Development of Identity Solutions for the Internet

Felix Hildebrandt
BC Development Labs GmbH as Blockchains LLC, Markt 16, D-09648 Mittweida

Mapping identities, digital assets, and people's profiles on the internet is getting much traction in the blockchain cosmos lately. The new technology is currently forming architectures that will further pave new ways to reach fundamental mechanisms to interact in a decentralized, user-centered manner. These schemes are often declared as the next generation of the web. Within the article will be shown, how the internet has evolved in managing identities, what problems arose, and how new data architectures help build applications on top of privacy rights. Both technological and ethical perspectives are viewed to answer which guidelines should be considered to fulfill the upcoming branch of decentralized services and what we can learn from historical schemes regarding their privacy, accounting, and user data.

1. Identity within the common Internet

Homepages could be described as windows into a new world as the internet pushed forward and the initial web appeared in the late 80s. They were mainly used to share knowledge from universities around the world and were read-only pages without user management. Within the backend, the network consisted of servers, forming a mesh around the globe. With the TCP and IP protocol, data transfers between machines were focused on transmitting information to a specific device address. All of the webpage data was stored on servers, and regular private computers could connect and load data from or to them. But the purpose of making information accessible for a wide variety of society was fulfilled quickly, and the urge to interact with computers to exchange personal data grew.

At this time, communication was still more or less done via phone or mail, and email use began to grow. Due to the rudimentary technologies and the inefficient computers, for administrators, it was only possible to determine how many devices saw certain pages and at what time they consumed the content. This disadvantage led to new technology to gain more information about the user in front of the device and simplify the communication process.

When the interaction between computers evolved, the internet was generally designated as Web 2 and fundamentally influenced by the previous questions. From today's perspective, it mainly was a front-end revolution with new browser functionalities, leaving server-centered structures and databases as a backend.

IT security and backup mechanisms increased drastically to manage the throughput and safety of the now most valuable goods: user data. Large server centers had to be built and user files secured from unauthored access because frauds rose. On the user side, cookies and APIs were developed to track users' behavior within sessions and store additional traffic- or user information within the browser. Tracking was in total focus, and cart content, areas of interest, or already seen advertising links were essential for business- with it, also identity management. New use cases like social media, e-commerce, or even interactive knowledge platforms proliferated. A vast market of user data emerged to create intricate user data patterns to optimize monetarization and predict behavior. [1] What started as the era of optimizing profits by tracking users emerged into directly gaining profit from personal information from the user. Price and advertisement align with gathered user behavior. Data analysis is a considerable immense amount of how digital products gain value nowadays. [2, 3]

Looking closer at what identity within the web means, it is mostly just tracked down to the device a person uses combined with several accounts created for almost every software product or service in use. Mostly an email plus the login password. Such an account allows the utilization of a particular utility and is set up as a top-to-bottom connection from the manufacturer to the blended-in user.

The manufacturer is the determiner, holding all of the user's information. A user login to this account just represents a device, entering a service and gaining access to a person's specified information. Such access can be created directly from a service provider or by linking to existing logins from others. The second scheme was specially evolved by huge IT giants such as Google, Facebook, and Microsoft, which have billions of users. Within seconds, they can just log in to multiple services using one main account, increasing convenience but also the risk of losing passwords or whole logins and raising problems if the referred account is not valid anymore or some service provider is currently unavailable.

