The future of soulbound tokens and their blockchain accounts

Felix Hildebrandt
LUKSO Blockchain GmbH, Köpenicker Chaussee 3a, 10317 Berlin

The topic of soulbound, non-transferable tokens is getting lots of interest within the blockchain space lately as decentralized societies become more tangible with Web3 social media applications and DAOs. In this article, I want to outline how such tokens function, their problems for adoption and standardization, and how they differ from verifiable credentials in the SSI field. As such soulbound assets will likely rely on extended recovery and asset management schemes to become viable identities that safely gain reputation and trust, features like social recovery and contract-based accounting are incorporated. By combining those new technologies and the theoretical crypto-native identity construct, the paper will give an impression of the future user-centric data economy.

1. Current NFT Landscape

NFTs are non-fungible, tradable tokens primarily used to represent something of monetary value, but use cases for documenting attendance, skills, and accomplishments have become more prevalent. These tokens are attestations to specific individuals and hold value similar to diplomas, certificates of achievement, or even reputations gained through interpersonal interactions. This use case reveals an issue with current NFT standards: they are transferable and cannot be bound to a specific individual. As Vitalik Buterin discussed [1], today's NFTs are tradable items that can gain value and inevitably become a signal of wealth, even when it is not the original intent.

2. Soulbound Token Functionality

Unlike regular NFTs, soulbound tokens (SBTs) are a concept of non-transferable assets. Once issued, they belong to a specific identity. They cannot move to a new address (without social recovery) and cannot be traded for a different asset. However, they can represent specific values. Soulbound tokens mimic special certificates, accomplishments, accurate proof of attendance, or social interaction graphs that cannot stem from another identity. Issuers of these tokens "are not interested in whether or not you paid someone who attended some event. They are interested in whether or not you personally attended that event." [1]

Bound tokens could be issued by the same account, acting as a post or information about themselves, but also attested or shared by other individuals or institutions. A Web3 attestation flow [2] would enable self-sovereign acting users with attesters and verify instances around them. Handing out such soulbound tokens from others to user accounts would enable bound airdrops from communities or a DAO controlled by accounts with certain SBTs instead of votes that could just be traded, building much stronger bonds within communities.

2.1 Issues with non-transferability

The decision POAP [3] made when creating their attendance token ecosystem breaks down the problems faced with developing bound tokens.

1. Users might have good reasons to migrate their assets to a different wallet for security concerns. Externally Owned Accounts (EOAs), the most prevalent blockchain wallets currently used, are bound to one single recovery phrase that cannot be changed if compromised. That's due to their minimal key-based [4] nature. Users would face the loss of their non-transferable tokens if these accounts became inaccessible or compromised.

2. Users could create a custom smart contract with a transfer or ownership function to hold the bound NFT. With such wrapper contracts, users could sell or trade the asset's "shell" instead of the non-transferable NFT if transfer functions are limited to one or static within an NFT's constructor.

Transferability has led to exploiting tokens that are not meant to be transferred, like secret drops or whitelist spots. One could argue that services that rely on those NFTs can verify ownership by checking if the asset has been moved, but there are further issues:

3. SBTs on EOAs could not exist without external proof and reissuing services. Imagine a user who wants to update their address. They would need to verify that they are the original identity of both the current and the new address, denying that the SBT has not been sold. It would require a dependency/process to authenticate. Such a service is provided by the Proof-of-Humanity attestation service [5] but might get complicated against non-human identities. However, even more cumbersome, every attestation service would have to implement an interface to either burn/reissue or transfer the SBTs, which will cause a tremendous number of transactions for rich histories of interactions.

4. What if only the owner of the anonymous smart contract wrapper has changed without transferring the NFT that it holds? Depending on the management of the roles of such a smart contract, the traceability of SBTs can become unmanageable, as people may just set up a non-standardized and non-bound shell around them.

The conclusion: Soulbound tokens are not easy to implement because they must be issued to specific identities that have met a particular prerequisite, which requires customer verification (KYC) or an established social construct. Once the framework is more tangible, prototypes will likely test different attestation aspects and protocols.

