BLOCKCHAIN BASED PERSONAL IDENTITY SECURITY SYSTEM

1st Sahil Mujawar
Computer Engineering
Savitribai Phule Pune University
Pune, India
sahilmujawar192001@gmail.com

2nd Farhan Shaikh
Computer Engineering
Savitribai Phule Pune University
Pune, India
farhan1919shaikh@gmail.com

3rd Mohammed Hares
Computer Engineering
Savitribai Phule Pune University
Pune, India
haresbenz@gmail.com

4th Dr. (Mrs)S.R. Khonde
Computer Engineering
Savitribai Phule Pune University
Pune, India
shraddha.khonde@mescoepune.org

Abstract— Identity theft is the unauthorized acquisition of another person’s confidential information in order to misuse it. Organizations and individuals should exercise caution when it comes to protecting their identities in order to avoid fraud as a result of identity theft. This information is freely available to attackers in user profiles. Attackers use this information to obtain additional information without raising suspicions about a final attack, identity theft, or fraud. Our blockchain based Personal Identity Security System assists in securely storing personal identity data without fear of it being compromised or lost. In this system, the admin can access all the users and verify those accounts. The admin has access to all of the user’s documents that have been uploaded to the system. They can view all of the user’s activity logs. The admin can view the status and see if any fabrication is taking place. The admin can view the user’s complaints.

Keywords— **Blockchain Learning, Node js, Etherium, remix IDE, polygon blockchain, metamask.**

1. INTRODUCTION

Our lives have become increasingly digital and so has the vast amount of personal data traces that we leave behind. The current situation is that a few large multinational corporations make the majority of profits through offering services users pay for with their data. While data analytics can provide users with better services, the users’ overview and control of their personal data has decreased. Moreover, the recent Cambridge Analyticascandal of misusing people’s personal information from Facebook to influence voters in the US Elections 20161 has raised serious concerns about the technical, commercial, political and ethical aspects of personal data.In May 2018 the European Union’s new GDPR.came into effect. While aiming to protect the users, the new regulation can potentially be a burden for companies. While the GDPR aims to give control of personal online data to European users through new regulation, several further initiatives have been launched both from private and public spheres, to argue for a human centric approach to personal information[2].

In 2014 the Finnish government published a study on the concept of MyData. MyData facilitates the idea that users should have a better overview of where their data is stored, who uses it, and be able to change this. It is a human centric approach to people’s data and aimed at giving control of personal data back to the users. On a different note, blockchain technology generated significant research interest and industry attention in recent years mostly due to the hype and success created by the cryptocurrencies. For example, Bitcoin was first described in 2008 and ever since has attracted the attention of the research community from diverse academic fields and gained mainstream popularity due to its disruptive characteristics, such as the absence of centralized control and high degree of anonymity. Applications which were previously run through a trusted intermediary, can now - using blockchain technology - operate more transparently in a decentralised mode without the need of having a central

authority and in a much more transparent way. We address the problem of personal data identity and management by adopting a human-centric approach that ensures a GDPR compliance by employing blockchain-based technologies Currently users lack transparency over which service is processing their personal data for which purpose and possibly handing over personal data to third party providers without the user’s knowledge.

This is partly due to extensive and complicated terms and conditions of a service and the user requirement to agree to these,if they wish to use the service. Moreover, there are no suitable mechanisms that enable users to opt- out from a service gracefully, e.g. deleting all the history of using the service from the service provider. And lastly,currently there is a lack of systems that enable users in an effective and user-friendly way to obtain an overview of the usage of their personal data and to exercise fine grained control over the usage of their personal data. While the GDPR addresses the aspects of transparency and consent and puts the legislation in place to enforce appropriate mechanisms, the latter issue of user control has not sufficiently been solved yet. Furthermore, after users have gained full transparency, they need adequate means to control the consent that is connected to the usage of their personal data.