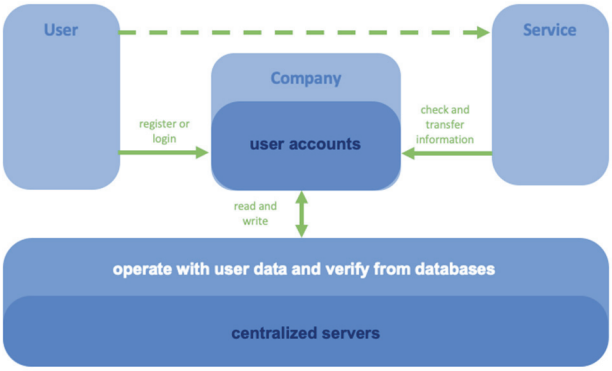

Fig. 1: Regular Web 2 Login Scheme

Many authentication methods evolved to gain authorization from companies or service providers, mainly the OAuth 2.0 protocol. [4] With this scheme, servers can hand out access tokens to users for authentication when using centralized servers on their login. Tokens imply that the user has to put trust in the service provider. However, they can only work with one provider, meaning users need to have accounts for every service in use. Not only do users need to authenticate on multiple token endpoints, but they're also permanently confronted with the man-in-the-middle principle: the intermediate provider can always surveil their relationship activities with the authenticated account to their connected services. Connected logins provide a colossal danger for privacy concerns and attacks that can affect all linked services at once. [5.1]

Another downside: regular schemes just work by transmitting data over device addresses, which can be manipulated or intercepted. The non-existence of a sophisticated identity layer within the internet is one of the primary sources of cybercrime. [5.2]

Further, IBM President Ginni Rometty describes cybersecurity about identity theft as the most splendid profession- and industry-wide threat globally, causing enormous financial and personal damage. [6]

The problem is that the internet was mainly built around machines with their MAC addresses, not for individuals. There is no accurate identity verification- only mechanisms to cover most frauds and give out copies of user rights. With passwords, users gain access to data and services operated and saved on the company's servers. On the other side, documents are digitalized and handed over to third parties, resulting in numerous hoardings of certified copies. It is easy to lose track of who owns, uses, or is up to date on your data because of all the different instances holding parts or duplicates. The scheme quickly shifts control over data to the respective entity, which guarantees its security and legal use. The bureaucracy and needed trust are immense.

Another negative point to mention is that the data is stored on servers operated by the company, meaning it technically belongs to them, even if users own parts of it. [7.1] Even if distortion needs to be done to be compliant with specific laws, if the user gains the right to delete or, more specifically, manage his scraped or purposely put data, it's just a matter of computation power how quickly companies can throughput their data in analytic schemes to get desired advantages. [8] The offset also counts when dodging specific mechanisms to be compliant with rights instantiated from the governments. For the average citizen, it is neither convenient nor user-friendly. At this point, managing all your data and accesses have become a rat-tail of problems.

2. Implementation of Data and Security Laws

The current state also raised issues with informatics ethical perspective, which lends to the General Data Protection Regulation of the European Union in 2018. The GDPR concluded that “everything that helps identify a person, regardless of whether it refers to a natural person's professional, private, or public life”, counts as personal data. [9.1]

The ethical classification is based on this definition and should ensure users full access to their own data management, may it be about critical information or not. User data is collected in any case and is very difficult to be limited. Therefore, the collection of data should not be restricted, but citizens should have full access and transparency regarding the data being collected from and on them.

The General Data Protection Regulation is used to protect the inhabitants of the European Union and their collected data. Data sovereignty must be presented as a fundamental right and guaranteed by all companies in the future. It applies to all citizens, constitutions, and businesses within the European Union. The goals of the GDPR are the protection of natural persons in the processing of personal data and the free movement of such, as well as the safety of fundamental rights, fundamental freedoms, and protection of personal data. Companies need to clearly define what personal data will be stored and which methods are applied to it, in order to be able to protect citizens. [9.2]

In the future, companies will have to continuedly adapt to new regulations. On the way, users will gain more rights to erase data and look up where and when the data was stored. Higher fines and the obligation to notify users in the event of infringements will follow as well. All requirements are always extraterritorial, meaning it is essential from whom the data is and where the data flows, not from where the company operates if servers are located outside the EU. Also, certificates, which verify that certain services and products fulfill the GDPR standards, were discussed. [10] Verification could be an obstacle because the EU has to check up on code and algorithms used within digital services and perform periodic tests. What's already ubiquitous in the food industry could be a lengthy restructuring of digital ecosystems.

Identities can be found in every business, healthcare, government, e-commerce, or future identities in IoT. There is a high relevance in rethinking and changing how data is stored or managed from small companies to big IT giants.