Here, modular standards [6] (LSPs) mainly developed by LUKSO for now, can solve some issues by replacing traditional EOAs with smart contract-based accounts built around the ERC725 Proxy Account [7] standard. Such can contain metadata for storing verifiable information or claims of identities and only use EOAs as their controllers. An example would be Universal Profiles [8], which can have descriptions, pictures, assets, and more data attached. Through a key manager, the account can be controlled by multiple keys with individual permissions, safely allowing numerous devices and services to restrict control of the identity. Unlike key-based accounts, contract-based ones can update security without losing tokens or relying on third parties to reissue assets. Services could only hand out non-transferable tokens directly to Universal Profiles if they prove their ownership through controller keys. Especially such an interface detection for universal contract standards further limits the use of wrapping up assets.

In theory, the only edge case remaining is setting up an abstract identity from an anonymous profile when buying an asset that starts gaining an honest reputation after the first (and final) SBT trade. For example, a Universal Profile that stays anonymous to get some SBTs. Since it cannot secretly sell the SBTs, it sells the whole anonymous account to someone instead. The buyer could change the keys, fill his profile with correct information, and act truthfully. The only remedy would be attesters introducing precautions.

2.2 Hybrid types for extended management

SBTs could also implement a revoke function for issuers or communities, where tokens are initially revocable and transferable before transitioning into a strict non-transferability. To ensure tokens are not financialized and sold to a different party, or if keys are lost or stolen, the issuer could burn and reissue (or transfer) the token to a new wallet. Such hybrid forms could also bring lots of value when proving if the user has authentic community membership or is new to Web3 and does not have his final account set up. Tokens or memberships could be easily revoked within a probationary period or after a duration of unexplained inactivity.

The more SBTs the account has, the easier it would be to prove the identity belongs to that address, thereby confirming the legitimacy of reputation-based NFTs and SBTs held within the account. These systems serve social media purposes, similar to a resume for job applicants. Instead of proving work experience and the completion of assessments, SBTs allow for the growth of online reputation as a means for being recognized and taken seriously. If there is only one SBT and an account with few interactions, it will become difficult to distinguish between honest members and blenders. Uncertainty may lead to actual engagement counters or metrics, as an SBT is only as good as its strict hand-out process and trusted issuer.

2.3 Cutting dependencies

Even if there is no standardization for SBTs yet, the concepts are slowly becoming tangible. Web2 was never built around sovereign identities; instead, machines with their device address connected to central servers and having their data managed and held by external services. [2] Even if Web3 could solve such dependencies in the future, it currently still lacks primitives to represent social identities in the first place. Most blockchain projects have become fundamentally dependent on Web2 or are using Web2-like structures in the backend. Some examples of the dependencies we face:

1. Since EOAs cannot represent profiles independently, NFT artists rely on centralized platforms like OpenSea and Twitter to commit to scarcity and initial provenance and act as authenticated projects. EOAs do not have data attached; they only serve as an address to hold assets and sign data with a private key so that outsourcing appears justified.

2. DAOs that try to move beyond sellable coins for voting often rely on Web2 profiles to authenticate and ensure Sybil resistance. Faucets or quota systems face the same issue. Using the Ethereum Name Service (ENS) as a Web3 equivalent mainly depends on a paid subscription [4], but also just acts as a sellable NFT held by an address.

3. Many Web3 participants rely on custodial wallets managed by centralized entities like Coinbase or Binance. Decentralized key management systems are not user-friendly and lack the functionality to act on happened transfers for tokens or NFTs, making it super hard to manage assets even before building more complex data economies like social media applications.

4. Most services gathering asset information about an account rely on centralized projects like Etherscan since services cannot easily read data directly from the network or smart contracts.

The common sense of criticism directs to the conclusion that there need to be multiple standards between the token and its account to enable convenient and decentralized societies, leading to the next question.

