5-15-2019

BLOCKCHAIN-BASED ELECTRONIC IDENTIFICATION: CROSS-COUNTRY COMPARISON OF SIX DESIGN CHOICES

Anar Bazarhanova  
*Aalto University*, anar.bazarhanova@aalto.fi

Johan Magnusson  
*University of Gothenburg*, johan.magnusson@gu.se

Juho Lindman  
*University of Gothenburg*, juho.lindman@ait.gu.se

Eric Chou  
*Snowbridge Inc.*, eric.chou@snowbridge.tw

Andreas Nilsson  
*Intelleqt*, an@intelleqt.se

Follow this and additional works at: [https://aisel.aisnet.org/ecis2019_rp](https://aisel.aisnet.org/ecis2019_rp)

---

**Recommended Citation**

[https://aisel.aisnet.org/ecis2019_rp/79](https://aisel.aisnet.org/ecis2019_rp/79)
BLOCKCHAIN-BASED ELECTRONIC IDENTIFICATION: CROSS-COUNTRY COMPARISON OF SIX DESIGN CHOICES

Research paper

Bazarhanova, Anar, Aalto University, Espoo, Finland, anar.bazarhanova@aalto.fi
Lindman, Juho, Swedish Center for Digital Innovation, University of Gothenburg, Gothenburg, Sweden, juho.lindman@ait.gu.se
Magnusson, Johan, Swedish Center for Digital Innovation, University of Gothenburg, Gothenburg, Sweden; Kristiania University College, Oslo, Norway, johan.magnusson@ait.gu.se
Nilsson, Andreas, Swedish Center for Digital Innovation; Intelleqt, Stockholm, Sweden andreas.nilsson@intelleqt.se
Chou, Eric, Snowbridge Inc., Stockholm, Sweden, eric.chou@snowbridge.tw

Abstract

Electronic identification (eID) solutions constitute a critical element in digitalised society. As such, eID has been studied from a variety of perspectives, yet most, if not all existing solutions that have been studied rely on a centralised approach. With the introduction of decentralised technologies such as the blockchain, new avenues for designing eID solutions become feasible. In order to accelerate the creation of blockchain-based eID solutions and their study, this paper offers a comparison of two traditional eID initiatives in Finland and Sweden and one blockchain-based eID initiative in Taiwan. Based on this comparison, we derive insights in the form of design choices for a blockchain-based eID initiative. The findings show that the repertoire for design choices in eID solutions is expanded by the application of the blockchain. These findings are used as a foundation for discussing the design of blockchain-based eID solutions and the need for future research.

Keywords: eID, Identity Management Solution, Blockchain, Banking, Self-Sovereign Identity

1 Introduction

Electronic identification (eID) solutions have evolved as one of the cornerstones of digital infrastructures. Offering the functionality of scalable identification, these solutions facilitate the continued digitisation of society (Husz, 2018). At the same time, previous research highlights that the design, realisation and implementation of said solutions are fraught with difficulty (Hoff and Hoff, 2010; Eaton, Hallingby, Nesse and Hanseth, 2014). Issues such as ownership, responsibility and architecture (Söderström, 2016) have proven difficult to manage, resulting in substantial failures and sunk cost (Beynon-Davies, 2011).

All previous examples of eID initiatives from literature have relied on centralised or federated architectures, in line with the technological development of their time. With the introduction of distributed
ledger technology (DLT) and blockchain\(^1\) technology (Nakamoto, 2008) in the late nineties, decentralised alternatives are currently becoming increasingly technologically feasible and interesting. So far, there has been only a limited number of efforts in the development of decentralised eID solutions, whereby this study aims to contribute.

On a general level, blockchain offers the opportunity for distributed trust through a radical decentralisation of transactional data (Glaser, 2017). We posit that previous examples of eID solutions offer a potential vantage point into how blockchain based eID solutions should be designed. Lessons learned from previous empirical examples may offer us valuable insight into how blockchain based solutions should be designed for optimal impact.

Based on this, the research question that this study aims to answer is: What advantages does blockchain bring to eID compared with previous designs?

The question answers the call for research by Bazarhanova et al. (2018) on a more nuanced understanding of eID solutions, as well as that of design (Xu et al., 2017) and governance (Beck et al., 2018) of blockchain ecosystems. The study was conducted through a comparative case study of three eID initiatives (Sweden, Finland and Taiwan). The findings contribute to research by offering clear design characteristics that fuel the design of blockchain based eID solutions, while at the same time offering avenues for future research on the basis of these findings.