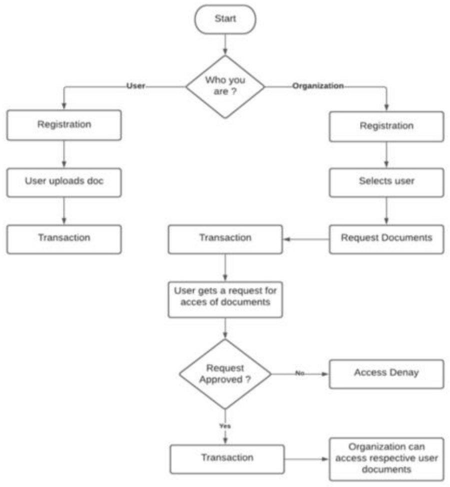
The GDPR will put the regulation in place to empower the user to request deletion of or revoke consent to use their personal data.However, there is a need to research and develop a system that facilitates this request or revocation of personal data. The main focus of this research work is to come up with a conceptual design for such a system called Blockchain Based Personal Data and Identity Management System(BPDIMS) that empowers users to get full transparency and control over the usage of their personal data. Consequently, the overarching research question is: How can blockchain be utilized to develop a system for personal data and identity security system which is human-centric and GDPR compliant?

2. RELATED WORK

Recent scandals on the abuse of personal information from social media platforms and numerous user identity data breaches raise concerns about technical, commercial, and ethical aspects of privacy and security of user data. The European Union's new General Data Protection Regulation (GDPR) is one of the largest changes in data privacy regulation and entails several key regulatory measures for both data controllers and data processors to empower and protect EU citizens' privacy. In this research work, we propose a conceptual design and high-level architecture for a Blockchain-based Personal Data and Identity Management System (BPDIMS), a human-centric and GDPR-compliant personal data and identity management system based on the blockchain technology. We describe how BPDIMS's architecture utilizes blockchain technology to provide a high-level of security, trust and transparency. We discuss how BPDIM's humancentric approach with GDPR compliance shifts the control over personal data to the end users and empowers them better. Our lives have become increasingly digital and so has the vast amount of tion is that a few large multina-tional corporations make the majority of profits through offering services users pay for with their data. While data analytics can provide users with better services, the users' overview and control of their personal data has decreased. Moreover, the recent Cambridge Analytica scandal of misusing people's personal information from Facebook to influence voters in the US Elections 20161 has raised serious concerns about the technical, commercial, political and ethical aspects of personal data. In May 2018 the European Union's new GDPR. came into effect. While aiming to protect the users, the new regulation can potentially be a burden for companies. While the GDPR aims to give control of personal online data to European users through new regulation, several further initiatives have been launched both from private and public spheres, to argue for a human centric approach to personal information. In 2014 the Finnish government published a study on the concept of MyData.

MyData facilitates the idea that users should have a better overview of where their data is stored, who uses it, and be able to change this. It is a human-centric approach to people's data and aimed at giving control of personal data back to the users. On a different note, blockchain technology generated significant research interest and industry attention in recent years mostly due to the hype and success created by the cryptocurrencies. For example, Bitcoin was first described in 2008 and ever since has attracted the attention of the research community from diverse academic fields and gained mainstream popularity due to its disruptive characteristics, such as the absence of centralized control and high degree of anonymity. Applications which were previously run through a trusted intermediary, can now - using blockchain technology - operate more transparently in a decentralised mode without the need of having a central authority and in a much more transparent way.

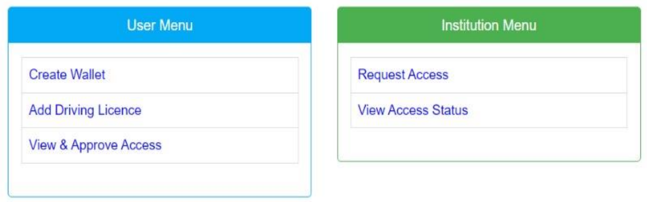
We address the problem of personal data identity and management by adopting a human-centric approach that ensures a GDPR compliance by employing blockchain-based technologies Currently users lack transparency over which service is processing their personal data for which purpose and possibly handing over personal data to third party providers without the user's knowledge. This is partly due to extensive and complicated terms and conditions of a service and the user requirement to agree to these, if they wish to use the service. Moreover, there are no suitable mechanisms that enable users to opt-out from a service gracefully, e.g. deleting all the history of using the service from the service provider. And lastly, currently there is a lack of systems that enable users in an effective and user-friendly way to obtain an overview of the usage of their personal data and to exercise finegrained control over the usage of their personal data. While the GDPR addresses the aspects of transparency and consent and puts the legislation in place to enforce appropriate mechanisms, the latter issue of user control has not efficiently been solved yet. Furthermore, after users have gained full transparency, they need adequate means to control the consent that is connected to the usage of their personal data. The GDPR will put the regulation in place to empower the user to request deletion of or revoke consent to use their personal data. However, there is a need to research and develop a system that facilitates this request or revocation of personal data. The main focus of this research work is to come up with a conceptual design for such a system called Blockchain-based Personal Data and Identity Management System (BPDIMS) that empowers users to get full transparency and control over the usage of their personal data. Consequently, the overarching research question is: How can blockchain be utilized to develop a system for personal data and identity security system which is human-centric and GDPR compliant?