3. What is a soulbound token without a Soul?

Souls as token enclosures in outlined decentralized societies could represent humans, machines, organizations, or anonymous or fictional personalities- anything that requires an identity and a reputation bound to them specifically. An identity has little value without external attestations of abilities, qualities, and character- the building blocks of reputation and trust. SBTs can represent these attestations for Web3 identities, but unlike most tokens today, they hold no value without this bond to an identity instance, e.g., "Soul."

It is crucial not to restrict what a Soul is and what it could become. Through Proof of Humanity [5], a human Soul might be able to expand the field of decentralized finance (DeFi) services into undercollateralized lending. SBTs could represent "digital twins" of real-world assets or other requirements from the DeFi world. But one might also gain a reputation in other communities by having a fictitious identity, as seen by the movement of Web3 communities where NFTs act as entry points to gated communities. SBTs could enable new horizons within public or private communities for both sides.

Still, Souls as regular EOAs make it hard to enable the full capability of SBTs in a decentralized society:

1. There is no standardized way of attaching data directly to the account other than by holding or owning an external contract that might be transferable.

2. There is only one backup seed for each account, and people could quickly lose their Souls and assets. This lack of security is especially problematic for individuals with valuable assets and cross-app reputations stored on one account. Users should not hold their whole identity or Soul on one single, static backup.

3. There is no structure to owning multiple social graphs or tokens with one identity. Every NFT is just thrown onto one address, which can be chaotic without Souls for every service.

4. They lack convenience. EOAs need funds before interacting with anything on-chain, cannot accept or reject transactions, cannot store data themselves, and do not store their set of owned assets in a decentralized, automated way.

In conclusion, SBTs do not directly bring more people into the blockchain ecosystem; it is the framework that surrounds them. Extended account functionalities and convenience are needed for new use cases and mass adoption. Souls must function as a user-centered identity manager, not just a simple token enclosure.

4. Mainstreaming contract-based accounts

As mentioned before, LSPs could be seen as a game changer for decentralized societies. Since 2020 the LUKSO project has been actively building standards to simplify and improve the blockchain experience. It could become the perfect framework for Souls, even without initially considering SBTs. In detail, the combination of an EC725 Proxy Account [7] and LSP2 Storage Schema [9] lets a basic EOA evolve into a contract-based identity that features attaching rich information to it in a unified list scheme that is easily parsable and expandable. This could become useful for direct claims or attached assets on the ERC725 Account. [6] LSP3 [10] further transforms the account into a Universal Profile, adding public data like images, names, tags, and descriptions. With the LSP6 Key Manager [11], a Soul could easily update and upgrade the security to swap out or manage multiple keys and define specific permissions. By having a Storage Schema, the frame of the SBT could already have its metadata before attaching anything to it. It would enable identities to start gaining some initial reputation and interact with each other in an easily accessible way, which is especially needed to go beyond the current Web3 adoption.

In combination, the ecosystem of LSPs [4] will remove numerous dependencies and bring more convenience. For instance, The LSP1 Universal Receiver [12] is a standard for transaction handling that could be used to reject or approve tokens. The feature is not only convenient, but it also allows for the safe listing of specific accounts. The ability to deny specific soulbound tokens and social interactions is vital in the context of Souls, as SBTs are ideally forever connected to an address.

4.1 Social Media adoption for Web3

LENS [13], a popular blockchain social media protocol, can serve as an example that further outlines the burdens of EOA-Souls. The project uses EOAs to receive an NFT that mimics account profiles. Using NFTs as profiles has considerable disadvantages. The social media identity is not only attached to a static EOA key but also uses regular transferable NFTs, which means Souls purely rely on data from held assets instead of data being directly attached to the account. Not just profiles, but also interactions (posts, follows, comments, or reposts) are represented by an NFT. Since there is no functionality to accept or deny incoming assets, bot accounts could register handles, follow spam channels and send NFTs representing a follow to other accounts, which would propagate the unapproved content within their feed. This spamming could get even worse if spam attesters handed out SBTs. Therefore, prompt or discard by default should be common sense when introducing future SBTs. By using the NFT method, multiple profiles could also be sent to one EOA, making them unusable with any social graphs, as their interactions are not linked directly. Uncontrollability of asset transfers may be why Aave, initiator of the protocol, is hesitant to issue handles.