As defined within the GDPR, companies must comply with the data protection rights shown in their checklist. [11] The identity infrastructure is expensive: many companies are still caught up in data ownership lawsuits, ambiguous data sales, and user behavior prediction within gray areas. [3] Because users have the right to manage their data with growing functionality, this will further increase. Users already have the right to prevent the collection of certain data and force its deletion. [12] The wording clearly defines that the data collected is owned by the users, and people can allow access if they wish to do so. Despite the existing Data Protection Regulation, not all companies fully adhere to the established rules or make it nearly impossible due to very cumbersome navigation. If companies provide more transparency, users will gain more possibilities for objection regarding personal data and user profiles. It also disclosures the sources and origin of the data. These aspects can limit the quality of Big Data processes if users deny the gathering of specific data streams. However, it is the right step to gain a fair interaction and comply with human rights without changing backside structures. It strengthens customer loyalty and significance of analysis simultaneously.

3. New Approaches on Digital Identities

Within the blockchain space, the adage "not your private key, not your coins" became public. [13] If this would be applied as common sense facing the current web 2, it could be translated into "not your service, not your data." Even with regulations and the right over data, you can never be sure how the data has been used or utilized until you force deletion.

The goal of decentralized identity is to image rights and identifications of identity reliably and give the people back their data's power. For this to happen, it must be defined what an actual online identity means. As individuals in the real world, persons share relationships. Both are individual operators, and the relationship doesn't belong to anyone, as it's the connection between them. Looking at the current Web 2, it is the opposite: companies and services operate identifiers of user's identities and manage the personal data they are giving away. As the previous chapter told, users never have their own identity or sovereignty. Citizens just gain more rights to access certain functionalities of their instantiated datasets at most. It's a very high workload for every party involved to comply with or check up on personal data. Web 3 concepts will make it much more efficient to comply with regulations because they are built on privacy rights and offer digital identities which have relationships like in the offline world, where nobody relies on each other. Users can just verify other participant's datasets by proving their verifiable credentials when asked.

The term Web 3 is already common sense when looking into the future, defining a more decentralized way how the internet works by using decentralized blockchain networks that act as the enablers but also processors behind. The new generation of web develops a bit more gradient than the previous, because for the first time, the fundamental backend technology of the internet is tackled. The unbeatable factor here: For the first time in history, actual digitally values can be signed, transmitted, verified, and used between global instances. Private and public keys are used to secure the connection between such parties. The cryptography within such networks has the power to abandon previous centralized server approaches for safer user-centric technology, without the need to trust intermediaries.

New concepts rely on decentralized peer-to-peer networks forming unified ledgers. This approach not only introduces more resilient and secure blockchain networks: the governance of software systems will also fully depend on protocol consensus from the blockchain itself, instead of large instances bearing power. Such networks also drastically lower system administration and IT security costs for companies because users hold their identity data independently. On top of that, transparency is a significant aspect.

When running decentralized applications, there is a huge trend to make source code public so everyone can adopt and build with it. Transparency comes from raising the level of trust participants have in the network or application and forming the governance of such. [14]

Not only are future identity solutions transparent, but they will also store most data on devices within wallet applications, pushing self-sovereignty even further. Sensitive Data will likely be stored off-chain, just releasing hashes as verifiable credentials onto the blockchain itself. Actions on the ledger can be executed by referring back to an actual address of an account, not only commands transmitted by a particular device as we used to know from Web 2. Within such an approach, multiple software systems can request the verification of one piece of public data or hashes from offline information. Publicly available encrypted files also solve data duplication. [7.2]

All features bring a lot of responsibility back to the user. Therefore, more user-friendly concepts need to develop over time for a seamless transition. As Alex Preukschat and Drummond Reed describe, the concept of Self-Sovereign Identity, SSI in short, is "the best overall analogy because it's how we prove our identity in the real world: by getting out our wallet and showing the credentials we have obtained from other trusted parties. The difference is that with decentralized digital identity, we are doing this with digital wallets, digital credentials, and digital connections." [5.3]

As already mentioned, blockchain technology offers the exchange of digital values by using digital signatures from one wallet to another. This value can be anything from fungible cryptocurrency to non-fungible credentials, artworks, documents, and so on.