The remainder of the paper is organised accordingly: following this short introduction, we present a brief overview of previous findings from eID and blockchain studies, along with the theoretical framing of our work. Then, we present the results in the form of a comparison of previous centralised initiatives, and the logically derived design implications for a current blockchain-based eID initiative. This is followed by a discussion of our findings and a call for future research.

\section{Precursory Findings and Theoretical Framing}

In this section, we outline the background for our research and describe the design choices for eID solutions as a theoretical framing. In this study, we confine the scope of electronic identification (eID) solutions to official systems for strong authentication of citizens at a national scope, that are used both in private and public sectors, as discussed in (Grönlund, 2010; Eaton, Hedman and Medaglia, 2017).

\subsection{Fundamentals of Blockchain Design}

The first example application of the blockchain was the Bitcoin payment protocol and the related currency. Launched in 2008, this payment infrastructure was established to strengthen decentralised (technical) trust and to secure data through an ordered, append-only and replicated transaction log. Bitcoin promised to get rid of centralised authorities and trusted third parties, and thus make the system more secure. Later, several other applications of the underlying blockchain technology were introduced (see, for example, Elsden et al., 2018; Tapscott and Tapscott, 2016).

Blockchain may be considered a new paradigm for both trust and storage alike (Beck et al., 2018), and in line with Davidson et al. (2018), it is not merely a new transactional technology but a new market coordination mechanism. At present, the implications of the technology are still unknown, but there has been a spike of interest from the research community trying to address the issue from an empirical perspective (see Beck et al., 2018). Research on blockchain design indicates that the design space for blockchain solutions is unclear (for example Beck et al., 2018). Thus, it is uncertain what the boundaries of blockchain are, i.e., what still constitutes a blockchain technology and what does not. It is also thus unclear how exactly it differs from earlier relevant technologies.

\footnote{\(1\) Distributed ledger technology and blockchain technology are not exactly the same thing, but in this article they are used interchangeably as an umbrella term for the technology.}
Inside blockchain design space, several different configurations and design choices are possible. These choices range from very private blockchains to very public designs (Buterin, 2015). A discussion is ongoing on a number of design considerations regarding, for example, programmability (smart contracts), consensus, tokenisation and permissions (Lindman, Tuunainen and Rossi, 2017). In a recent typology, Xu et al. (2017) listed some key design choices related to the technology:

- Decentralisation (centralised, permissioned or fully de-centralised, i.e., permissionless)
- Data storage and computation (on-chain item data, item collection, computation)
- Configuration (scope, data structure, consensus, protocol, side-chains).

### 2.2 Earlier Literature on Blockchain and eID solutions

Earlier literature on identity solutions can be roughly divided into two separate streams: 1) moving existing certificates “on-chain” and 2) building new self-sovereign identity solutions on blockchain (Dunphy and Petitcolas, 2018).

- The more traditional eID stream is about decentralised trusted identity, which is primarily concerned with how to move existing trusted (non-digital) certificates of identity to the “on-chain” and how to use these proofs, for example, to sign in a decentralised infrastructure (example Public Key Infrastructure, PKI). Example services are ShoCard, BitID, ID.me and IDchainZ.

- The second stream of literature is centred around the notion of self-sovereign identity (SSI), where the idea is to build identity solutions that run on a peer-to-peer network without a need for a central coordination authority (Dunphy and Petitcolas, 2018). The main idea is that nobody except the data owner can alter personal data or remove identity-proofs, which are only stored in the user wallet. Example services are uPort and OneName. Another example of an open source-based SSI network is called Sovrin (Tobin and Reed, 2016). Sovrin is a permissioned chain, which means nodes need permission prior to connecting to the network consensus and that there is an onboarding process when the nodes want to join. There is a hierarchy of nodes to handle this onboarding process.

Recent developments in blockchain technologies promise a number of attributes that are interesting for eID design. These include, for example, that they are decentralised i.e., no single authority owns or controls the information; tamper-resistant, i.e., all changes to the data are transparent; may facilitate inclusiveness by bootstrapping user identities in new innovative ways; increase user control and may generate cost-savings by reducing the need for data replication (Dunphy and Petitcolas, 2018).

