Budapest University of Technology and Economics
Faculty of Electrical Engineering and Informatics

Self-sovereign identities on central bank digital currency ledgers

Created under the MNB-BME Cooperation Agreement

Authors:
Imre Kocsis, Bertalan Zoltán Péter, Attila Klenik, László Gönczy
Department of Measurement and Information Systems

Budapest, 2022.

Executive summary

The emerging Self-Sovereign Identity (SSI) technologies put sovereignty over identities and credentials literally in the hand of their holder – into a hardware or software *wallet*. Coupled with blockchains as trusted identity and credential issuer and issuance registries – like the one the EU is building in the EBSI project for cross-border use cases – these technologies are about to deeply transform how we handle electronic identities and prove our credentials to various parties.

In this exploratory study, we describe some potential applications of SSI-based identity handling in CBDC settings; a coupling that hasn't received much attention yet. The possibilities we envision are wide ranging; from the mundane, but impactful (for instance, strongly reducing the challenges of Know-Your-Customer processes) to the deep cutting (enabling cash-like privacy for CBDC by creating cash-like ”encumbrances” – inconvenience of use).

Contents

1 Introduction

Self Sovereign Identities (SSI) is an emerging philosophy, technology ecosystem and set of standards for a new approach towards handling identities. Cryptocurrencies proved that sovereign authority of the holders of "money" over their funds can be assured through a combination of holding private cryptographic keys in a personal "wallet" (for proving authority) and a decentralized ledger (for enforcing commonly understood transaction rules, if some sufficient majority of the participating nodes remains honest).

SSI has similar goals: enabling the creation of globally unique, holder-controlled identities through decentralized, blockchain-based registries. In SSI, parties that in classical settings issue identities, issue *claims* about one of the possibly numerous identities of an end user, and *attestations* to those claims. Attestations to the claims may be revocable – but not the identities themselves, which remain under user control.

In the recent years, numerous successful use cases for SSI have been created – from business registries to the cross-border acceptance of diplomas in Europe. In this report, we argue that Central Bank Digital Currencies (CBDC) could also benefit from applying SSI concepts and technologies in their identity handling approach. Our treatment is "by example"; we target specific challenges of CBDC solutions and outline how SSI-based identity management can provide a better solution than classic approaches. To the best of our knowledge, supporting identities in CBDC with SSI is a proposition which hasn't received much attention yet; in this sense, our work is as much a call to attention as an initial enumeration of the possible patterns of using SSI in the CBDC context.

2 Self-Sovereign Identities

Self-Sovereign Identity (SSI) is a new approach to implement a digital identity solution; one that was born in concert with the emergence and proliferation of (blockchain-based) distributed ledgers.

Identity can mean several things. Different fields have different notions of what constitutes an "identity"; similar to [9], we define identity as *a unique "something" that describes all attributes of a person (or thing) over the course of their lifetime*.

It is simplest to think about this concept in terms of us, human beings. Every person has their own identity, which is unique to them. What can distinguish one person from others is an *identifier*. This could very well be, for example, a very long number. If every person has their own number and every number belongs to exactly one person, than this number is a valid identifier for people. But in real life, it is common to identify people by a set of attributes: e.g., their full name, birth date, and perhaps their mother's name, place

of birth, or both. The latter is an identifier that is a set of attribute values instead of being a single value (like a number).

One person may have more identifiers. Normally, it should not be a problem if a person has two long numbers that both identify them – they are still unique, they just happen to point to the same entity. For example, a person can be identified by her/his bank account number when it comes to finances. Conceptually, specifying this number should be enough for someone to deposit some money to the account of another person. On the other hand, this same identifier can not be used at a general practitioner's office; they will instead ask for a social security card or similar document, which has been issued by the government – another identifier (assuming a universal health care setting).

In today's digital world, the "ID card" can also be some form of digital document; cryptographically secured data on a smart phone or in a smart card. But there's also another conceptual alternative, one on which SSI relies: it could be "publicly known that I exist", but to prove that I am me (and am currently covered), I have to present a digital document to the verifying party (e.g., a GP). *Self-sovereignty*, as a concept, means that the identity is ultimately controlled by the holder; the holder chooses who the identity is exposed to and what happens to the identifiers.

2.1 Verifiable Credentials and Presentations

SSI is a rather general concept, which, somewhat similar to CBDC, can be realized in many different ways. That being said, most proposals and existing solutions provide a decentralized, DLT-based approach. We therefore call identifiers in SSI Decentralized Identifiers, or DIDs in short. The DID is like an ID card number, it uniquely identifies a person (or any other object, for that matter; the German federal project IDunion explicitly targets the IoT/IIoT space, too).

DIDs correspond to so-called DID documents (DIDDocs), which contain additional information associated with the DID: most importantly, the way to cryptograhically authenticate the controller of the DID, i.e., the person it belongs to. An SSI system shall make it possible to resolve DIDs to DIDDocs – DIDDocs (usually) contain the DID they belong to. This way, if I have a DID `did:foo:123`, I can prove that it is indeed mine by proving, for example, that I have the private key associated with the public key found in the DIDDoc of `did:foo:123` (which is available in a public registry).

A DID is just an identifier. What actually unlocks the power SSI are so-called *Verifiable Credentials* or *Verifiable Claims* (VC). As the name suggests, a VC "claims" something about the holder of a DID. For example, a birth certificate could be issued as a VC, claiming that the birth name of the holder of an identifier is John Doe, born 1963, in Budapest, Hungary. In accordance with self-sovereignty, the holder "owns" this electronic credential document and shows (presents) it to only such parties that he or she wishes to.

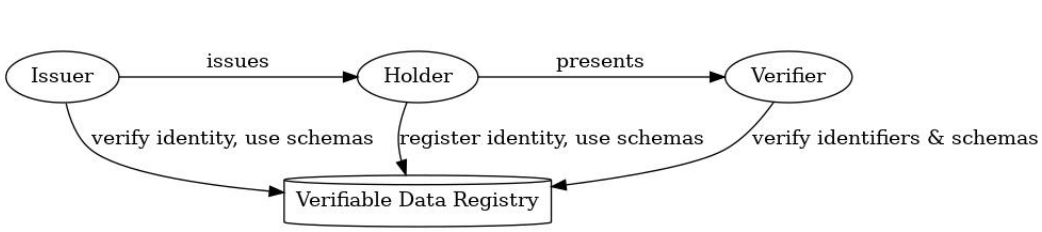

Figure 1: Key roles in a decentralized identity setting

The VC ecosystem allows a verifying party – say, a university – to verify this claim in a way that needs neither coordination nor synchronous communication with the issuer of the credential (in this example, a governmental body). The VC contains the information verifiably that it was issued by the government (through digital signatures) and the university knows that this issuer can be trusted. Thus, if the presented credential conforms to the expected format of, e.g., a birth certificate and the presenter can prove that it has been issued by the government, the university will have no reason not to accept it. The ability to check the conformance of the "proving" digital signature to the public key of a public body and checking whether the credential (but not the identity it refers to!) has not been revoked yet are certainly as much necessary as with "classic" Public Key Infrastructures (PKI) based on standard, X.509 certificates; but are actually radically easier if we can assume a trustworthy (distributed) public registry.

It is common to model the structure of SSI as the interaction of three actors and a database (or registry), as seen on Fig. 1. An `Issuer` issues credentials to the `Holder`, who can later present this to a *Verifier*. All three of them access the *Verifiable Data Registry* in the process. This architecture is sometimes referred to as the *Trust Triangle*.