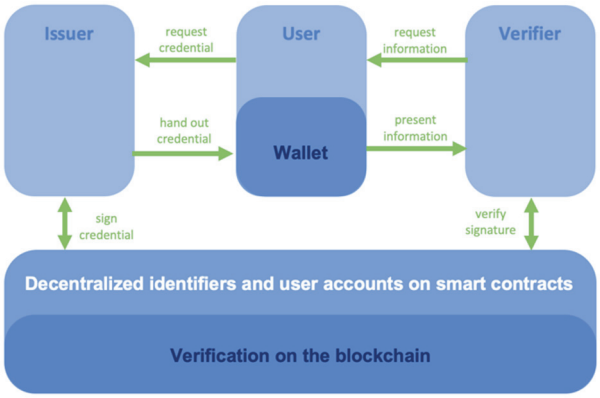

Fig. 2: Web 3 Identity

There are three main roles within the network: a issuer, a verifier, and the user itself. As in the real world, the user has the owned wallet and requests a credential from the issuer. The individual, therefore, may need to give additional data to him. After the request is fulfilled, the issuer signs a credential on the blockchain, referred to the user's address, and issues the new credential to the user's wallet. With the issuers signature and proof that he holds the identity-related data in his wallet, the holder can now use services that need those certificates. For instance, he could use a passport handed out before an exchange. The verifier, in this case, the exchange provider, will request the newly acquired value and verify its signature, before the exchange is transacted. For this to happen, the user needs to present the credential to him. [15, 16]

Some examples of use cases can further help understand its potential on top of it. For e-Commerce, registration and payment could be made directly through the SSI, evading passwords and accounts. All receipts could be handed out as credentials and are written into the blockchain. For finance, citizens could demand any bank service on the fly, eliminating bureaucracy and submission of the same forms. If both parties support SSI interfaces, they can exchange their required credentials and even use multi-signature for essential documents and high value transactions. Health documents could also be shared instantaneously with clients, friends, or nurses within healthcare, providing consent for medical procedures. Because of the blockchain, there could also be lifetime histories of vaccinations, which can be verified or shared with other instances.

For traveling, boarding passes and checkpoints of trips can be documented to verify places visited in the past, and calculate hazard potentials. Even tickets for airlines, hotels, trains or music could be automatically connected to someone's wallet. [5.3]

As the last example, different interpretations of SSI could be used to fully digitalize grade certificates, file transfers, and cross-university or even transnational IDs within the education field. Currently, one colossal driver is Educhain. [17]

Like in the real world, both sides will always show their verifiable credentials to ensure instances are the ones they claim to be. As expected, every example could be managed directly from the smartphone, fully self-sovereign, if all participants accept one ledger system. Decentralized solutions are always tied to network effects. If only a minority of services uses SSI, it could be an obstacle. The needed network effect is an enabler for cross-chain solutions like Polkadot to connect transactions of wallets and contracts to fit into one huge SSI ecosystem. [18] An obvious downside also is that data cannot be verified offline. This could be solved by making the internet accessible to every corner of the world from satellite meshes. Such a principle is currently in an early release from Starlink. [19] The final problem could be seen as the management of keys for wallets, which are needed to operate the SSI software. One solution to this topic will be solved within the next section.

4. Contract-Based Accounting

Within the future, users could freely manage a lot of digital information about themselves. For people, there needs to be proper accounting and ordering of all glimpses of verifiable credentials. That's why even user profiles on the blockchain are in transition. Regularly, users just have wallets to interact within the blockchain for simple transactions. But there are also smart contracts, which can add a lot more functionality: scripts running on decentralized virtual machines from blockchain networks, that act like regular applications. Such smart contracts can be referred to as a decentralized "world computer" where blockchain nodes collectively provide the machine's power. [20] They can execute programs, and map user accounts or profiles as known today. More complexity mostly comes with additional functionality and defines a huge step to get closer to the initial defined goal of Web 3 identities.

By using this computation power, which is triggered when certain network transactions were sent, complex business logic can be mapped on top of it, starting chains of smart contract code execution. With the help of such, even multiple wallets from different devices can be combined to user accounts on fully manageable identity ecosystems. All devices or wallets connected to one account can then speak as one combined identity, enabling role- and right- as well as separated key-management.