In addition to potential benefits, blockchain comes with the inherent challenges and risks associated with e.g., the immaturity of the technology, poor understanding of the governance implications, need for extensive inter-organizational integrations with existing systems, legal risks and lack of regulatory frameworks. In other words, the adoption of blockchain is not a “magic bullet” solution (Dunphy and Petitcolas, 2018) and research should be explicit in presenting how blockchain can overcome the challenges present in existing e.g., centralised or federated identity architectures and what inherent limitations does it bring.

### 2.3 Six Design Choices for eID

We summarize the design choices for eID solutions from earlier literature into six categories: solution architecture, data control, initial identification, chaining of eIDs, ecosystem architecture and strategy, see Table 1. These design choices are relevant for our data analysis and the presentation of findings.

1. **Solution architecture.** As the applications of blockchain in digital identity cases increase, it remains to be seen what is its role in new forms of digital identity (Dunphy, Garratt and Petitcolas, 2018). Dunphy et al. (2018) propose a research agenda in this regard, where the evaluation of blockchain deployability in the light of PKI challenges is one of the most prominent research directions. Inherent challenges of PKI infrastructures include operational and deployment issues,
such as certificates issuance, recovery and revocation. Another limitation in current implementations is the lack of certificates’ reusability in ecosystems with multiple certificate authorities that do not cross-accept each other’s certificates for business reasons. Thus, the investigation on how blockchain-based eID systems can “optimally replace, integrate with or disregard principles from PKI architectures” is worthwhile to pursue (Dunphy et al., 2018).

2. **Data control.** Increased user control is one of the main benefits of applying blockchain in digital identity cases. End users should be in control of their digital identities, and any personally identifiable information should be revealed only with their explicit consent. It is important to critically investigate how the choice of primary design properties of immutability, transparency or auditability and decentralization play out in digital identity applications.

3. **Initial identification.** Depending on the desired assurance levels of identification (“Assurance levels for electronic identification means,” 2015), users might be required to go through the process of initial identification at least once requiring the physical presence of the user when verifying the identity. In many identity management systems, this onboarding phase is regarded as a bottleneck, especially in highly regulated markets such as banking. There is a clear need to investigate new innovative means of user onboarding.

4. **Chaining of eID.** A number of blockchain-powered economic identity projects\(^2\) have appeared that facilitate banks and financial institutions in using blockchain to foster financial inclusion. One way to bootstrap a digital identity can be achieved by identities chaining, i.e., creating new blockchain-based eIDs based on existing legacy methods of identification. Such an approach could solve the potential challenge of the identity information locked in silos of organizations that own and control users’ digital identity-related information; and to expand the reach of legal identities.

5. **Ecosystem architecture.** On a bigger scale, the success of any digital identity initiative depends on the user uptake, which often requires interaction with governments and public agencies. While there is a strong need to comply with the local and global regulations, interoperability with legacy eID schemes is an advantage for the wide diffusion of the next generation of eID solutions.

6. **Strategy.** eID applications result from various degrees of cooperation among actors, such as partnerships, competition or coopetition. Generally, cooperating at the infrastructure level while competing at the level of service helps to derive cost savings among participants. Governments could also involve private organisations in establishing digital infrastructures for national eID schemes, and such initiatives are found to be contingent on the distribution of power dependence between the actors (Medaglia, Hedman and Eaton, 2017b, 2017a).

The traditional stream of blockchain eID literature on decentralised trusted identity has an impact on two of these six design choices: initial identification and chaining of electronic IDs, see Table 1. The SSI has an impact on three design choices of these six: solutions architecture, data control and ecosystem architecture. The sixth design choice refers to the strategies that companies are adopting vis-à-vis each other in the marketplace.

<table>
<thead>
<tr>
<th>Design choice</th>
<th>Options</th>
<th>Considerations in earlier literature</th>
<th>Example references</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution architecture</td>
<td>PKI / non-PKI / Multi-factor Authentication (Password / Biometric)</td>
<td>SSI solutions rely on PKI architecture to sign and use identity the proofs.</td>
<td>Davis, 1996; Dunphy et al., 2018.</td>
</tr>
</tbody>
</table>

\(^2\) [https://github.com/peacekeeper/blockchain-identity](https://github.com/peacekeeper/blockchain-identity)
Data control | Identity providers (IdPs) / users | SSI starts with the assumption that the user holds his/her personal data in his/her “wallet”. | Cameron, 2005.  
Initial identification | Physical / virtual | Traditional eID is interested in how to move non-digital proofs of identity to on-chain. Visiting an identity provider or a bank physically for initial identification. | Dunphy and Petitcolas, 2018.  
Chaining of eID | Yes / no | Traditional eID is interested in how to move non-digital proofs of identity to on-chain. This could be an accepted start of a chain. | Dunphy and Petitcolas, 2018.  
Ecosystem architecture | N frameworks and digital heritage | Decentralised ecosystem architectures are discussed in SSI literature. While SSIs require interoperability for cross-institutional claims of different IdPs, there would be a need to assimilate into an existing ecosystem and legacy eID schemes. | Söderström, 2016.  
Strategy | Competitive/ cooperative | In order to reach full potential, blockchain requires interoperability that in turn makes the cooperative aspect crucial for organisations | Medaglia et al., 2017a; Constantinides, Henriksson and Parker, 2018.