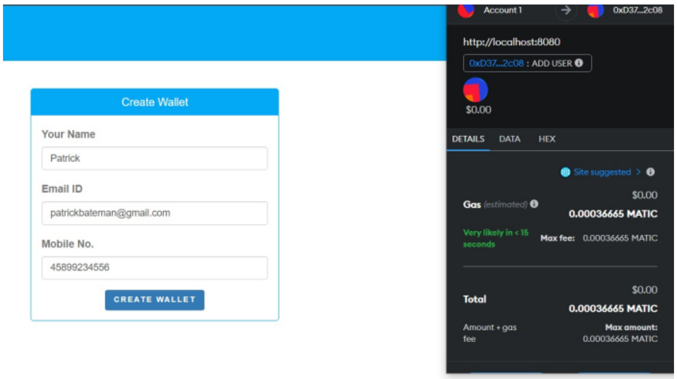
Flow Chart for Identity Management

3. METHOD OR IMPLEMENTATION

a. Blockchain is the decentralized distributed database technology that is combined with guarantees against tamper-resistance of transactions/records using cryptographic methods. By using time stamping of its transactions and messages, blockchain provides universally verifiable proofs for existence or absence of a transaction in the distributed database and the underlying cryptographic primitives using hash functions and digital signatures provide guarantee that these proofs are computationally secure and verifiable at any point in time. Blockchain is decentralized, jointly maintained by a plurality of independent parties/nodes and achieves consistency of transactions among distributed nodes by using distributed consensus protocols (such as Byzantine fault tolerance algorithm) without the need of having a central authority. Blockchain transactions are transparent and visible to all users of the system and at the same time blockchain provides anonymity to its users by allowing them create A blockchain can be defined as a purely distributed peer-to-peer system in the form of a Ledger (accounting book) that uses a software/algorithm that adds informational content into ordered and connected data blocks, ensuring the inviolability of previous blocks, through cryptographic technology [10].pseudo -anonymous transactions without the need for disclosing their personal information.



The disruptive and innovative nature of blockchain technology resulted in the evolution of many decentralized applications such cryptocurrencies and smart contracts. Bitcoin, a decentralized cryptocurrency based on blockchain technology was introduced in 2009 and as of now, Bitcoin is the largest cryptocurrency with a market capital of approximately more than 100 billion USD2 [7]. Simply put, blockchain technology is built on three main concepts: a distributed database, a trust protocol and cryptography. In the following subsections we will explain them briefly Distributed database: Built on the concept of peer-to-peer networks and distributed storage , blockchain technology can be considered as a distributed data store with state machine replication using peer-to-peer protocol, where the transactions are the atomic changes to the data store which are grouped into blocks.


Create Wallet

Your Name: Patrick

Email ID: patrickbateman@gmail.com

Mobile No.: 45899234556

http://localhost:8080

0xD37...2c08 : ADD USER

$0.00

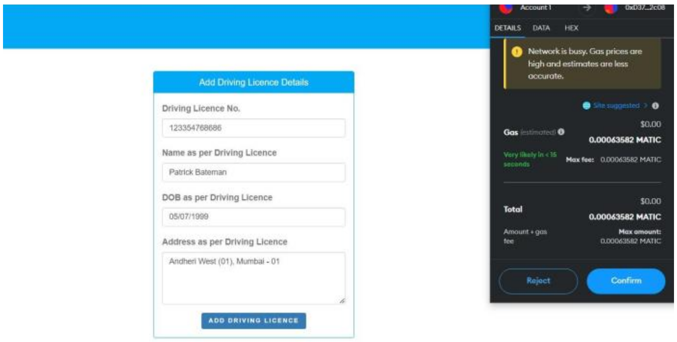
Gas (estimated) $0.00 0.00036665 MATIC

Very likely in < 15 seconds Max fee: 0.00036665 MATIC

Total $0.00 0.00036665 MATIC

Amount + gas fee Max amount: 0.00036665 MATIC

b. Once the wallet is created in metamask a transaction hash value is generated and the details are stored in the polygon scan. Trust Protocol In order to avoid having a central authority for enabling the trust in the system, there needs to be some mechanism that establishes trust consensus of the involved parties.In blockchain trust is ensured through a distributed consensus protocol. Next the user can add its details and can store it using the blockchain.