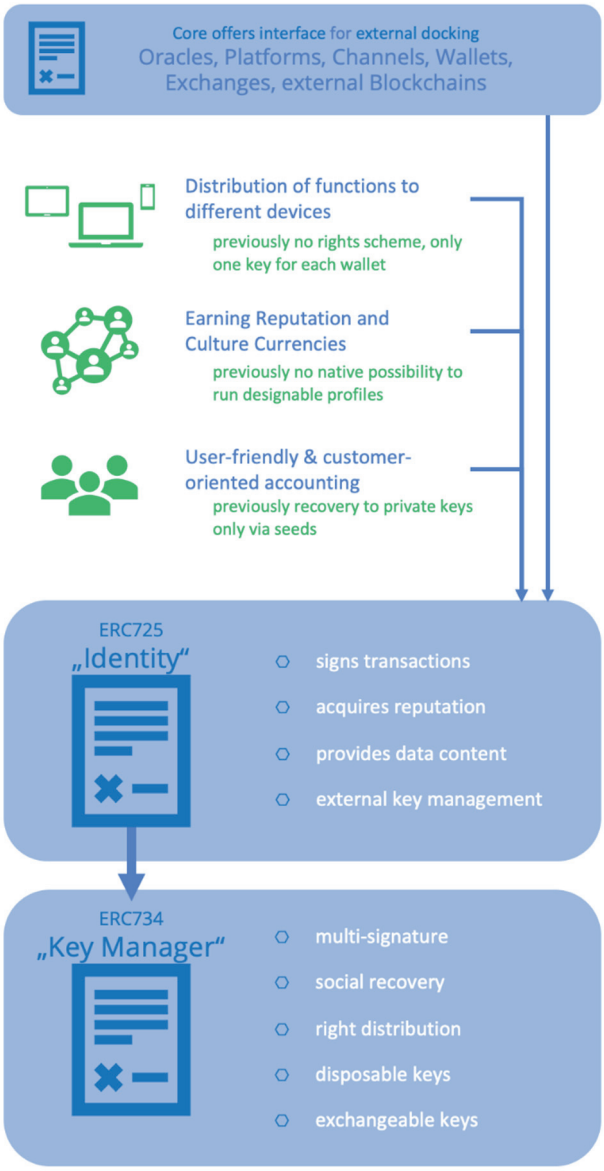

Fig. 3: Contract-Based Accounting

This single contract account can then manage all kinds of digital assets, currencies, etc. Even security contracts could be interposed to reverse accidental transactions back to the initial situation. The clue here is that actual data can always be hashed and written into smart contracts, acting like profiles. As for the identity controller, the owner can encode the attached secret information with all its keys in the value store of the contract. This way is more user-friendly than regular blockchain solutions, because of the more accessible backup and recovery schemes with such key management. The initial idea of contract-based accounting was already discussed within the early days of Ethereum in 2014. However, it was dropped because of the early smart contract functionality's complexity, key security, time-limits and black swan potentials. [21]

In 2017 identity was first standardized as ERC725 on the Ethereum blockchain and further developed afterwards, as seen in figure 3. [22]

Because of the utilization of the Ethereum blockchain, mainly coming from the DeFi space [23], it would be too expensive to realize contract-based accounting nowadays. Complex contracts have to include lots of transactions and all of them need to be covered with expensive fees. Even grand scaling schemes like the rollup technology [24] or sharding [25] won't solve that much throughput if every human being or device's identity is managed within one blockchain system.

Scalability issues are why the term "blockchain of blockchains" evolved. The scheme describes a network where blockchains can connect with each other. Those connections could be similar to the internet, which grew larger with more and more connected servers. Within the Web 3, branches likely will need to split apart in different networks.