2.2 DIDs, DIDDocs and other standards

DIDs are in the process of standardization by W3C, the World Wide Web Consortium [7]. The data model for VCs is also being standardized as a W3C recommendation [8].

On a technical level, a DID is a simple text string that consists of three parts:

- a scheme identifier (did),
- a DID method identifier,
- and the method-specific identifier.

The parts are separated by colons (:). Listing 1 provides an example.

```
did:example:12345689abcdefghi
```

Listing 1: A DID

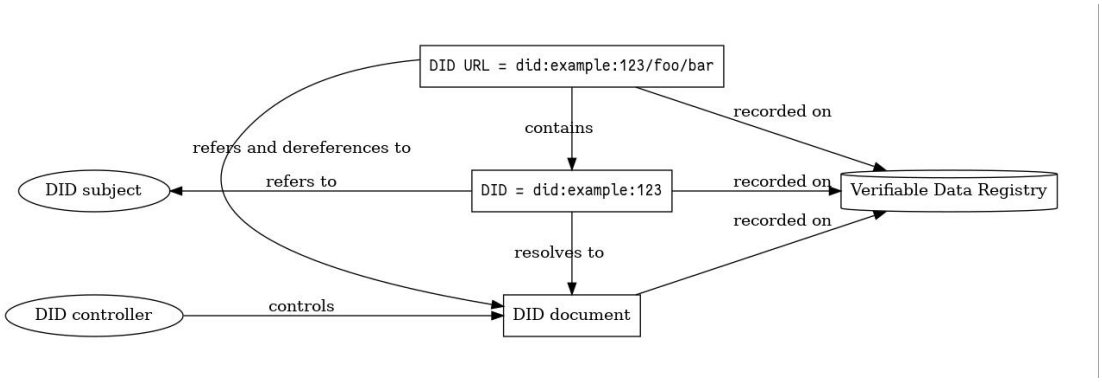

Figure 2: The relationship of DIDs, DIDDocs and Verifiable Data Registries

Every DID resolves to a DIDDoc (informally, much like web URLs resolve to web page documents) – Listing 2 provides an example for a possible DIDDoc which the DID as an identifier could resolve to.

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

Listing 2: Example of a DIDDoc

Both DIDs and DIDDocs are recorded in a (distributed) database (called the *Verifiable Data Registry*), as depicted on Fig. 2.

DIDs, DIDDocs and VCs are foundational elements in SSI; and in the context of the latter, we also have to introduce the concept of *verifiable presentations* (VPs). As per the VC standard [8], a *presentation* is *"Data derived from one or more verifiable credentials, issued by one or more issuers, that is shared with a specific verifier.* A verifiable presentation *is a tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. Certain types of verifiable presentations might contain data that is synthesized from, but do not contain, the original verifiable credentials (for example, zero-knowledge proofs)."*

Zero-Knowledge Proofs (ZKP) are a relatively novel field of cryptograpy, which came to the limelight in recent years due to their eminent applicability for creating privacy-preserving techniques in blockchains. Informally, a ZKP is such a mathematical proof of knowledge or the ability to perform a computation that does not leak any further information; i.e., the information itself or any further details about the computation (the ZKProof Initiative maintains a community reference [10] with the goal to help "mainstreaming" ZKP solutions).

In the SSI space, ZKP-based VPs are expected to become an immensely powerful mechanism as they enable *selective disclosure*. The schoolbook example is that using a VP created from the appropriate "Zero-Knowledge Credential", when challenged by a verifier, a `Holder` can prove that she or he is over 18 – but in contrast to what happens when we, e.g., present a physical ID card, no further information is disclosed (name, gender, exact age, etc.). Such mechanisms have many exciting potential real-life applications, from buying controlled substances to public elections.

A complete SSI ecosystem will include even more components, and from the point of view of open standards, the "standards stack" for SSI is still forming. However, from the point of view of this document, we do not need to introduce further concepts; for the purposes of further exploration, we kindly refer the interested reader to the resources provided by the Decentralized Identity Foundation (DIF) [2].

2.3 Hyperledger Indy and the Sovrin network

Currently, the Hyperledger Indy project [5] provides the most mature open technology ecosystem for SSI. Indy is a set of integrated tools for providing digital identities in a decentralized manner – through a blockchain system designed primarily for maintaining identities (rather than money or other tokens). Its components include Indy Plenum (the core distributed ledger implementation), Indy Node (which extends Plenum's functionality and runs on the blockchain nodes), an SDK and CLI tools. For cryptography, Indy utilizes Hyperledger Ursa, the common cryptographic library for projects under the Hyperledger umbrella.

Under the hood, Indy maintains a few separate ledgers to store data. The most important is the domain ledger, which contains the registered DIDs, called "NYM"-s in this context. NYMs have attributes (ATTRIBs). This ledger also contains the SCHEMAs of claims that can be issued. Another ledger worth mentioning is the pool ledger, which maintains what nodes operate on the network.

The same way as there's the Ethereum protocol specification and there are multiple different networks running protocol-conformant software, chief among which is the "Ethereum mainnet", Indy also has multiple known "instantiations". The closest equivalent to the "mainnet" is Sovrin, an open-access, permissioned consensus network. The

Sovrin BuilderNet supports testing, StagingNet serves pre-production SSI applications and the main network, MainNet, is for production. Other notable users of the Indy technology include the IDunion consortium (formerly: SSI for Germany) and the OrgBook project of British Columbia.

2.4 EBSI: the European Blockchain Services Infrastructure

Under the umbrella of the European Blockchain Partnership (EBP), the European Union is in the process of creating a blockchain-based infrastructure – operated by permissioned organizations of the Member States[1] – for supporting a wide range of cross-border applications within the Union. The initial use cases target the public sector with such use cases as cross-border electronic identification of citizens and verification of diplomas; the mid-term plans also include providing services for businesses.

A core component of EBSI is ESSIF, the European Self-Sovereign Identity Framework (see [3]). Currently, ESSIF is an "SSI-style" identity framework in the sense that it builds on standardized SSI technologies, but does not provide a "full SSI stack" and it has its own framework of concepts which flow from its intended application, as depicted on Fig. 3.

Importantly, ESSIF recognizes `Registration Authorities` which manage `Verifiable ID issuers` – very broadly speaking, mirroring the mechanism of national enumerations of trust service providers in "Trusted Lists" in the current implementations of the eIDAS (electronic IDentification, Authentication and trust Services) EU regulation.

By definition, EBSI Verifiable IDs *"are a special type of Verifiable Credentials (VCs) that Natural Persons and Legal Entities can put forward as evidence of who they are (comparable to a passport or a physical ID card). In other words, Verifiable IDs serve to enable identification and authentication and as such contain digital claims about certain personal attributes. If someone provides, for example, a Verifiable ID that states information about this person's identity and is issued and signed by a government, service providers may trust and rely on this information (if they trust the government and the cryptography) to decide whether or not to conduct a transaction."* [3] Verifiable IDs build on the W3C Verifiable Credentials data model, but also take into account eIDAS and implement the eIDAS Minimum Dataset.

In addition to Verifiable IDs, EBSI recognizes two fundamental VC categories: *Verifiable Attestations* and *Verifiable Authorizations*. As defined by EBSI, *Verifiable Attestations are a special type of Verifiable Credentials (VCs) that Natural Persons and Legal Entities can put forward as evidence of certain attributes/properties or as evidence of a permit/attestation/authorization he/she/it received. If someone provides, for example, a Verifiable Attestation that states information about this person's education credentials and is issued and signed by an accredited university, service providers (e.g. recruiters,*

[1] The Budapest University of Technology and Economics also operates a node.