Add Driving Licence Details

Driving Licence No.: 123354768686

Name as per Driving Licence: Patrick Bateman

DOB as per Driving Licence: 05/07/1999

Address as per Driving Licence: Andheri West (01), Mumbai - 01

Network is busy. Gas prices are high and estimates are less accurate.

Gas (estimated) $0.00 0.00063582 MATIC

Very likely in < 15 seconds Max fee: 0.00063582 MATIC

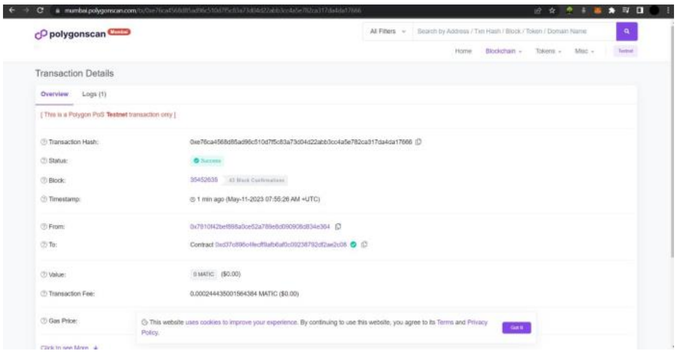
Total $0.00 0.00063582 MATIC

Amount + gas fee Max amount: 0.00063582 MATIC

Transaction sucessfully submited and find below transaction hash

0x7f00949c76f452149c838dd18790ef19a7aa881dd50d9fc0b01c72724c30feba

For each transaction a hash value is generated.



Transaction Details

[This is a Polygon PoS Testnet transaction only]

Transaction Hash: 0xe76ca4568d85ad96c510d7f5c83a73d04d22abb3cc4a5e782ca317da4da17666

Status: Success

Block: 35452635

Timestamp: 1 min ago (May-11-2023 07:56:26 AM +UTC)

From: 0x7810f42be898a0ce52a789e8d090908d834e304

To: Contract 0xd37c896c4fecf8afb6af0c09238792df2ae2c08

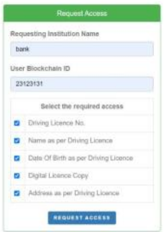
Value: 0 MATIC ($0.00)

Transaction Fee: 0.000244435001564384 MATIC ($0.00)

Gas Price:

This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy.

c. Proof-of-work (PoW) refers to the idea that a service: requester is required to solve a cryptographic puzzle (computational work) to participate in a network and it was initially proposed in hashcash as a countermeasure for denial of service attack using CPU cost functions. In blockchain and especially in Bitcoin, it is used as a verification techniques for finding the appropriate header for new blocks of data and to append them to the chain of blocks.



Request Access

Requesting Institution Name: bank

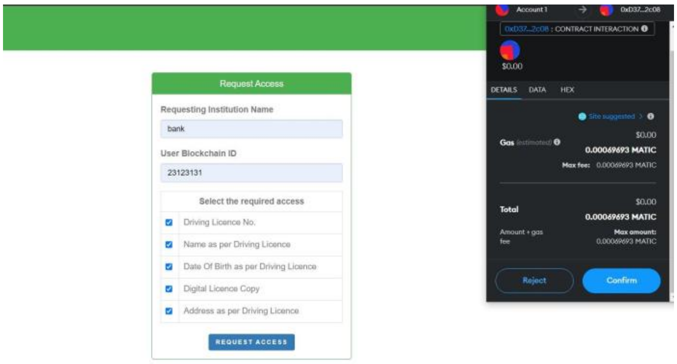
User Blockchain ID: 23123131

Select the required access

☑ Driving Licence No.
☑ Name as per Driving Licence
☑ Date Of Birth as per Driving Licence
☑ Digital Licence Copy
☑ Address as per Driving Licence

REQUEST ACCESS

To add a block, a node has to solve a cost-function (find the right nonce), that results in a pre-defined hash format with certain restrictions. At the same time, blocks can only be added to the longest chain (with the most proof-of-work invested), to avoid ’dishonest’ attempts of altering the ledger.