With this idea in mind, Lukso was founded in 2018. [26] Creating an ecosystem for new smart contract standards and revealing the possibilities of user accounts and their identity for the creative economy are the project's primary goal. The network will be tackled by using universal profile structures known from social media. It differs from personal identities, often meant in SSI development, and creates public personas with the same functionality, holding any kind of digital art or unique NFTs. While shifting around smart contracts behind the scenes, users can add credentials, links to other networks, or functionalities for different apps. This could be perceived as a light identity management system and a new era of self-sovereign social media platforms. The system could also be used for decentralized login mechanisms for software services. [27]

In comparison to the regular servers used to log in, data loss or downtime can be eliminated with blockchain networks, if their nodes are decentralized around the world. Even personal identities could, at some point, be linked to universal public profiles as hybrid SSI solutions, while only gaining access to personal off-chain data via on-chain logins. With the ERC 1056 standard, the Ethereum ecosystem already has its solution for personal off-chain SSI data, linking public keys from users to them to utilize identity references. [28]

5. Guidelines for Decentralized Development

The famous question is how to define ethics and principles by which we can assess software services operating with user data, e.g., their identities. The GI, an IT representative in Germany, offers prefabricated guidelines by which standard software should develop and evaluated. The GI is the largest German non-profit professional society that has set itself the goal to promote computer technology. It has 20,000 members and counts as a member of the Council of the European Societies for computer science. The guidelines have been designed so that professional ethics or moral conflicts are objects of joint reflection. The instructions are intended to provide guidance to design, create, operate, or use IT systems.

Because of the user data-related topic, the guidelines are linked to the SSI context.

The programmed software should be designed and legally verified by people that possess current and comprehensive expertise. Within the blockchain space, programmers should have deep knowledge about the network and governance they build on, as well as their smart contracts. At the same time, constructive criticism is needed, which is amplified through the high transparency within Web 3. For the exchange of information, good communication skills are necessary to evaluate solutions, communicate them to other people, and simplify them to an abstract level. In this topic, permanent training in the subject should be necessary, especially on new approaches and news on decentralized identifiers and verifiable credentials. Developers also need legal competence when working with tokens or user data within the blockchain space.

Companies bear social responsibility and impact because identities will work and live within new blockchain accounting systems. In this regard, users and builders will contribute to socially acceptable and sustainable solutions. [29]

Developers have to adhere to the principles of ethics about data protection. They should ideally also build their applications on them, not with them. When collecting large datasets with unique content, as "big data" applications do, the National IT Summit has designed its own guidelines. These principles can be summarized in the following sections and transferred directly to the development of SSI software. [30]

Consumers and users must be aware of the purpose or benefit of the application, its processing, and the amount of data collected. They must also be notified when data is transferred to third parties.

The transparency of this information is needed to ensure self-determined actions. Secondly, users have to approve the usage of data, need to see their collected data as well as resulting evaluations. They must also explicitly agree with the linking of data and transfer of information.

The software only has to gather the minimal required data, which is indispensable to reach the solutions target. On this topic, anonymous or pseudonymous data has to be preferred. It also has to be regularly checked for responsible handling of the personal data and that no violation of rights and interests has happened. If so, users also need to be transparently informed about it. The data should never be processed for ethically or morally dishonest purposes and evaluations, links, or data transfers must not harm users nor their possibilities. [30] To summarize, there are many ways to collect data, but a clear line is drawn when the user shows dislike or harms the user instead of adding value. [9.3]

Ethics also cover how the software is instantiated and brought to the user base. As already told in the last chapter, total transparency, e.g., open-source code, is mandatory when identifying solutions that claim to be self-sovereign. Users must have the right to prove and modify their digital identity software. As this right is given, the identity owner's use case possibilities further increase. The analogy can be drawn to the real world of social behavior.Within a modern democratic government, citizens as individual human beings can rely or demand on their rights and human dignity. Anyone can express freely, and the political opinions of the majority are taken into the main focus when developing future governmental plans. To relish everyone's rights and eliminate upcoming problems, citizens must work as a union to provide and establish bright, reflected futures. This approach also reduces the risk of exploitation from corporations, so that individuals can move on in life with fewer boundaries. We should build fair digital systems like we do in the real world: empower individuals, and form strong relationships while remaining fully independent. Therefore, it is necessary to promote the open-source development of self-sovereign identity. [5.4]

6. Current State of SSI and Outlook

The significant advantage of Web 3 with its user-centered approach is that it represents human interaction-like relation between digital software services. When connected to blockchain networks SSI's, it can unfold their true potential. The network is fail-safe, decentralized, executes actions on its store of value all in one. On the negative side, accurate SSI accounting is in its early age and not as fast and scalable as centralized services. Creating complex schemes on SSI-based components requires a lot of transactions when instantiating. On top of that, even identity standards have not found significant adoption by now. In 2018, Nick Poulden first released a fully functional prototype on the first version of the ERC 725 identity standard on Ethereum. [31] It was a huge success, seeing the technical concepts being brought to life. Ethereum is currently trying to create its standalone login functionality, and so it is expected from multiple other blockchains.

