewards for their behavior applied to local economies in Germany, taking into account the General Data Protection Regulation (GDPR) legislation. Nevertheless, the main differentiating factor in our approach is the application of SSI to it. In this way, consumers are not only the owners of their data, but also they can choose what to share and in which granularity, being incentivised by perks of different degrees. Due to the main

Partially supported by the Ministry of Economic Affairs, Innovation, Digitalisation and Energy of the State of North Rhine-Westphalia

principles of SSI, they can only share the minimum amount of information that is needed for their reward. Moreover, since the system is thought to be regional, it supports small and medium companies and organizations.

II. Behavior Modeling and incentivising economic activities

With incentivised tokens, it is possible to transcend the behavior of a community to a collective goal by providing tokens in exchange of specific actions [2]. With set goals, nudging individuals can change their overall behavior to reach them, e.g. nudging the population to live a healthier life [11]. Centralizing the goals around monetized incentives on direct actions gives the individuals a tangible reward which they can measure. This results in a more motivated individual that will follow the course of actions [12]. Exchanging data as a part of each action in an economic field can revolve around sharing the items that have been bought in a specific store at a specific time. By rewarding the revelation of their shopping behavior, individuals can earn money that can then be spent for new items again. With the definition of the goal by any authority building a token economy, many possibilities open up. For example, reducing the CO2 emissions by rewarding ecological behavior or getting patients with mental conditions into more social activities [13]. In an economic setting, the incentives resolve around monetizing the shopping behavior of a consumer. A good example of this is the current Payback point system, where all shopping behavior is tracked by an authority. However, when presenting monetary incentives to a customer in exchange for their data, they normally are not free to choose which of their data is shared with any authority. Our proposed system can change this by providing the ability of selective sharing mechanisms, e.g. each participant of said system can choose which category of their shopping behavior will be shared. It is then possible to get rewards for sharing data on food purchases with restrictions on data shared from hygiene products, unlike the Payback system, which will process all the shopping data at once [14]. It is still possible to generate higher rewards for sharing more sensitive data. With our concept, there is freedom in exchanging the data, which differs from already implemented systems due to the high amount of privacy gains.

III. System Design

In this section the overall system design (as shown in Fig. 1) is discussed. After a general overview of the system context, the underlying technologies and communication protocols are explained in detail.

A. *Overall system design*

The main goal of our proposed system is to allow the incentivation of a certain consuming behavior of a community by encouraging data sharing. Unlike existing solutions, as mentioned in I, its members can choose up to which extent they want to participate while not disclosing their real identity. The targeted application area is anchored in local economies of Germany. Our system involves three main actors, namely the customer as Individual (IND), Local Shop (LS), and a Local Retail Association (LRA). The latter is the one in charge of deciding which behavior is the one to encourage, since it is the issuer of tokens based on each individual's consuming trends and data sharing behavior. The LRA is also tasked with generating and distributing shopping trends to LS after a posteriori analysis of the aggregated shared data was processed. Every time IND shops at LS, LS issues them a credential with the details of the purchased items, which are called claims in the technical terminology (a credential as an aggregate of claims is therefore the domain specific representation of the real world shopping receipt, or invoice, aggregating a set of invoice positions). IND can fully use it, use it partially (showing only a portion of the items bought), or not use it at all. IND may then show the credential to LRA that, based on the desired behavior, gives back a token to IND, and IND can use this token as part of the payment in the next purchase (see the Use Case diagram in Fig. 2).