Request Access

Requesting Institution Name: bank

User Blockchain ID: 23123131

Select the required access

☑ Driving Licence No.
☑ Name as per Driving Licence
☑ Date Of Birth as per Driving Licence
☑ Digital Licence Copy
☑ Address as per Driving Licence

REQUEST ACCESS

Account 1 → 0xD37...2c08

0xD37...2c08 : CONTRACT INTERACTION

$0.00

DETAILS DATA HEX

Site suggested

Gas (estimated): $0.00, 0.00069693 MATIC. Max fee: 0.00069693 MATIC

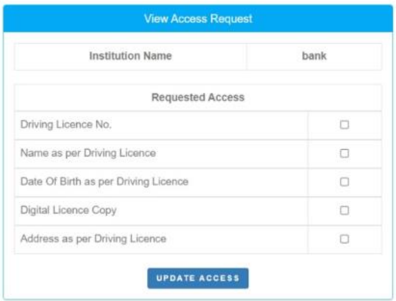
Total: $0.00, 0.00069693 MATIC

Amount + gas fee. Max amount: 0.00069693 MATIC

Reject Confirm

Proof-of-Stake (PoS) is another method for verifying and adding blocks to the blockchain, where the node that creates the next block is chosen. Therefore, a node adds and verifies blocks according to how much stake they have in the system. Thereby, ownership will lead to actors behaving honestly, otherwise they would lose their stake, if they behave dishonestly. Even though there are other anchoring schemes similar to the above, we skip their description due to space limitations..

d. At the same time a request is sent to the user and the respective user can see the institute name and the access requested for the required documents.



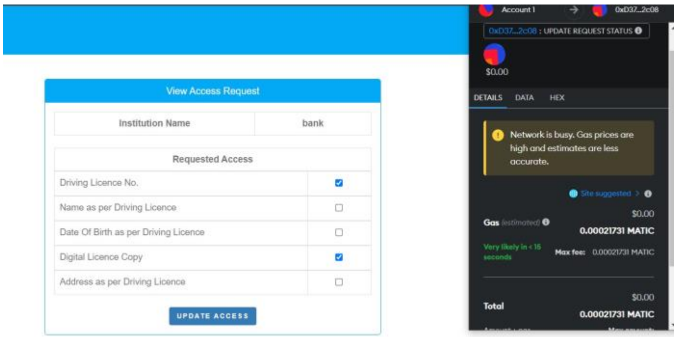
View Access Request

Institution Name	bank

Requested Access	
Driving Licence No.	☐
Name as per Driving Licence	☐
Date Of Birth as per Driving Licence	☐
Digital Licence Copy	☐
Address as per Driving Licence	☐

UPDATE ACCESS

As per the users will it can give the access to its documents and once the access is updated the transaction hash value is also generated.



View Access Request

Institution Name	bank

Requested Access	
Driving Licence No.	☑
Name as per Driving Licence	☐
Date Of Birth as per Driving Licence	☐
Digital Licence Copy	☑
Address as per Driving Licence	☐

UPDATE ACCESS

Account 1 → 0xD37...2c08

0xD37...2c08 : UPDATE REQUEST STATUS

$0.00

DETAILS DATA HEX

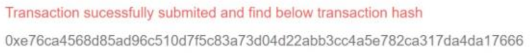
Network is busy. Gas prices are high and estimates are less accurate.

Site suggested

Gas (estimated): $0.00, 0.00021731 MATIC. Very likely in < 15 seconds. Max fee: 0.00021731 MATIC

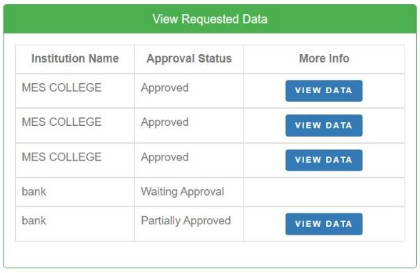
Total: $0.00, 0.00021731 MATIC

e. Once the request is updated by the user the institution can see the granted request documents and the institution can see the documents and can use it for a purpose.