For the development industry, SSI is understood as the new hype. There are plenty projects directing into different areas: may it be strictly private identifiers, public profiling or hybrid variants. Many research facilities are working out various concepts and protocols for citizenships, student organization, financing-, travel- or new social media, etc. The key will be interoperability, which is difficult to determine, because of the rough standartisation being done by now. [15, 16]

Mass adoption will most likely be gradual because existing solutions are convenient and currently functional to use. An additional downside is that the technology needs to be brought to the issuers across all industries, mainly governmental or old established instances. Both, issuers and users need to accept the same ledger so that

verifying instances can prove their verified credentials. It has to be said, that it will require great products to change the industry. Overall, SSI is just facing the start of a new century of how digital relationships are managed.

Acknowledgements

Special thanks to BC Development Labs GmbH as Blockchains LLC which supports my research, and practical work as well as giving me the opportunity to build meaningful and up to date software which will be used in future development.

References

[1] Kaushik, A. (2010): Web analytics 2.0. The art of online accountability & science of customer centricity. Hoboken, N.J.: John Wiley (Sybex serious skills).

[2] Patel, N. (2019). The future of AT&T is an ad-tracking nightmare hellworld. The Verge. Retrieved August 31, 2021, from https://www.theverge.com/2019/5/22/18635674/att-location-ad-tracking-data-collection-privacy-nightmare

[3] Bernet, D. (Director). (2015). Democracy [Documentary]. INDI FILM.

[4] Parecki, A. (2021). OAuth 2.0 — OAuth. OAuth.Net. Retrieved August 31, 2021, from https://oauth.net/2/

[5] Preukschat & Reed, A. & D. (2021). Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials. Manning Publications Co. 1) p. 9; 2) p. 4; 3) p. 10; 4) p. 285

[6] Morgan, S. M. (2015, November 24). IBM's CEO On Hackers: "Cyber Crime Is The Greatest Threat To Every Company In The World." Forbes. Retrieved August 31, 2021, from https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/

[7] Voshmgir, S. (2020). Token Economy: How the Web3 reinvents the internet. Shermin Voshmgir. 1) p. 32; 2) p 27 ff., p 95 ff.

[8] Mitchell, J. (2019). The Evolution of the Internet, Identity, Privacy and Tracking – How Cookies and Tracking Exploded, and Why We Need New Standards for Consumer Privacy – IAB Tech Lab. IABTechLab. Retrieved August 31, 2021, from https://iabtechlab.com/blog/evolution-of-internet-identity-privacy-tracking/

[9] GDPR-Info.eu. (2021). Datenschutz-Grundverordnung: DSGVO als übersichtliche Seite. Datenschutz-Grundverordnung (DSGVO). Retrieved August 31, 2021, from https://dsgvo-gesetz.de/. 1) ch. 1 art. 4; 2) ch. 1 art. 1-3; 3) ch. 2

[10] Keithahn & Conway. (2020). DSGVO: Zusammenfassung und Ausblick. Mailjet. Retrieved August 31, 2021, from https://www.mailjet.de/dsgvo/?gclid=EAIaIQobChMIx9nyhb7S5QIVgrTtCh3y9g2VEAAYAiAAEgLdIPD_BwE#was-ist-dsgvo

[11] GDPR.eu. (2019). GDPR compliance checklist. Retrieved August 31, 2021, from https://gdpr.eu/checklist/

[12] Wolford, B. (2020). Everything you need to know about the "Right to be forgotten." GDPR.Eu. Retrieved August 31, 2021, from https://gdpr.eu/right-to-be-forgotten/

[13] Ledger Academy. (2020). Not Your Keys, Not Your Coins: Why It Matters. Retrieved August 31, 2021, from https://www.ledger.com/academy/not-your-keys-not-your-coins-why-it-matters