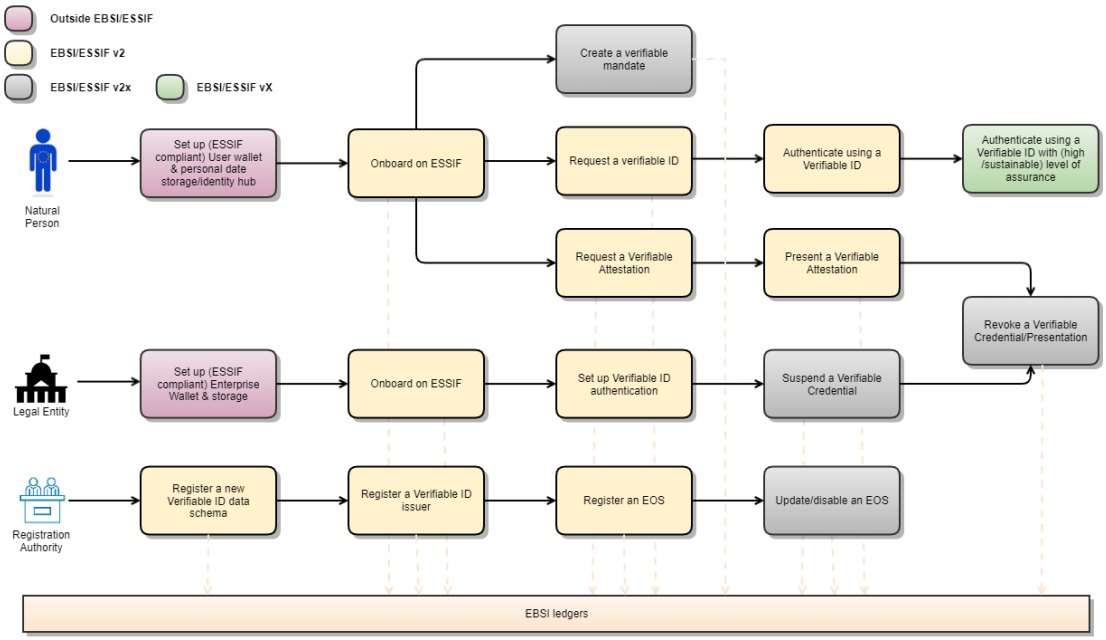

Figure 3: Self-Sovereign Identities in EBSI[2]

other education providers) may trust and rely on this information (if they trust the issuer and the cryptography). Verifiable Authorizations ("mandates") is a concept which has not been finalized yet.

As of this writing, the EBSI documentation recognizes the Technology Readiness Level of EBSI v2 as a decentralized identity framework to be 6/7. Additionally, EBSI declares certain "natural" VP exchange scenarios as out of scope: importantly, VPs with selective disclosure. Last but not least, the review and update of eIDAS, the regulatory framework EBSI will have to adhere to, is an ongoing process.

Consequently, when we discuss the applicability of SSI solutions in the CBDC context, we do not imply that EBSI can be a production ready SSI component for a CBDC operated by one or more Member States in the short term. On the other hand, we do want to emphasize that it has the *definite potential* to provide a pan-European SSI substrate for CBDCs; one which is able to support the cross-border federation of identity checking. Additionally, it can carry a broad range of other claims which are potentially important from the CBDC point of view – from KYC/AML through credit ratings to tax and social security status.

[2]Source of the figure: `https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=379913698`, accessed on: 13-06-2022

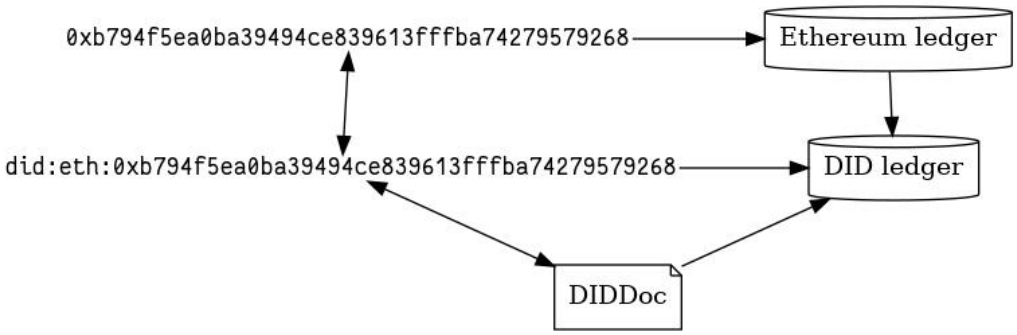

Figure 4: Cryptocurrency pseudonyms as DIDs

3 SSI-backed CBDC ledgers

The most basic application imaginable is probably using SSI "simply" as an identity backend on the CBDC ledger: the CBDC system could use DIDs as account identifiers.

3.1 Minimal example: smart contract based CBDC

For a minimal – if rather unrealistic, for reasons practical, regulatory and platform trustability – example, consider a smart contract based CBDC implementation on an Ethereum network: essentially, a central bank issued stablecoin.

At first, one may implement the contract in such a way that CBDC accounts correspond to Ethereum accounts, which are identified by public keys (essentially, hashes of the truncated public key [4]). In this case, there is a clear 1:1 correspondence between Ethereum and CBDC accounts and the smart contract takes care of CBDC balances.

It is a natural thought to use other identifiers, like DIDs as account identifiers in the CBDC system. This can provide the same pseudonimity as public keys, but allows us to take advantage of the SSI system as well.

The fact that an `eth` so-called DID method can theoretically be created makes it unnecessary to define a mapping between Ethereum accounts and CBDC accounts; technically, the Ethereum public key simply needs to be prefixed with the string `did:eth:`. Naturally, these DIDs must be registered to the SSI `Verifiable Data Registry`, which is likely to reside in a separate distributed ledger; see Fig. 4.

With this setup, while using the CBDC system, useful SSI mechanisms, such as VCs can be used. For example, consider one wishing to pay 200 CBDC units to `did:eth:deadbeef`. Firstly, one may not know, who this actually is. This is not a new feature, as public keys were already pseudonymous identifiers. But now one has a simple and safe way to open a communications channel with this party; one could request that

they show a VP proving that they have the right to receive the money (e.g., they shipped a product).

Of course, the CBDC implementation does not need to rely on smart contracts. All we assume is that there is a way to use DIDs as account identifiers on the CBDC ledger.

3.2 Generalized CBDC setting

Moving on from Ethereum, let us now elaborate how a general CBDC system could work together with SSI, relying on DIDs as identifiers. Note, that some of the ideas and procedures described here are inspired by [1]. We begin with identifying the relevant components and actors of our generalized setting.

Central Bank (CB): it is assumed that the CB issues CBDC and maintains the balances, i.e., the CBDC ledger. At this level, it does not matter what ledger structure or implementation is used.

Identity Provider: the identity provider maintains the registries of the decentralized identifiers, i.e., the DIDs and DIDDocs. It provides lookup services, such as finding the DIDDoc for a given DID. In practice, this could be the Sovrin network, for example.

Alice & Bob: Alice and Bob both have DIDs, which they would like to use with the CBDC ledger. They are clients of the CB. Furthermore, they would like to perform transactions between each other.