Table 1. Typology of design choices and options for blockchain based eID solutions.

In what follows, we investigate these six choices from our empirical data.

3 Method

The method applied in this study is a comparative qualitative interpretative case study (Walsham, 1995), where three cases were selected as a basis for comparison. Following this, we shifted to an approach of building theories from case study research (Eisenhardt, 1989). However, in this paper we refrain from developing full-fledged theory and instead limit ourselves to defining the construct of design choices.

The three cases were selected utilizing a combination of leading edge and convenience sampling (Kaplan et al., 2006). With both Sweden and Finland ranked highly in terms of digital maturity (European Commission, 2018), with a long tradition of eID solutions active in the community, we consider these two cases leading edge. At the same time, these two cases differ in terms of development and governance, where the Swedish case is cooperation-driven by the core banks and the Finnish case is a combination of quasi-cooperative banks and government regulation. The third case (Taiwan) was selected on the basis of it (to our understanding) being one of the few now active blockchain based eID initiatives. We use primary and secondary data sources for this study: interviews with regulators and eID ecosystem stakeholders, online sources such as legal frameworks and policy descriptions, and secondary documents such as research on eID in Sweden, cross-country comparisons and architectural documentation, see Table 2. Interviews on the Finnish case were conducted in person, while interviews on the Swedish case were conducted via Skype. This was complemented through ethnographic observation where three of the researchers attended the business and technical discussions in Taipei (Taiwan) in October 2018. All interviews were recorded and transcribed.

<table>
<thead>
<tr>
<th>Interviews</th>
<th>Documents</th>
<th>Online sources</th>
</tr>
</thead>
</table>
| 1. Head of division for digital government, Sweden – 08.2018  
2. Digital Management Authority (DIGG), | 1. Söderström (2016)  
https://elegnamnden.se/ |
Using the six dimensions that were summarized from the literature, we looked for their occurrences in the data (Eisenhardt, 1989). We analysed the data in two broad stages. First, we started with a ‘within-case’ analysis to familiarise ourselves with all three cases individually, increase rich understanding and identify the distinct patterns (Eisenhardt, 1989). Second, we performed a cross-case analysis in order to find analytical commonalities and differences. The cases of eID development in Sweden and Finland are more mature, and they were chosen as a base for the comparison. We searched for indications of benefits, tensions and solution peculiarities along the six dimensions from the Finnish and Swedish eID implementations. Comparing these two cases resulted in a wider perspective on the design implications that were applicable to the new blockchain-based eID initiative in Taiwan. In this stage, we applied axial and selective coding techniques and extensively referred to the design choices in search for data that corresponded to (or mismatched with) the concepts from the first stage of analysis (Eisenhardt, 1989).

4 Results

4.1 A Comparison of the Swedish and Finnish eID Solutions

In this section, we present our findings on the Swedish and Finnish eID schemes comparison (see Table 3) along with the design choices and the tensions.

<table>
<thead>
<tr>
<th>Design choices</th>
<th>Sweden</th>
<th>Finland</th>
<th>Tensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Solution architecture</td>
<td>PKI</td>
<td>Non-PKI</td>
<td>High operational costs, deployment concerns</td>
</tr>
<tr>
<td>2. Data control</td>
<td>IdPs, banks</td>
<td>IdPs, banks</td>
<td>Data stored in silos, limited federation of identity information, lack of user control, privacy issues</td>
</tr>
<tr>
<td>3. Initial identification</td>
<td>Physical at IdP</td>
<td>Physical at IdP</td>
<td>Inclusiveness or exclusiveness of user groups, user experience</td>
</tr>
<tr>
<td>4. eID chaining</td>
<td>No</td>
<td>Yes</td>
<td>Inclusiveness or exclusiveness of user groups, bootstrapping an identity</td>
</tr>
<tr>
<td>5. Ecosystem architecture</td>
<td>3 frameworks</td>
<td>1 framework</td>
<td>The governments’ involvement in regulating market-procured eID solutions G2BankID</td>
</tr>
<tr>
<td>6. Strategy</td>
<td>Cooperation</td>
<td>Competition</td>
<td>Public-private relationships, non-cooperation or cooperation among banks on a common infrastructure</td>
</tr>
</tbody>
</table>