[14] Simon, A. (2018). Blockchain evolution: A quick guide and why open source is at the heart of it. Opensource.Com. Retrieved August 31, 2021, from https://opensource.com/article/18/6/blockchain-guide-next-generation

[15] W3.org. (2019). Verifiable Credentials Data Model 1.0. Retrieved August 31, 2021, from https://www.w3.org/TR/vc-data-model/

[16] W3.org. (2021). Decentralized Identifiers (DIDs) v1.0. Retrieved August 31, 2021, from https://www.w3.org/TR/did-core/

[17] Educhain. (2021). The issue, Share and Verify Any Academic Record Digitally. Educhain.io. Retrieved August 31, 2021, from https://educhain.io

[18] Wood, G. (2016). Polkadot Whitepaper. Polkadot. Retrieved August 31, 2021, from https://polkadot.network/PolkaDotPaper.pdf

[19] Crist, R. (2021). Starlink explained: Everything you should know about Elon Musk's satellite internet venture. CNET. Retrieved August 31, 2021, from https://www.cnet.com/home/internet/starlink-satellite-internet-explained/

[20] Buterin, V. (2014). Ethereum whitepaper - whitepaper.io. Ethereum. Retrieved August 31, 2021, from https://whitepaper.io/document/5/ethereum-whitepaper

[21] Recksiek, M. (2021). Fabian Vogelsteller über NFTs, LUKSO, Krypto & die Zukunft. YouTube. Retrieved August 31, 2021, from https://www.youtube.com/watch?v=KYoBJq9lA3w&ab_channel=Bitcoin2Go

[22] Vogelsteller, F. (2017). ERC: Proxy Account · Issue #725 · ethereum/EIPs. GitHub. Retrieved August 31, 2021, from https://github.com/ethereum/EIPs/issues/725

[23] Varshney, A. (2021). Ethereum and DeFi are forcing smart contract platforms to evolve. Cointelegraph. Retrieved August 31, 2021, from https://cointelegraph.com/news/ethereum-and-defi-are-forcing-smart-contract-platforms-to-evolve

[24] Interdax. (2020). Scaling Ethereum on L2: Optimistic and ZK-Rollups | Interdax Blog. Medium. Retrieved August 31, 2021, from https://medium.com/interdax/ethereum-l2-

optimistic-and-zk-rollups-dffa58870c93
[25] Ethereum. (2021). Shard chains. Ethereum.Org. Retrieved August 31, 2021, from https://ethereum.org/en/eth2/shard-chains/
[26] Vogelsteller, F. (2018). Lukso Whitepaper. Lukso Network. Retrieved August 31, 2021, from https://lukso.network/assets/LUKSO_Whitepaper.pdf
[27] Patel & Sahoo & Mohanta. (2019). DAuth: A Decentralised Web Authentication System using Ethereum. Reseachgate. Retrieved August 31, 2021, from https://www.researchgate.net/publication/337513916_DAuth_A_Decentralized_Web_Authentication_System_using_Ethereum_based_Blockchain
[28] Thorstensson, J. (2018). ERC: Lightweight Identity · Issue #1056 · ethereum/EIPs. GitHub. Retrieved August 31, 2021, from https://github.com/ethereum/EIPs/issues/1056
[29] GI. (2021). Unsere Ethischen Leitlinien - Gesellschaft für Informatik e.V. Gesellschaft für Informatik e.V. (GI). Retrieved August 31, 2021, from https://gi.de/ueber-uns/organisation/unsere-ethischen-leitlinien/
[30] Nationaler IT Gipfel. (2015). Leitlinien für den Big-Data-Einsatz im Überblick. Digitale Technolo-gien. Retrieved August 31, 2021, from https://www.digitale-technolo-gien.de/DT/Redaktion/DE/Downloads/Publikation/Smart_Data_Positionspapier_BigData_Leitlinien.pdf?__blob=publicationFile&v=7
[31] Origin Protocol. (2018). ERC 725 Demonstration. YouTube. Retrieved August 31, 2021, from https://www.youtube.com/watch?v=jjUKWRK8H2g&feature=youtu.be