Even for the organization of assets and attached services, LSP9 offers Vaults [14] that mimic profile subfolders or separated wallets, keeping NFTs well organized and enabling services to read and write contents from or to certain sub-contracts. This categorization might

become essential long-term when things like social media posts fill up accounts with thousands of NFTs. For SBTs, it has to be said that such Vaults would also need to be bound. Without proper organization, searching for a token from the past becomes unwieldy. This chaos can already be seen on some OpenSea profiles of larger LENS accounts: it quickly happens to lose sight, which will only get messier for future social graphs. Like subdomains on ENS [15], Vaults could be the best solution for these organizational issues. The read access to Vault contracts would further allow users to focus on enjoying social applications. In contrast, the applications manage their transactions but always keep data and rights on the user's side.

4.2 Convenience is essential

LUKSO standards can provide users unprecedented convenience and reduce dependencies on centralized entities [16] with standards for tracking received assets and a tool to subsidize transaction fees. Currently, most blockchains rely on centralized instances like Etherscan's block explorer to query a profile's current and previously owned assets and transaction history. For future decentralized societies, frequent tokenized rights or interaction checks will result in heavy demand for these queries. LSP5 [17] and LSP10 [18] keep track of every owned asset or Vault by default. This information can always be read directly from the contract, removing the need for block explorer APIs and making room for truly decentralized frontends.

Developing a novel blockchain ecosystem goes beyond the creation of smart contract standards. A standardized off-chain relay tool [19] built by LUKSO also allows services to pay for transactions and execute them on the user's behalf. Users are alleviated from directly paying fees, so they no longer have to get coins from crypto exchanges to start interacting with the blockchain. Projects and companies can develop new business models, such as advertising or subscription-based financing, network quotas allowances, or subsidized onboarding. These features provide a more familiar experience for the user, significantly lowering the entry barrier for newcomers who expect a Web2 user experience. For services like LENS, users would not have to get MATIC tokens before claiming a handle or publishing a post. Instead, EVM-based projects could run their funded off-chain relay service to create better onboarding.

Using extended complexity like smart contracts as accounts requires more gas per transaction and therefore comes with a higher cost. The team at LUKSO spent years developing those fundamental building blocks and making them as modular and lightweight as possible. However, it won't be the best experience on occupied networks, which are struggling with fees already. If most of the network still uses EOAs, they further heavily lack the feature set while interacting with contract-based accounts. Blockchain standards can only achieve long-lasting and proper convenience if the entire ecosystem relies on them. That's why LUKSO focuses on a standalone ecosystem. However, standards and tools are compatible with all EVM chains and developed for various economies.

5. The need for community recovery

The last chapter explained the significant impact contract-based accounts bundled with a key manager could offer for Soul recovery. For security concerns, services could implement varying burn-and-reassign methods for SBTs. One example would be using social recovery schemes [20], where trusted relationships are relied upon to back up a Soul instead of just creating more self-recovery options for the user. But defining the right set of Souls to restore an identity might be difficult. The user must balance choosing a significant enough number of friends to avoid both power positions and collusion. Group size can have a substantial effect on interpersonal relationships within a group. Collective thinking dominates in large groups, as opposed to small groups, where each voice carries more weight and has a high impact in the event of discrepancies.

For social recovery decision-making, large groups may succumb to a collective opinion more than the individual's wishes. In contrast, smaller groups with closer interpersonal relationships can more accurately manage a Soul's wishes but have less collective accountability, making them more prone to collusion. Here, death, disputes, or falling out of touch would require frequent updates to maintain a successful recovery.

A more robust solution, is tying Soul recovery to its memberships across communities or services, drawing on a broad set of real-time relationships for security. [21] People a user currently and frequently interacts with could attest that an old account is no longer accessible or under that user's control. After a certain number of attestations, the previous SBT can be removed, and a new token reissued to a new address. Such a community recovery model would require consent from a member belonging to a qualified majority of a random subset of Soul communities.