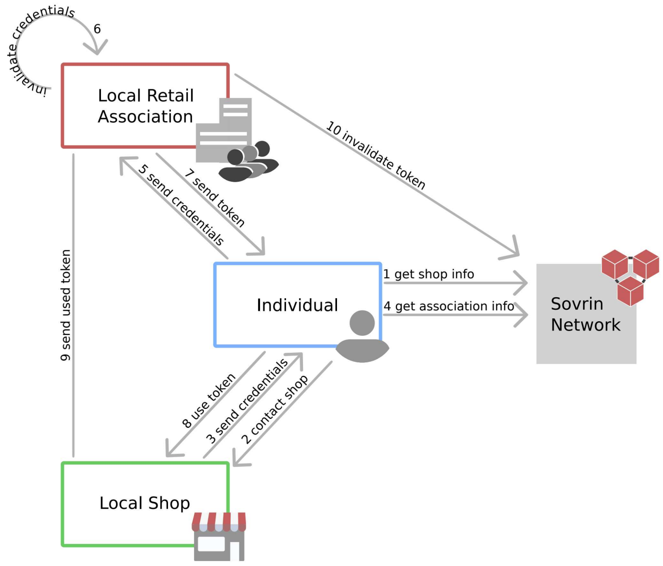

Fig. 1. Claim Sharing Process

Our system relies on Sovrin Network (Sovrin) (see III-B), so the starting point for IND is fetching the information of LS from Sovrin. After setting up a communication channel with LS, IND is given a credential. Each credential can only be fully used once. If IND wants to share their credential with LRA, it fetches its information from Sovrin, starts a new communication, sends the credential, and is given back a token. LRA keeps track of the credentials to prevent from IND using the same credential or the same part of the same credential indefinitely. Now, IND can contact LS again and use this Token towards it. Lastly, LS sends the used token to LRA so that it invalidates it towards Sovrin.

The actual flow of the complete business process can be summarized as the following sequence of use cases (with all uses cases shown in Fig. 2):

1) Establish connection IND→LS
2) Receive credential
3) Establish connection IND→LRA
4) Share credentials and receive token
5) Redeem a token

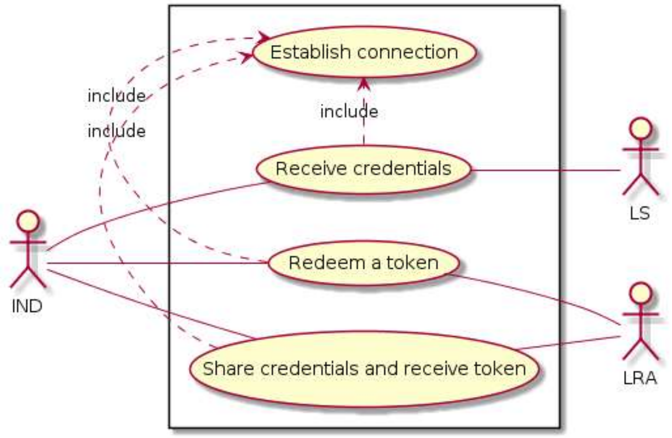

Fig. 2. Use Case diagram

B. Sovrin Network

The Sovrin Network is "the world's first distributed ledger engineered specifically for self-sovereign identity", which is operated as a network of decentralized nodes hosted by different organisations [15]. It contains the Sovrin Public Ledger, a blockchain based registry for Decentralized Identifiers (DID) and their associated DID Documents [16], a "file that contains all the metadata needed to prove ownership and control of a DID as well as share the cryptographic keys and resource pointers (endpoints) necessary to initiate trusted peer interactions between Sovrin entities" [15]. Every identity holder establishes a unique pseudonymous DID for every relationship they have. A DID added directly to Sovrin is called a public DID whereas a pairwise pseudonymous DID shared and stored privately off-ledger between identity holders is called a private DID [15]. Public DIDs are needed mainly by issuers of credentials. Neither credentials nor their hashes are stored on Sovrin; they are only issued and exchanged off-ledger. Also note, that the public DID is only used to establish cryptographic trust. The establishment of human trust, so that IND can verify that a certain LS is the owner of their corresponding DID, has to happen off-ledger and is outside of the context boundary of the proposed system [15].

To allow the revocation of credentials, the issuer submits a revocation registry data structure to Sovrin which references the credential definition and contains a single number called cryptographic accumulator. Only the credential holder, using their knowledge of which credential belongs to them, can create a cryptographic Zero Knowledge Proof of Non-Revocation: a proof that their credential belongs to the set of valid credentials. When an issuer needs to revoke a credential, it subtracts the credential hash from the cryptographic accumulator and posts the new number to Sovrin. The moment that happens, the credential holder will no longer be able to produce a valid Proof of Non-Revocation. [15]

C. Establish a private connection with entities

Every time an entity wants to establish a connection with a publicly registered entity, it fetches their public DID Document from Sovrin and creates a new unique private DID and DID Document. Following this, it contacts the entity and sends this tuple. As a result, the public entity also creates a new private DID and DID Document and returns the tuple to the connection initiating entity. These tuples will be used for all further communications between both entities during this time based communication session (see Fig. 3 for a concrete example in case of the IND →LS relationship).

Since the establishment of a new private connection is the same for every Entity-to-Public-Entity relationship, the diagrams for IND →LRA and LS →LRA are omitted.