At first, neither Alice, nor Bob have a CBDC balance. It is assumed that they have already created a new DID to use with the CBDC, which has been published to the Identity Provider's database.

3.3 Opening CBDC balances

Now Alice and Bob want to open their CBDC balances at the CB. This is already something SSI can help with. At the time of enrollment, the CB would have to perform a relatively long Know-Your-Customer (KYC) process, to verify that Alice and Bob are allowed to possess CBDC (and that they are indeed who they claim to be). If both of them are new to financial institutions and have never gone through such a process, the CB cannot avoid taking the time and resources to "KYC" them now.

However, the process itself can be improved if Alice and Bob are able to prove certain facts through their electronic identities. For example, they may have previously obtained a VC proving that they have a permanent address in a given country (issued by a governmental body trusted by the CB). Notice that taking advantage of selective disclosure and ZKPs, it is possible for Alice and Bob to prove some attributes (such as the fact that they

have a permanent address) without disclosing sensitive information (such as the address itself).

If the CB is able to rely on these VCs during the KYC process, the required time for the procedure can be greatly shortened. Actually, Alice and Bob potentially need not even to show up personally at the CB – using a VC/VP exchange protocol, they are able to present their VCs, which are tied to their DIDs, electronically and remotely. And they can also prove that the DIDs are indeed theirs: since they have the private keys belonging to them, they can appropriately sign a challenge message provided by the CB as a Verifier (this is a standard technique in exchange protocols for SSI).

Additionally, it is possible that Alice or Bob have actually been already KYC'd previously – by the CB itself, or another financial institution. For isntance, Alice may already have a CBDC account, but she wants to open a new one for some specific purpose; or she has been already KYC'd by a retail bank and now seeks access to the newly introduced CBDC ledger. Arguably, in these cases, she should not have to be KYC'd again; and if her KYC status is available as a VC, she indeed may not have to be. The envisioned process is outlined on Fig. 5.

3.4 Performing transactions

Now the two parties have their CBDC accounts, which are identified by their DIDs. When requesting a transaction from the CB (possibly offline), they must prove that they are in charge of their account. This is easily done by signing the transaction request by the private key that belongs to their DID (and whose public counterpart can be found in the DIDDoc for signature verification). For example, if Alice intends to send 100 CBDC units to Bob, she simply needs to send a transaction request, signed by her private identity key, in which she pays 100 units to Bob – and she specifies Bob by his DID. Fig. 6 outlines the key elements of this scheme; Fig. 7 depicts the sequence of activities.

4 CBDC bridging and SSI

"Bridging" assets between (distributed) ledgers is a common technique in the cryptocurrency world. Assets are locked down in a source ledger and their corresponding "shadow" asset units are "minted" on the target one; afterwards, they can be used on the target ledger with the assumption that they represent assets in essence kept in secure "escrow" on the authoritative (source) ledger. A current holder of the shadow assets can also decide to "burn" the shadow assets on the target ledger and begin to use them on the source one.

While such techniques are mostly known for "wrapping" foreign cryptocurrencies and tokens in native tokens on Ethereum networks (this way, we can use, e.g., "wrapped Bitcoin" on Ethereum), the concept is eminently applicable in the CBDC context, too, as de-