By "embedding security in sociality," [21] users can constantly regenerate the keys to access their accounts through community recovery, deterring Soul theft or sale. If someone wants to sell a Soul, he would also have to bribe all his recovery relationships, annihilating its or his social circle's credibility.

Social recovery does not provide a solution for recovering compromised EOA private keys from an attacker. Once known, the attacker can always act as the compromised identity, since the backup is static. Again, a set of smart contract-based accounts could likely bring SBTs forward. Mainstream adopters could secure their identity with multiple private keys for different devices. Since the smart contract address will stay the same, SBTs would not need to be burned and reissued from old

addresses. Only the keys and security will require updating through recovery, reducing the overhead issuers would deal with. LSPs, as sophisticated building blocks coming out of the ERC725 Alliance [22] work field, are a giant leap forward in developing security options for the ecosystem. With changeable keys with different permissions, hackers will likely be limited in functionality by default. If set up correctly, the scheme efficiently prevents unauthorized users from accessing the higher permission keys of the Soul. Proper backups, like community recovery, could be added in the future to act as the final option for regenerating keys to control a lost Soul.

6. Caution when binding Souls

Although possibilities may sound promising, people must use Souls with caution and anonymity. SBTs have great potential to "compensate for in-group dynamics and achieve cooperation across differences." [21] Still, they risk being "used to automate red-lining of disfavored social groups or even target them for cyber or physical attack, or enforce restrictive migration policies." [21] Initially, individuals might only carry SBTs that they are comfortable sharing publicly. Still, as most of society grows into such ways of interaction, some will not question the consequences of sharing. An excess of SBTs may reveal too much, making the Soul transparent and vulnerable to social control. Blockchain-based systems used for social media are likely public by default, and so are the profile and NFT data written into contracts. "Any relationship recorded on-chain is immediately visible not just to the participants, but also to anyone in the entire world." [21] If improperly managed, having multiple anonymous Souls and pseudonyms for various social corners and SBTs could make it very easy to correlate different Souls to each other.

Services could use zero-knowledge proofs for linked off-chain data that can only be seen by certain other Souls if revealed. However, when examining the other extreme, having too many private SBTs may lead to hidden communication channels that eschew correlation discounting for governance and social coordination, forming dangerous manipulative bubbles that undermine healthy social systems.

Cheating can also be an uncomfortable subject. "Souls may misrepresent their social solidarity, while coordinating through private or side channels." [21] For example, if SBTs were issued to prove attendance to a required conference, unscrupulous conferences could offer such SBTs in exchange for bribes. With an adequate number of bribed people, Souls and bots could generate fake social graphs that make the account look authentic.

Managing faked social bubbles could become cumbersome for DAOs and their voting power. "Conversely, if SBTs are used to discount coordination, Souls may avoid SBTs to maximize their influence." [21] Coordination is a game theoretical problem on its own. Solutions include creating highly frequented community channels with strong social ties and repeated interactions, similar to school classes or working environments. Services could also require SBTs or strong bonds to others to participate in discussions to detect superficial, collusive groups. Regarding the backend, protocols could implement incentives and punishment systems to encourage honest behavior. Fortunately, there is already research on social media behavior from the recent decade that can be drawn upon.

7. Connection to Verifiable Credentials

For self-sovereign identity (SSI), the W3C [23] has been setting up new standards for years with Decentralized Identifiers [24] (DIDs) and Verifiable Credentials [25] (VCs) to issue certificates. These standards use a Web3-like Identity Flow [2] similar to SBTs, where data is managed in a user-centric way. Issued certificates are shareable depending on the user's location. Still, they often include personal, sensitive items such as driver's licenses or passports and mainly focus on institutional, centralized issuers like universities, governments, etc. VCs also differ since they do not specifically need to operate on a public blockchain. Hadrien Charlanes, founder of the SSI attestation project Sismo [26], mentioned: "VCs fit well with systems requiring off-chain operators, databases, and traditional actors." [27] They are perfect for use cases like "KYC, off-chain certificates and to bridge from Web2 to a blockchain native environment." [27] Instead, SBTs are crypto-native, fully operating as a data layer on the blockchain.