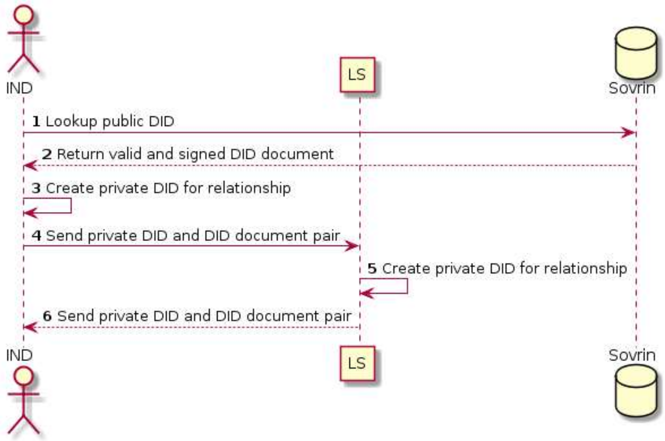
IND
LS
Sovrin
1 Lookup public DID
2 Return valid and signed DID document
3 Create private DID for relationship
4 Send private DID and DID document pair
5 Create private DID for relationship
6 Send private DID and DID document pair
IND
LS
Sovrin

Fig. 3. Use Case: Establish connection

D. Receive credentials

After IND initiates a request to receive a credential, a credential containing all claims for the current shopping event is issued by LS and transferred to IND, where it is stored securely within their private wallet (see Fig. 4). A wallet, in the context of SSI and Sovrin, is a component for managing private data necessary for participating in the system [15].

In addition, each credential contains a globally unique identifier for protection against being shared multiple times.

E. Share credentials and receive token

Once IND shares a set of credentials with LRA, the latter checks if they were already used and, if they were not, afterwards marks them internally (this process happens completely off-chain and could theoretically be implemented by using a regular database backed system). Subsequently, a new valid token is issued and transferred to IND, who saves it securely in their private wallet (see Fig. 5).

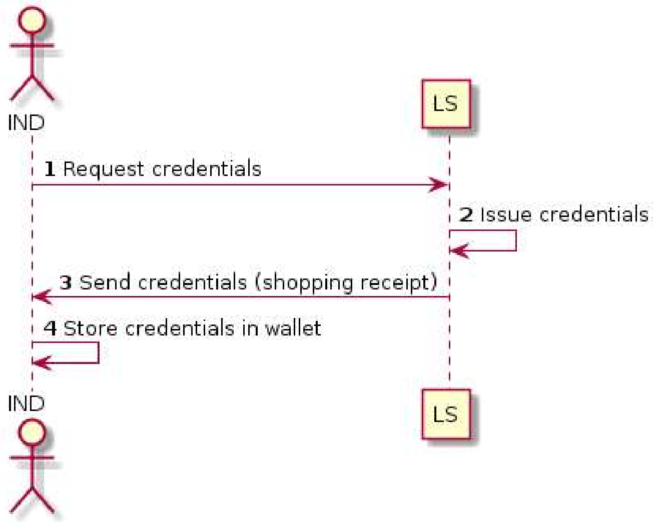
IND
LS
1 Request credentials
2 Issue credentials
3 Send credentials (shopping receipt)
4 Store credentials in wallet
IND
LS

Fig. 4. Use Case: Receive credentials

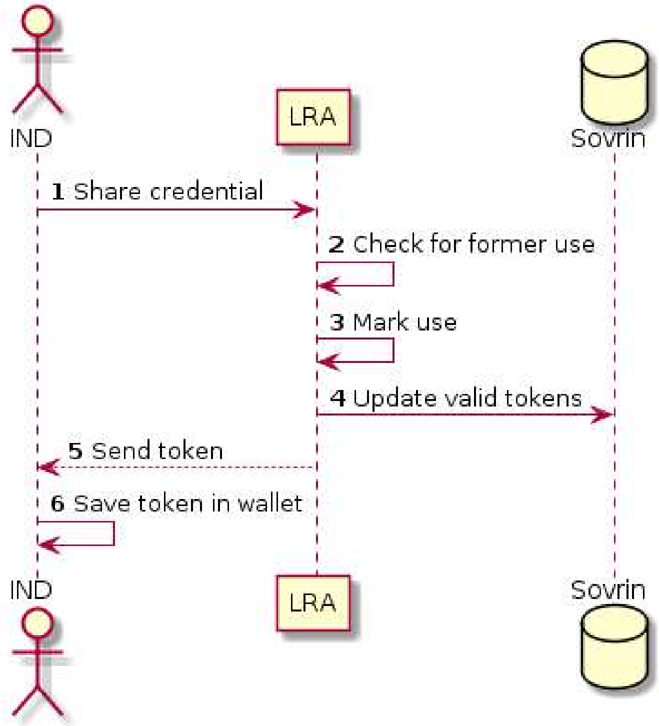

Fig. 5. Use Case: Share Credentials and receive token

F. *Redeem a token*

In order to redeem a token, IND will leverage Sovrin to create a Zero Knowledge Proof stating its validity. Afterwards, it sends the valid token to LS where it is applied according to business rules. Consecutively, LS establishes a connection with LRA (see section III-C) and sends the used token, which allows LRA to invalidate it on Sovrin (see Fig. 6).