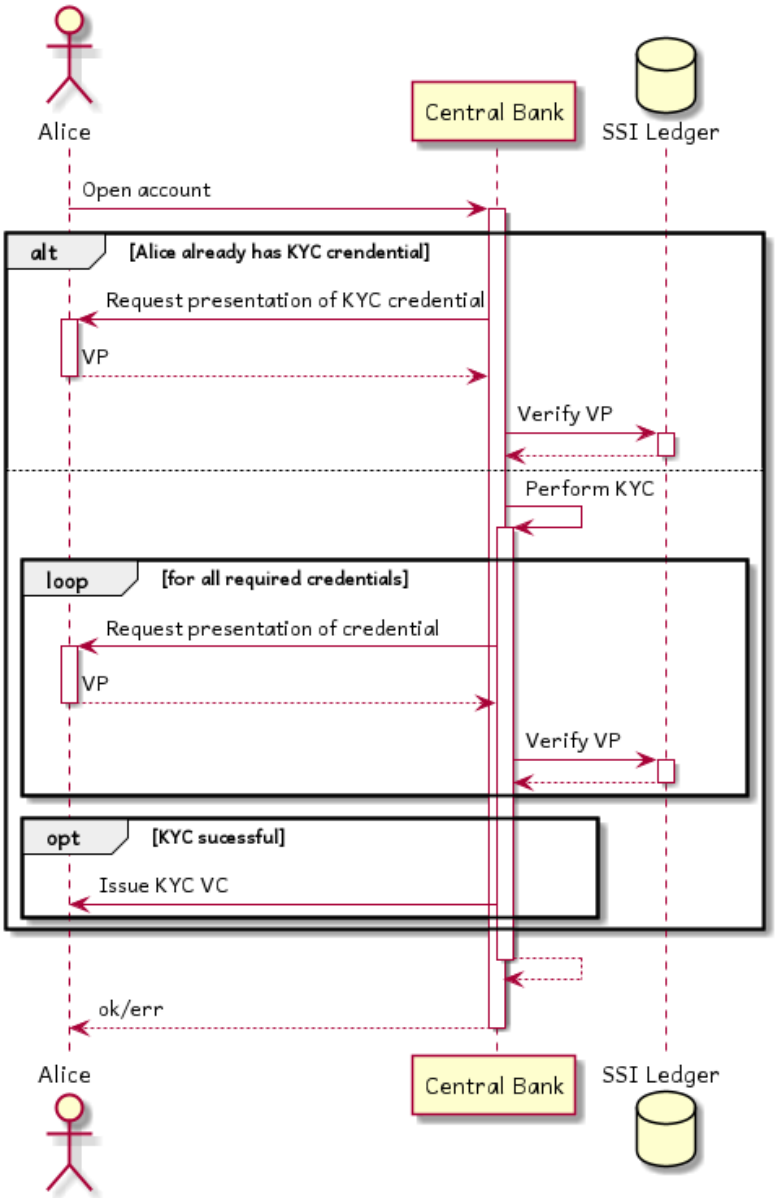

Figure 5: CBDC KYC with existing VCs

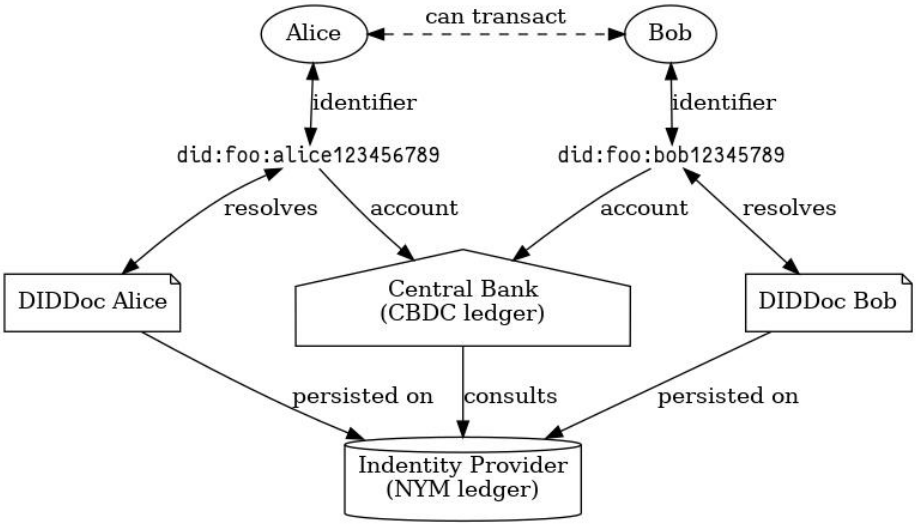

Figure 6: Key concepts of DID-based CBDC transactions

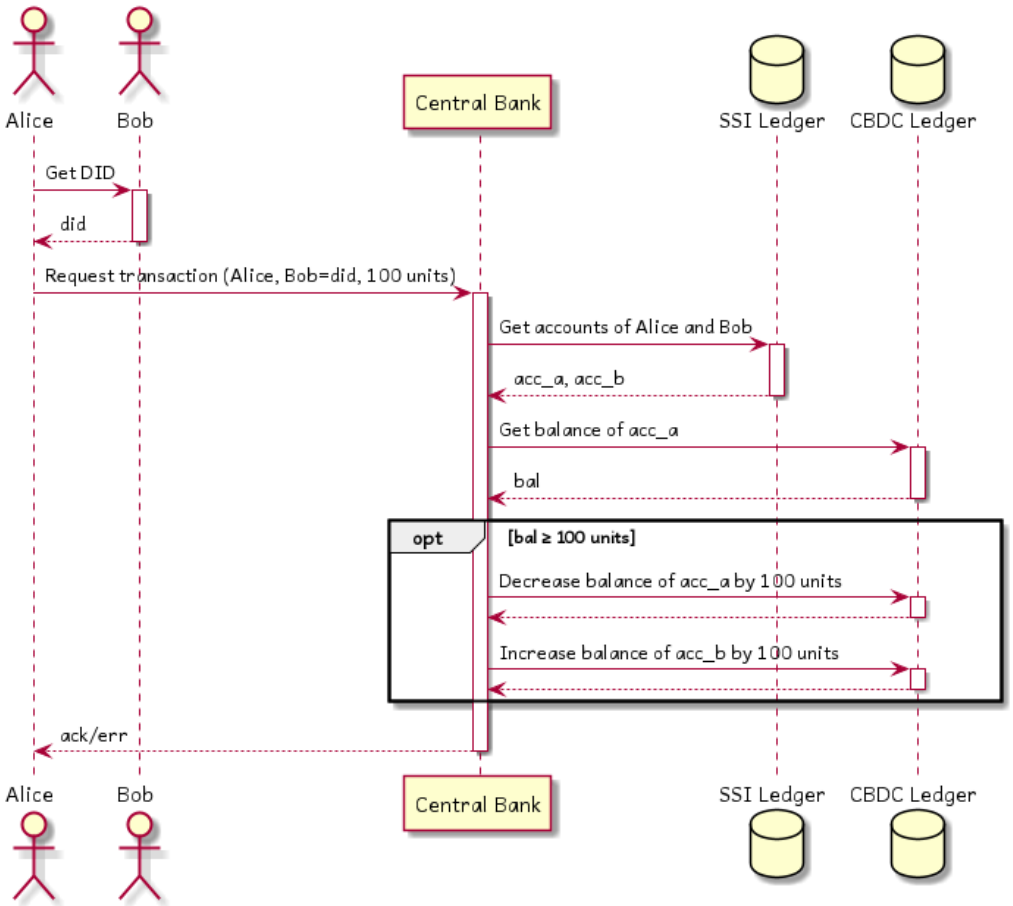

Figure 7: DID-based CBDC transactions

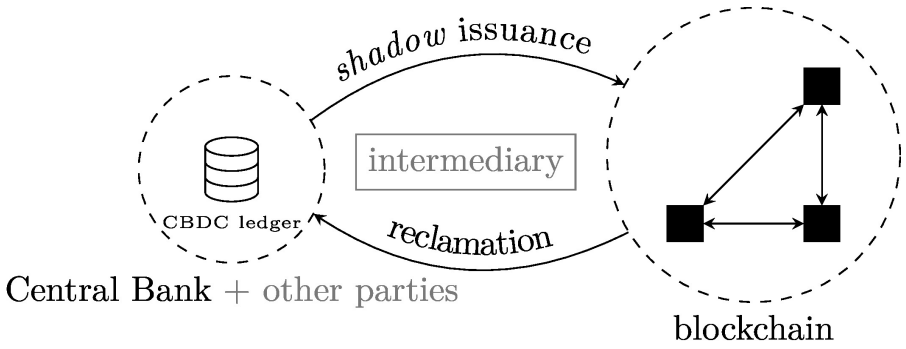

Figure 8: CBDC bridging: a conceptual view

picted on Fig. 8. A CB may decide to give permission to a consortium of parties to "bridge out" CBDC assets to a permissioned distributed ledger of their own; this not only eases the workload on the CBDC ledger (which may be especially important in high frequency, low value machine-to-machine scenarios) and protects the business confidentiality of the cooperating parties, but is also a viable way to facilitate CBDC-handling smart contracts – without creating widely accessible smart contract support on the CBDC ledger itself.

Temporarily releasing CBDC to a "sidechain" does raise a number of regulatory and auditability questions, but many of these are already known to be addressable efficiently and in a confidentiality/privacy preserving manner (see, e.g., [6] for ZKP-based audits of continuous adherence to CBDC-holder whitelisting requirements).

We will assume that there exists a 3rd party identity blockchain for SSI purposes, where the identity documents of the blockchain users (consortium members, organizations) are stored and are reachable by the CB.

4.1 Proving permission when minting or burning

When an organization on the blockchain requests either minting some funds into their blockchain balance (meaning they pay actual CBDC, which appears on the side-chain as a shadow; in other words, this is shadow issuance) or burning some funds on their blockchain balance (meaning shadow CBDC is removed from their blockchain balance and appears on their CBDC balance), the bridging provider (intermediary on the diagram) must verify their identity. For example, the organization/user may give a VP proving that they indeed have an account on the blockchain and are allowed to use it (i.e., they have been properly KYC'd). See Fig. 9.

4.2 Audits and KYC

Periodic as well as ad-hoc audits must be performed on the side-chain state by the CB. During these, besides verifying that the blockchain state is valid, the CB must ensure