SBT standards can become new members of the already actively developing SSI tech stack. SBTs and VCs complement each other because of the data protection terminology. [21] SBTs are initially public, making them unsuitable for private data. On the contrary, VCs are used to sharing information unilaterally, making them unsuitable for joint social applications since they rely on some level of publicity and community. When sharing VCs, Souls cannot know that another one owns an SBT until that information is shared. Invisibility makes establishing a reputation, credible commitments, and visibly verifiable governance impossible. Secondly, it is almost impossible for an identity in a multiparty social relationship to have the unilateral right to disclose the relationship without the consent of the others. When two parties co-own an asset and choose to represent their relationship through a VC, such a credential does not enable mutual consent and permissions. This problem carries over to more complex cases in managing ownership and complex organizational forms such as DAOs and permissions, a feature of decentralized societies. [21]

The DID and VCs standards built on top of the current economy that deals with restrictions on private data are slowly seeing adoption. Ideas that take an approach by focusing on public data push development forward rapidly. [2] Here, SBTs and LSPs have the significant advantage of developing on a blue ocean for a data economy

that is yet to come. Various businesses outside the creative economy could adapt, expand or dock onto standards to make mainstream decentralized services a reality for the younger generation, whose most crucial skill is the exchange and finding of interests among each other that SBTs could soon enable.

9. Outlook

The path from the current web3 ecosystem to augmented sociality mediated by SBTs faces a classic adoption dilemma: SBTs encourage non-transferability and identity-specific approvals, but today's EOA wallets do not have proper backup schemes and risk losing their digital Soul. As the paper about decentralized societies stated, “In order for community recovery wallets to work, they need a wide variety of SBTs across discrete communities to be secure. What comes first: SBTs or strong social recovery?” [21]

This question of the SBT’s birth is the perfect starting point for contract-based accounts and the first set of LSPs [28] built beyond the ERC725 Proxy Account [7] standard. Here, communities can develop various key and backup schemes beyond a key manager without reissuing SBTs, as their Soul will only update its controller keys. Such contract-based Souls can also deliver much more convenience like permission handling, relayed transactions, or transfer approvals. Extended functionality would allow accounts to exist with solid onboarding, directly added claims, and recovery before more significant amounts of SBTs are handed out. Due to their integrated data storage, proper enclosures will further give more weight to who users are and less about what they have acquired. All this leads to safeguarding people and their assets without relying on 3rd parties.

Hybrid versions of SBTs could be another good starting point by giving communities time to build proper recovery before tokens are locked, further strengthening SBT issuing. But it has to be said that such management schemes still would have to be laid out and tested in the wild. For now, ideas are novel, and there is no commonly adopted flow regarding social media solutions.

Judging by all the community building happening in Web3, proper Soul frames and related SBTs could move the crypto scene from a generally money-oriented mindset into a more social space, giving people back not only power over their data and interactions but also placing focus on what truly matters: individuals and their genuine, unique relationships.

Acknowledgements

A sincere thank you to Rob Golden who assisted me in polishing this article and giving early feedback.

References

[1] Soulbound. (2022, January 26). Vitalik Buterin. Retrieved August 10, 2022, from https://vitalik.ca/general/2022/01/26/soulbound.html

[2] Hildebrandt, F. (2022, February 19). Identity Solutions for the Internet: Part 2 | KEEZdao. Medium. Retrieved August 10, 2022, from https://medium.com/keezdao/identity-solutions-for-the-internet-part-2-44aa1111b435

[3] Introduction. (n.d.). POAP. Retrieved August 10, 2022, from https://documentation.poap.tech/docs

[4] Hildebrandt, F. (2022b, March 5). LUKSO Ecosystem: Part 1 by Felix Hildebrandt | LUKSO. Medium. Retrieved August 10, 2022, from https://medium.com/lukso/lukso-ecosystem-part-1-4c3f5d67b081

[5] Proof Of Humanity. (n.d.). Proof Of Humanity. Retrieved August 10, 2022, from https://www.proofofhumanity.id/