Note: The definition and application of the business rules of token usage happens outside of the provided system and could range from a price discount to free products. Therefore, it is an important adjustable parameter for controlling and influencing the incentivation properties of the system, but outside of the scope of this paper.

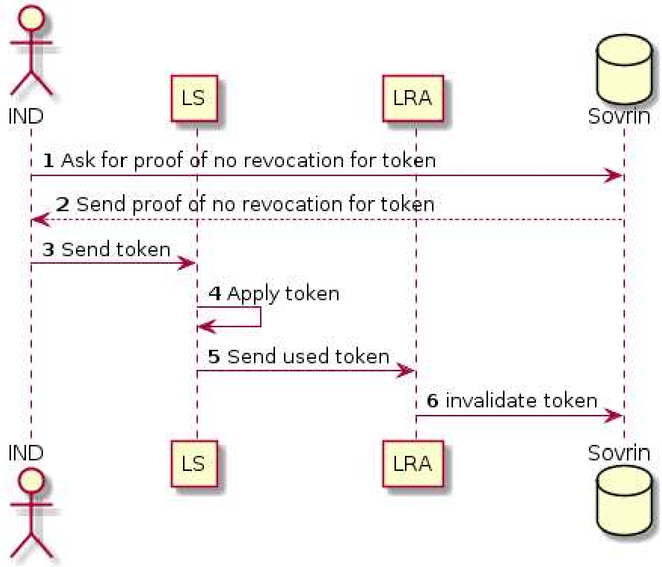

Fig. 6. Use Case: Redeem a token

IV. Relevance for Practice and Legal Implications

In spite of the existence of some tensions between certain Blockchain systems and the GDPR - as stated by the European Union Blockchain Observatory and Forum (EUBOF) [17] - our proposed system will take all the necessary considerations to fulfill the regulations into account. GBA mentions that the GDPR will apply to SSI only in the cases in which the Blockchain is processing the personal data of natural persons. This includes all pseudonymous data but omits data that has been anonymised. Public keys and addresses are considered personal data unless they are sufficiently anonymised. The European Data Protection Board (EDPB) mentions that hashed personal data is pseudonymous [18]. GBA states that while there is no direct guidance from EDPB as to whether a DID is personal data, it is expected to be when it belongs to a natural person. Since in our proposed system, only DIDs of participating business entities are stored on the ledger, the identity of the IND is never disclosed directly. However, more sophisticated efforts of data flow analysis and cross-correlation of data between multiple LS entities might allow for identification of INDs in case of insufficient big data sets. Other key challenges of applying the GDPR to solutions like SSI include determining who the data controllers and processors are, determining and enforcing rules for cross-border or extra European Union transfers of personal data, disclosing automated processing, and giving effect to the rights of restriction of processing and erasure.

V. Related Work

Decentralizing data is proposed by Zyskind et al. while employing a blockchain to protect privacy data of individuals [19] .In their work, they state how third-parties collect and control massive amounts of personal data, hence they propose a decentralized personal data management system that ensures users own and control of their data, with a protocol that turns a blockchain into an automated access-control manager. Similarly, Tomas Isdal et al. also describe the implementation of an alternative P2P data shared protocol in which users are in full control of their data: the same data can be shared publicly, anonymously, or with access control, with both trusted and untrusted peers [20] Moreover, a combination of aggregating pseudonymous data in a local blockchain mining node while leveraging bloom filters for authentication has been proposed for the design of privacy-preserving data sharing in the context of a smart power grid [21].

VI. Main Findings and Further Work

The technical feasibility of our proposed system can be easily demonstrated. It has been shown that it is possible to design a system for incentivizing behaviour using tokens while at the same time honoring user privacy according to SSI concepts. It also demonstrates the flexibility of the SSI approach for application in existing business domains. However, it is still up to question how the system will perform in a real economic scenario and how the behavior and dynamics of the customer-business relationship will change in the context of said system.