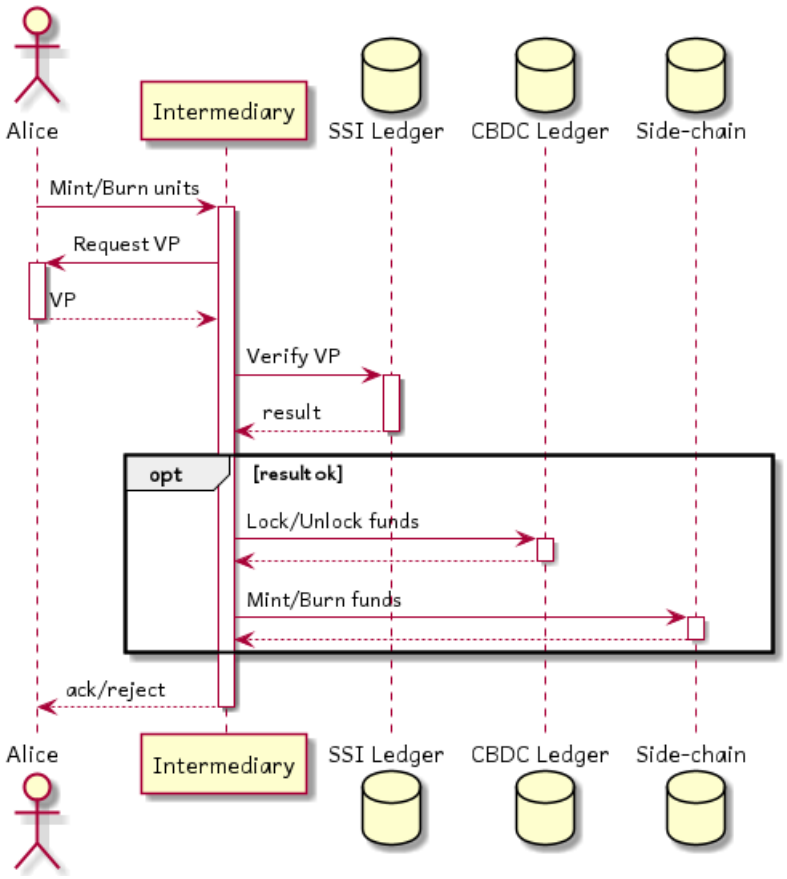

Figure 9: Proving minting and burning permissions with VPs

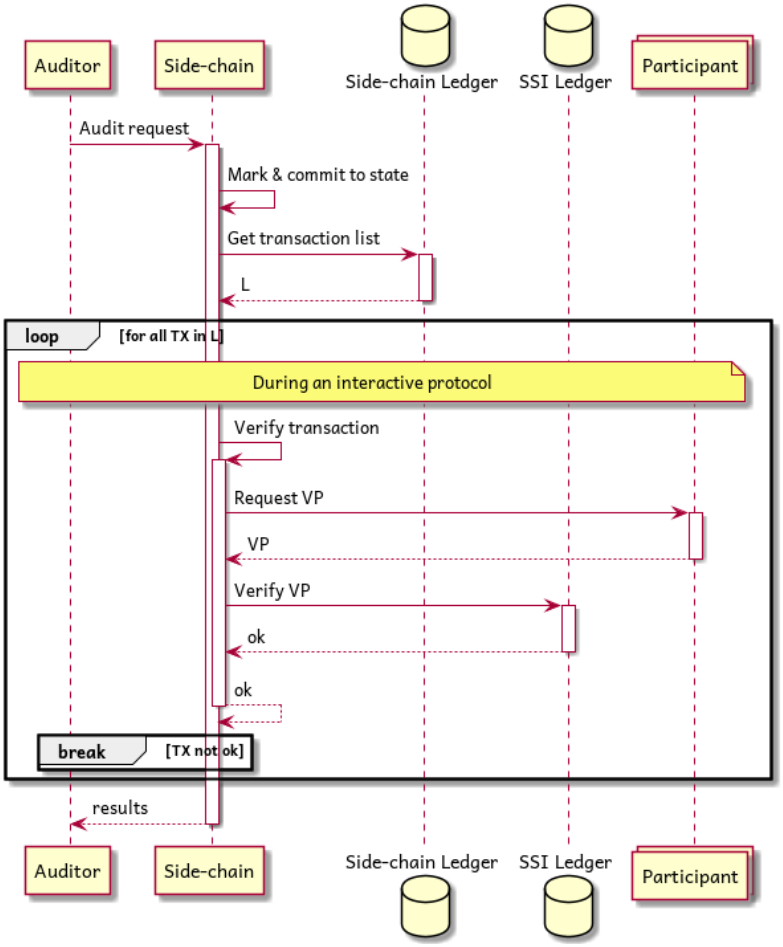

Figure 10: A possible sidechain audit protocol

conformance to KYC requirements. For example, it must be verifiable that all transaction participants are KYC'd.

To this end, participating organizations/users can use pseudonymous DIDs as account identifiers (which can be connected to actual public keys in their DIDDoc). Then, during an audit, the CB may simply verify whether the organization behind a given DID is KYC'd (via a certificate presentation, essentially).

[6] proposes an approach to perform audits in zero-knowledge in a bridged CBDC scenario, where the audit process can be described as a computation (essentially a program). In the simple case explored in the article, the computation checks that transactions have only been conducted between allowed parties. There is nothing preventing reliance on SSI in the audit computation. It can be a part of the audit to request a VP of a KYC document (or any other claim), which can be interactively (or even automatically) presented by a given transaction participant.

4.3 Sidechain membership management

Let us assume there is a working CBDC system and it is being bridged to a consortial blockchain network, where around a dozen organizations perform regular transactions with these funds. The CB has been conducting periodic audits on the ledger to ensure no illicit activity is happening. In the latest audit, however, they notice that some transactions involve a new, previously unseen party – a new organization that just started using the blockchain.

Normally, this could be a problem. The CB must know where bridged CBDC goes (for KYC requirements), but this new participant has not been previously identified.

Without SSI and related concepts, the new participant would most likely need to identify itself to the CB, therefore exposing that it started some sort of cooperation with the consortium and potentially even what transactions it is making.

With SSI, there is another way. It is possible, even likely, that this new organization has previously done business with either the CB or another institution, where it did already confirm its identity, ie went through the KYC enrollment procedure. If this institution can give a VC to the organization proving that they are KYC'd, the organization can later simply present this to other parties, without revealing any of the information that was originally required to get KYC'd.

So, in our case, the CB could contact the organization by their DID, request this VC to be presented (or even the organization could request a presentation) and upon a successful presentation, simply acknowledge that this new participant is allowed and KYC requirements are still met.

5 Cash-like CBDC encumbrances with SSI

When CBDC is proposed as a digital alternative to physical cash, questions of privacy versus auditability arise almost immediately.

Physical cash offers a very high level of privacy; on the downside, this translates to a high risk of it being used as a vehicle of illegal activities. Still, its potential usage is tampered by its physical nature: handover involves physical contact; truly large sums are not straightforward to physically move; and quick successions of cash handovers are generally impractical to implement, at least in comparison to electronic forms of money.

Various controls on cash and restrictions of cash payments around the world show that these natural "encumbrances" on the ease of usage of cash are deemed insufficient from the point of view of the state in modern times. However, even if to widely varying degrees – famously, by 2020, only 9 percent of Swedes used cash – many societies still prefer having access to cash as a largely privacy-preserving and not trivially (electronically) forfeitable form of money.

There seems to be a wide consensus that, as an electronic form of money, CBDCs will not provide nearly as much privacy as cash and will be much easier to forfeit as part of, e.g., legal or police procedures. However, as cash is still part of our everyday life, meaning that it is there's an expectation for it to exist and there are mechanisms to mitigate its associated risks, providing a *subcategory* of cash-like CBDC may be a useful element in a CBDC introduction/transition strategy.

Pseudonymization with low levels of KYC are already an accepted approach for "holding small amounts" of CBDC, but we think that such proposals miss the core issue: even to begin to seriously consider to allow a subset of CBDC to be truly private, *at least* the following properties have to be ensured *in addition to* privacy.

- **Holding and money flow limits which can not be circumvented with "smurfing" (small transactions, multiple accounts)**: constraints on, in lieu of a better term, "individual-localized speed of money" and upper thresholds on holding must be ensured on a per natural or legal person basis. A "single account for everybody" model could easily ensure this, but on the other hand, that makes privacy a hard problem.
- **No remote transfers**: there shall be an option to require cash handovers to be tied to physical proximity in a robust way.
- **Constraints on the speed of money for the asset units itself**: no quick succession of handovers for sufficiently large amounts.