[6] Hildebrandt, F. (2022c, March 5). LUKSO Ecosystem: Part 2 by Felix Hildebrandt | LUKSO. Medium. Retrieved August 10, 2022, from https://medium.com/lukso/lukso-ecosystem-part-2-fdc6abedf9dc

[7] Fabian Vogelsteller (n.d.). ERC: Proxy Account · Issue #725 · ethereum/EIPs. GitHub. https://github.com/ethereum/EIPs/issues/725

[8] Universal Profiles. (n.d.). LUKSO Universal Profile Explorer. Retrieved August 10, 2022, from https://universalprofile.cloud/

[9] LSP2 - ERC725Y JSON Schema | LUKSO Tech Documentation. (2022, June 15). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/generic-standards/lsp2-json-schema/

[10] LSP3 - Universal Profile Metadata | LUKSO Tech Documentation. (2022, August 6). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/universal-profile/lsp3-universal-profile-metadata/

[11] LSP6 - Key Manager | LUKSO Tech Documentation. (2022, August 2). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/universal-profile/lsp6-key-manager/

[12] LSP1 - Universal Receiver | LUKSO Tech Documentation. (2022, April 28). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/generic-standards/lsp1-universal-receiver/

[13] Lens Protocol. (n.d.). LENS Protocol. Retrieved August 10, 2022, from https://lens.xyz/

[14] LSP9Vault | LUKSO Tech Documentation. (2022, June 10). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/smart-contracts/lsp9-vault/

[15] Adams, R. S. (n.d.). How to maximize your ENS domain. Ryan Sean Adams. Retrieved August 10,

2022, from https://newsletter.banklesshq.com/p/how-to-maximize-your-ens-domain?s=r
[16] Hildebrandt, F. (2022e, May 10). LUKSO Ecosystem: Part 3 by Felix Hildebrandt | LUKSO. Medium. Retrieved August 10, 2022, from https://medium.com/lukso/lukso-ecosystem-part-3-9af6bbcc24da
[17] LSP5 - Received Assets | LUKSO Tech Documentation. (2022, July 8). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/universal-profile/lsp5-received-assets/
[18] LSP10 - Received Vaults | LUKSO Tech Documentation. (2022, July 8). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/universal-profile/lsp10-received-vaults/
[19] Execute Transaction | LUKSO Tech Documentation. (2022, July 15). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/tools/relayer-api/execute-transaction/
[20] Why we need wide adoption of social recovery wallets. (2021, January 11). Vitalik Buterin. Retrieved August 10, 2022, from https://vitalik.ca/general/2021/01/11/recovery.html
[21] Weyl, G. E. (2022, May 10). Decentralized Society: Finding Web3's Soul. SSRN. Retrieved August 10, 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763
[22] ERC725 Alliance. (n.d.). ERC725 Alliance. Retrieved August 10, 2022, from https://erc725alliance.org/
[23] Oskoboiny, G., Ran, R., & Jaffe, J. (n.d.). World Wide Web Consortium (W3C). W3C. Retrieved August 10, 2022, from https://www.w3.org/
[24] Decentralized Identifiers (DIDs) v1.0. (2022b, July 19). W3C. Retrieved August 10, 2022, from https://www.w3.org/TR/did-core/
[25] Verifiable Credentials Data Model v1.1. (2022, March 3). W3C. Retrieved August 10, 2022, from https://www.w3.org/TR/vc-data-model/
[26] Sismo - Curate your identities with privacy. (n.d.). Sismo. Retrieved August 10, 2022, from https://www.sismo.io/
[27] dhadrien.sismo.eth. (2022, May 27). Twitter. Retrieved August 10, 2022, from https://twitter.com/dhadrien_/status/1530171210121846787?t=Ly4yvOSI6pg30ng5CUskSw&s=19
[28] Introduction | LUKSO Tech Documentation. (2022, July 21). LUKSO Tech Docs. Retrieved August 10, 2022, from https://docs.lukso.tech/standards/introduction/