Our system presents a trade-off between eradicating the possibility of using a credential indefinitely and preserving the user's sovereignty to the fullest. The generation of a unique identifier for a credential and its storage by LRA might result in a cross-correlation between LRA and LS for obtaining the complete original credential even if claims have been shared partially. Nevertheless, even if this disclosure happened, thanks to the creation of different DIDs for every relationship the identity of the user is never disclosed. An improvement of this aspect may occur in future implementations of the system.

Acknowledgment

This work was partially supported by the Ministry of Economic Affairs, Innovation, Digitalisation and Energy of the State of North Rhine-Westphalia as part of the connect.emscherlippe project at the Westphalian University of Applied Sciences in Gelsenkirchen. We would like to thank the anonymous reviewers for their valuable feedback.

References

[1] K. Schwab, A. Marcus, J. R. Oyola, and W. Hoffman, "Personal Data: The Emergence of a New Asset Class," p. 40, 2011.

[2] K. Zlomke and L. Zlomke, "Token economy plus self-monitoring to reduce disruptive classroom behaviors." *The Behavior Analyst Today*, vol. 4, no. 2, pp. 177–182, 2003.

[3] "China's Third-Party Mobile Payment Market Soared 58.4% in 2018." [Online]. Available: http://www.iresearchchina.com/content/details7_54345.html

[4] "How China Is Using Big Data to Create a Social Credit Score." [Online]. Available: https://time.com/collection/davos-2019/5502592/china-social-credit-score/

[5] "Studie: Bonusprogramme wirken!" [Online]. Available: https://www.splendid-research.com/de/ueber-uns/presse/item/studie-bonusprogramme-bei-verbrauchern-beliebt-wie-nie-zuvor.html

[6] M. Pokorra-Brockschmidt, "Der Einzelhandel in Rheda-Wiedenbrück setzt auf die CityBonusCard." [Online]. Available: https://www.nw.de/lokal/kreis_guetersloh/rheda_wiedenbrueck/22545572_Der-Einzelhandel-in-Rheda-Wiedenbrueck-setzt-auf-die-CityBonusCard.html

[7] "Bonuspunkt Wittgenstein." [Online]. Available: http://www.bonuspunkt-wittgenstein.de/

[8] "meinbonus.cash." [Online]. Available: https://www.meinbonus.net/

[9] K. Wager, "Self-sovereign Identity. A position paper on blockchain enabled identity and the road ahead." [Online]. Available: https://bundesblock.de/wp-content/uploads/2019/01/ssi-paper.pdf

[10] "The Path to Self-Sovereign Identity." [Online]. Available: https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

[11] T. M. Marteau, D. Ogilvie, M. Roland, M. Suhrcke, and M. P. Kelly, "Judging nudging: can nudging improve population health?" *BMJ*, vol. 342, 2011. [Online]. Available: https://www.bmj.com/content/342/bmj.d228

[12] M. Pessiglione, L. Schmidt, B. Draganski, R. Kalisch, H. Lau, R. J. Dolan, and C. D. Frith, "How the brain translates money into force: A neuroimaging study of subliminal motivation," *Science*, vol. 316, no. 5826, pp. 904–906, 2007. [Online]. Available: https://science.sciencemag.org/content/316/5826/904

[13] M. Hersen, R. M. Eisler, G. S. Alford, and W. Agras, "Effects of token economy on neurotic depression: An experimental analysis," *Behavior Therapy*, vol. 4, no. 3, pp. 392 – 397, 1973. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0005789473801194

[14] "Allgemeine Datenschutzhinweise für das PAYBACK Bonusprogramm." [Online]. Available: https://www.payback.de/info/hinweise-datenschutz

[15] A. Tobin, "Sovrin: What Goes on the Ledger?" p. 12, 2018.

[16] "Decentralized Identifiers (DIDs) v1.0." [Online]. Available: https://www.w3.org/TR/did-core/

[17] T. Lyons, L. Courcelas, and K. Timsit, "Blockchain and the GDPR." [Online]. Available: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

[18] D. P. W. PARTY, "Opinion 05/2014 on Anonymisation Techniques." [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[19] G. Zyskind, O. Nathan, and A. . Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, May 2015, pp. 180–184.

[20] T. Isdal, M. Piatek, A. Krishnamurthy, and T. Anderson, "Privacy-preserving P2P data sharing with OneSwarm," *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 4, pp. 111–122, Aug. 2010. [Online]. Available: https://doi.org/10.1145/1851275.1851198

[21] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, Jul. 2018.