These properties, as requirements, certainly have to be *parameterized* for a given CBDC setting and may require multiple levels of subdivisions (e.g., natural persons vs. various types of businesses). These are questions of policy which we do not wish to make any recommendations about here. Instead, in the following, we define an initial outline of how SSI technologies can help with meeting the first two constraints in a technical sense – and in a privacy-preserving manner. Note that meeting the third constraint is quite straightforward in a centralized as well as hierarchical setting and does not seem to be related to identities and identity handling.

5.1 Towards cash-like encumbrances using SSI

In the following, we propose a few initial, theoretical setups, which rely on Verifiable Credentials to maintain pseudonymous CBDC balances. We fundamentally assume that *every citizen is issued a single Verifiable Credential (VC) for this purpose.* This VC may be presented to financial institutions (in the CBDC context, this can include the Central Bank) by means of *selective disclosure,* revealing only the necessary properties of the VC.

5.1.1 A simple model

In our simplest model, every user may have a number of CBDC accounts, which correspond to addresses on the CBDC ledger. The addresses are pseudonymous, hence users are able to make transactions without revealing their true identity – just like with cash. Multiple addresses per person ensure at least the possibility of applying privacy-preserving techniques to obfuscate the transaction graph (see tumblers/mixers in the cryptocurrency world).

Every user also owns the aforementioned VC issued by the government, which contains, as a *claim,* the list of CBDC addresses the user owns. If we ensure that a person can only ”open” (begin to use) a new balance if this VC is accordingly updated, the person can use this VC to prove to another organization which CBDC balances they control (*and that they do not control any other*). This is certainly a heavily *simplified model*, which puts claim management (a sensitive aspect) in the hands of the government. However, the basic approach can be taken some significant steps further; see below.

From here, all the Central Bank needs to do is to maintain, for each account, a special quota value which keeps track of how much funds were used within a given time window. Using a “leaky bucket” analogy, the account’s spendings go into a “bucket”, which also has a hole on its side: contents slowly pour out, but if the bucket is overfilled and spills, the quota has been reached. In a more technical sense, we are talking about a record that is periodically decremented by some constant value and is incremented every time some money is spent (by the amount spent).

When a transaction is requested by a user, they would present their proof describing which CBDC balances are theirs. After verifying the proof, the Central Bank checks the cumulative quotas for all accounts and whether the amount involved in the requested transaction still fits the quota. If not, then the transaction cannot be performed at the desired level of privacy.

Fig. 11 shows an overview of the model described above. In the figure, the VC contains multiple claims, each describing ownership of a specific account. It should also be possible to use a single, more complex claim that describes all owned accounts.

5.1.2 Towards better privacy with encumbrances

Privacy in the above, simplistic model is certainly not ideal. We can consider the following alternate scheme to improve on this.

- A citizen generates a *master private key*, from which a series of private keys can be derived deterministically, with the corresponding public keys and pseudonymous ”addresses” (”account identifiers”).

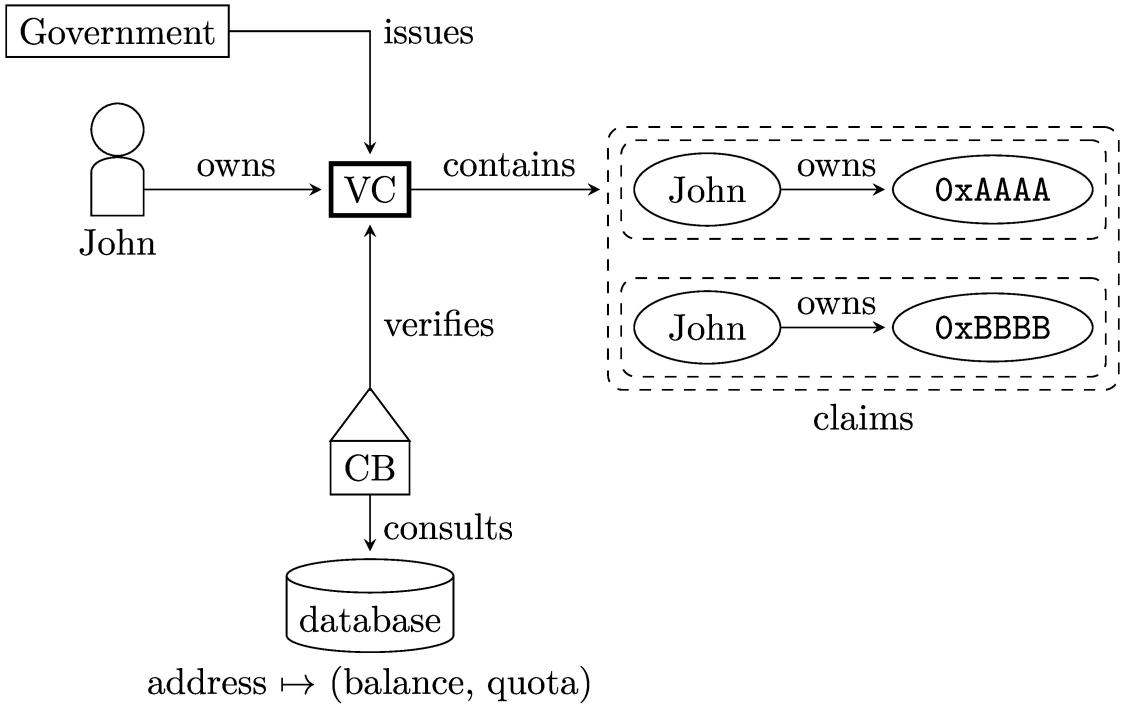

Figure 11: Overview of the simple SSI-supported cash-like encumbrances model

- Using his or her government-issued (single) identity VC, a citizen negotiates the issuance of a VC for his or her DID from the CB or another appropriate government body with the following content:
  - A hash of the master key (the master key is not shared with the issuer).
  - The lower and upper indices of the keys in the key generation sequence that are deemed active.
- The VC is published to a trusted registry (without personal information – apart from the DID), so that it serves as a basis for checks, revocations, and updates.
- Transaction requests are non-SSI based, cryptocurrency-like (digital signing with the private key corresponding to a source address), but carry a number of Zero-Knowledge Proofs.

The proof obligations of the transaction requester – in addition to signing with the proper private key – are the following.

1. The master private key underlying the private key is one of the master private keys with non-revoked hash commitments in the trusted registry. (Zero-Knowledge Proofs of set membership is a fairly well understood area.)
2. The private key used can be generated from the master private key. (*)

3. The sequence index of the private key used falls in the interval which the trusted registry currently accepts as active.

4. For the active keys *together* – that is, for all funds held by the citizen – the encumbrance requirements are observed with this transaction. (*)

The points with an asterisk (*) denote aspects where the existence of a practically feasible ZKP scheme is only a conjecture at this point yet; we are working on formulating these aspects more precisely. That being said, if the encumbraces only target maximally held amounts, then that aspect is known not to be problematic.

In summary, relying on an SSI-based eID infrastructure (which will potentially also enable tha participation of foreign citizens), a highly privacy-preserving ”cash-like” CBDC seems to be a feasible proposition.

5.1.3 Enforcing physical proximity

To simulate the proximity factor imposed by physical cash transactions, a device capable of positioning is required. For example, transactions performed using mobile phones may require cryptographic signatures by nearby cell towers, proving that the user is in the vicinity of the tower. Then, the transaction is only permitted if participants are close enough based on their cell tower signatures. Naturally, a full-fledged GPS-based approach is also possible. Fig. 12 shows a visual representation of this concept in the form of a sequence diagram.