Transaction sucessfully submited and find below transaction hash

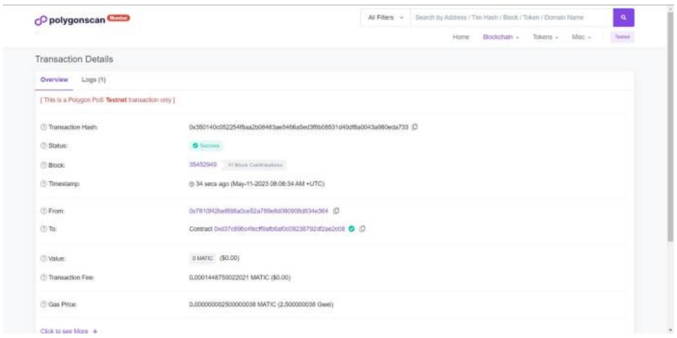
0xe76ca4568d85ad96c510d7f5c83a73d04d22abb3cc4a5e782ca317da4da17666



View Requested Data

Institution Name	Approval Status	More Info
MES COLLEGE	Approved	VIEW DATA
MES COLLEGE	Approved	VIEW DATA
MES COLLEGE	Approved	VIEW DATA
bank	Waiting Approval	
bank	Partially Approved	VIEW DATA

f. This system is developed to securely store the data and because of the security feature the documents of the user cannot be used against ones will.



polygonscan

All Filters | Search by Address / Txn Hash / Block / Token / Domain Name

Home Blockchain Tokens Misc Testnet

Transaction Details

Overview Logs (1)

[This is a Polygon PoS Testnet transaction only]

Transaction Hash: 0x350140c052254f8aa2b08463ae5466a5ed3f6b08531d40df8a0043a980eda733

Status: Success

Block: 35452949 11 Block Confirmations

Timestamp: 34 secs ago (May-11-2023 08:06:34 AM +UTC)

From: 0x7810f42befd98a0ce52a789e8d090908d834e364

To: Contract 0xd37c896c4fecff9afb6af0c08238792df2ae2c08

Value: 0 MATIC ($0.00)

Transaction Fee: 0.0001448750022021 MATIC ($0.00)

Gas Price: 0.000000002500000038 MATIC (2.500000038 Gwei)

Click to see More

4. EXTERNAL INTERFACE CHALLENGES

User Interface (UI): The user interface has two main purposes: firstly, to give an overview over all personal data of the user and secondly, to be able to manage all the data and system functionalities. The system displays all personal data that is stored at any service provider and the respective given consents (e.g. billing, targeted advertising or newsletter mailing), the data selling history and all data that is currently stored on the off-chain repository of the user. The user can manage all data in the same system, which is based on giving and revoking consents to use the data and to access the data. The data is accessed either when it was purchased by a company or when the user identifies himself through the system.

5. CONCLUSION

In this paper, we provided an in-depth review of blockchain-based identity management systems. As part of the review, we identified a number of challenges, such as those related to block data storage. For example, the user's storage requirement will increase 26% with the increase of the number of users and the subscribed services. Hence, how do we design a scalable mechanism that also takes into consideration the differing storage capability of different users?

Another challenge is associated with the de-authorization classification in blockchain. Some nodes can participate in book-keeping while others can only view the block data. This can potentially result in the boundary division of the chain, due to the existence of node identity. Blockchain-based IdM systems overcome a number of limitations inherent to conventional IdM systems. Such blockchain-based systems might be described as an identity revolution. For example, the user becomes the owner of the identity, and it does not require users to sacrifice safety for convenience. In addition, one potential future extension is to adopt some unique factor in reality as a main evidence for account reset.

6. REFERENCES:

[1] G. D. P. Regulation, "Regulation (eu) 2016/679 - directive 95/46," Official Journal of the European Union (OJ), vol. 59, pp. 1–88, 2016.

1)

[2] C. Tankard, "What the gdpr means for businesses," Network Security, vol. 2016, no. 6, pp. 5–8, 2016.

[3] O. K. Foundation and the Open Rights Group, "Personal data and privacy working group," 2014.

[4] A. Poikola, K. Kuikkaniemi, and H. Honko, "Mydata a nordic model for human-centered personal data management and processing," Finnish Ministry of Transport and Communications, 2015.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[6] R. B ¨ohme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," The Journal of Economic Perspectives, vol. 29, no. 2, pp. 213–238, 2015.

[7] S. T. Ali, D. Clarke, and P. McCorry, "Bitcoin: Perils of an unregulated global p2p currency," in Cambridge International Workshop on Security Protocols, Springer, 2015.

[8] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[9] G. Zyskind, O. Nathan, et al., "Decentralizing privacy: Using blockchain to protect personal data," in Security and Privacy Workshops (SPW), 2015 IEEE, pp. 180–184, IEEE, 2015.

[10] N. Kaaniche and M. Laurent, "A blockchain-based data usage auditing architecture with enhanced privacy and availability," in Network Computing and Applications (NCA), 2017 IEEE 16th International Symposium on, pp. 1–5, IEEE, 2017.