6 Summary

Self-Sovereign Identity techniques are emerging as the next evolution of electronic identity management. In this exploratory study, we outlined how we expect them to be applicable to address key CBDC challenges. Interestingly, their potential does not seem to be constrained solely to identification and credential exchange; the fact that they facilitate selective attribute disclosure and can have singleton-like properties (e.g., we can trust each citizen to have only a single, valid, government-issued VC for identification) opens up new possibilities. Among these, we discussed techniques for equipping a (sub) CBDC with cash-like, or even more serious encumbrances – which can theoretically lead to limited CBDCs with cash-like privacy.

Our study only provided outlines; all the more so that right now SSI implementations, as the European Blockchain Services Infrastructure, are either not used very widely, or are not production ready yet. That being said, for strategic planning purposes, we believe that it is important to see that what the confluences of the SSI and CBDC worlds are and to further pursue the research questions we raised here.

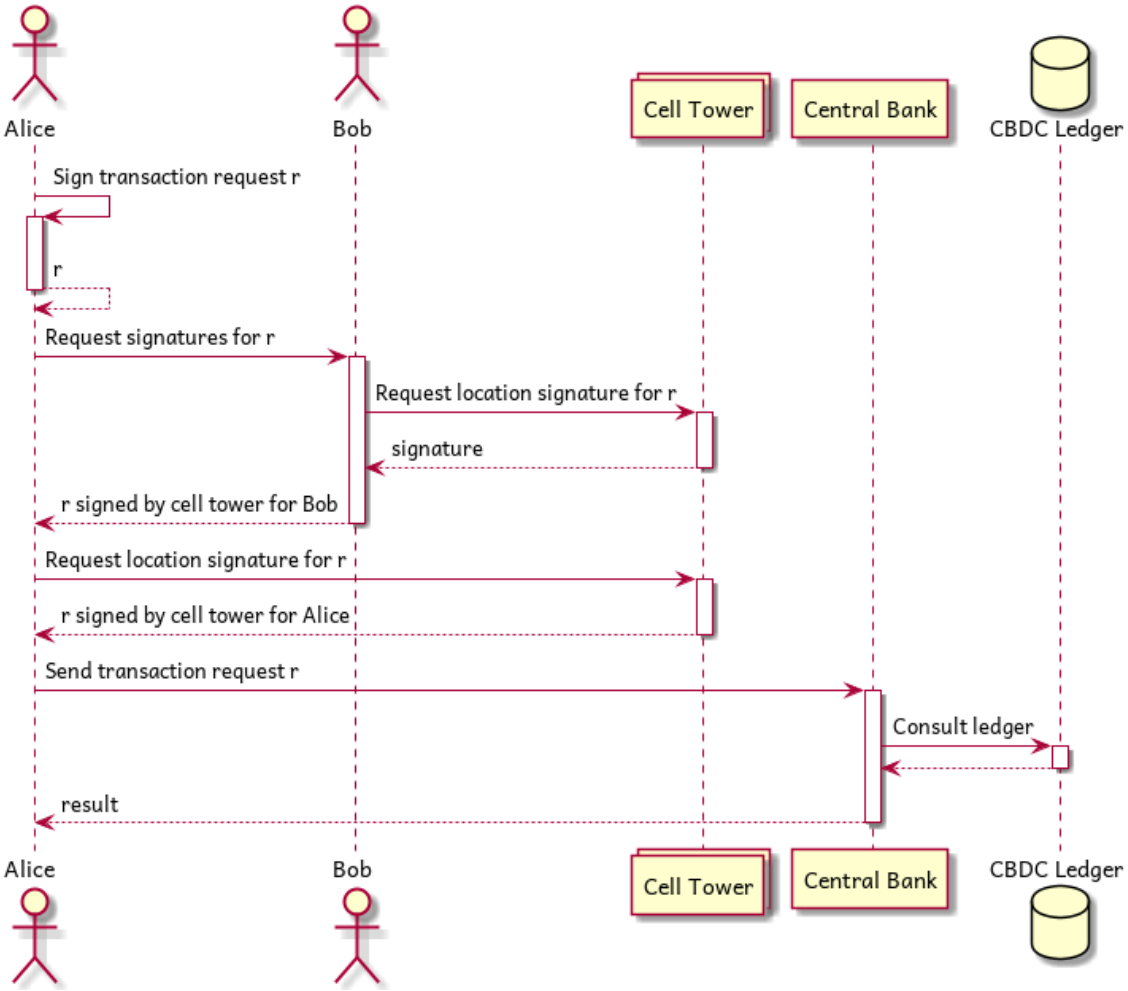

Figure 12: Proximity verification based on signatures by cell towers

References

[1] Michael Adams, Luca Boldrin, Ralf Ohlhausen, and Eric Wagner. An integrated approach for electronic identification and central bank digital currencies. *Journal of Payments Strategy & Systems*, 15(3):287–304, 2021.

[2] DIF. Home page of the Decentralized Identity Foundation. `https://identity.foundation/`, 2022. [Online; accessed 13-July-2022].

[3] EBSI. European Blockchain Services Infrastructure public documentation home page. `https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Documentation+Home`, 2022. [Online; accessed 13-July-2022].

[4] Ethereum Foundation. Ethereum Accounts. `https://ethereum.org/en/developers/docs/accounts/`, 2022. [Online; accessed 13-July-2022].

[5] Hyperledger Foundation. Hyperledger Indy. `https://www.hyperledger.org/use/hyperledger-indy`, 2022. [Online; accessed 13-July-2022].

[6] Bertalan Zoltán Péter and Imre Kocsis. ZKP-based audit for blockchain systems managing central bank digital currency. In *29th Minisymposium of the Department of Measurement and Information Systems*, pages 70–73. Budapest University of Technology and Economics, 2022.

[7] W3C. Decentralized Identifiers (DIDs) v1.0. `https://www.w3.org/TR/did-core/`, 2021. [Online; accessed 13-July-2022].

[8] W3C. Verifiable Credentials Data Model v1.1. `https://www.w3.org/TR/vc-data-model/`, 2022. [Online; accessed 13-July-2022].

[9] Fennie Wang and Primavera De Filippi. Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. *Frontiers in Blockchain*, 2:28, 2020.

[10] ZKProof Initiative. ZKProof Community Reference - Version 0.2. `https://docs.zkproof.org/reference.pdf`, 2019. [Online; accessed 13-July-2022].

About the authors

Imre Kocsis
Dept. of Measurement and Information Systems
Dr. Imre Kocsis is an assistant professor with the Critical Systems Research Group, researching and teaching blockchain technologies since 2016.

Bertalan Zoltán Péter
Dept. of Measurement and Information Systems
Bertalan Zoltán Péter is an MSc student with the Critical Systems Research Group.

Attila Klenik
Dept. of Measurement and Information Systems
Attila Klenik is a PhD candidate at the Critical Systems Research Group.

László Gönczy
Dept. of Measurement and Information Systems
Dr. László Gönczy is an associate professor at the Critical Systems Research Group.

A tanulmány a Magyar Nemzeti Bank és a Budapesti Műszaki és Gazdaságtudományi Egyetem között létrejött Együttműködés keretében és finanszírozásával készült a Digitalizáció, mesterséges intelligencia és adatkorszak műhelyben.

This work was created under, and financed through, the Cooperation Agreement between the Hungarian National Bank (MNB) and the Budapest University of Technology and Economics (BME) in the Digitisation, artificial intelligence and data age workgroup.