Table 3. Comparison and tensions.
1. Solution architecture. Swedish BankID is a PKI infrastructure implementation, a technology based on asymmetric cryptography that involves the use of two different keys for encrypting and decrypting data. TUPAS – a household name for Finnish BankID – is a non-PKI solution based on symmetric key cryptography. While the Swedish BankID infrastructure is governed by a consortium of banks, Finnish banks run their TUPAS implementations separately. There are three different types of Swedish BankID: on file, on a card and mobile BankID. In BankID on a card, the digital certificate is stored on the smart card and the user accesses it using a PIN for authentication and digital signing operations. In BankID on file and mobile, public-private key pairs are generated in the bank’s central infrastructure and downloaded to the customer’s computer or smartphone. TUPAS is based on a combination of username, password and one-time codes that can be generated by a token generator, mobile app or printed on paper. In both countries, the identification service is available only to (1) citizens and permanent residents (2) holding an official identification document that are (3) customers of a participating bank. Bank-specific identifiers are widely reused across e-government and e-commerce services, and both eID implementations qualify as level of assurance (LoA) substantial according to the eIDAS regulation (European Union, 2014), neither solution qualifies for a high level because TUPAS is a non-PKI solution and due to the lack of a tamper-resistant security token for keys storage in Swedish BankID. Tensions. Because the use of digital certificates is fairly prevalent, PKI implementation involves costly operational burden across the full life cycle of certificates (Dunphy et al., 2018). The advantages of PKI over symmetric encryption include lower availability demands, better performance and reliability (Davis, 1996). Symmetric key encryption used in Finnish BankID, on the other hand, is simpler to administer because there is no need to maintain the Certificate Revocation List (CRL) servers across multiple banks. The problem with the latter implementation is that banks act as independent certificate authorities that do not accept each other’s keys, which prevents the reuse of certificates.

2. Data control. In both cases, personal data are revealed with users’ consent only. However, personally identifiable data in Swedish BankID and TUPAS are very limited and include the users’ Social Security Number (SSN) and name, which are shared with the relying party along with the digital certificate. This means that whenever the user authenticates herself, both name and SSN are shared with the relying party, which may not always be necessary. Thus, only limited personal information can be shared, and the identifiers cannot be reused outside the ecosystem. As stated by the Finnish agency, “The current solution that identity information is stored in silos within certain organisations and that you have very little control over that information – that is not a very good solution. I don’t think that it will last for many years”. Moreover, the Finnish agency highlighted the limitations of existing initiatives and the potential of blockchain-based solutions in the eID domain: “eIDAS is also built on traditional ideas that you get the identity from some government-backed provider and get certain attributes from that central register. But the concept of self-sovereign identity is much more gradual. The idea is that there are many attributes related to you. [It is up to you] with whom you share those attributes, blockchain technology kind of gives a nice tool to handle these... we should somehow find the bridge between the old world with the new one. What kind of steps would we take to reach that?” Tensions. While the identity information can be stored in a distributed manner in individual bank infrastructures, banks act as central authorities that own and control that data. Moreover, depending on each implementation, log files with user information, such as unencrypted SSN data, could potentially be in the hands of the relying parties, raising privacy questions. Personal data shared with relying parties are limited to, for example, SSN and name, and there is no support for a more discreet way of identity information sharing (i.e., anonymise some data fields).

3. Initial identification. The very first step of acquiring an eID is the initial registration process, namely binding the digital identifier with the real legal or physical person. Normally, this requires the user to visit a designated government registration authority (RA), such as the police office or a bank branch office, where the applicant’s personal details are collected, and the identity is verified. As banks become more digital and have fewer offices, the process of initial identification is becoming more challenging. Moreover, bank-procured identity verification processes need to comply with a number of regulations, such as the Anti-Money Laundry legislation, Know Your Customer and other fraud prevention checks. Initial identification is also one of the most challenging entry barriers for new
market entrants. For example, Verisec, a security company with an eID solution called Freja³, is a newcomer in the Swedish market that came up with an innovative solution for overcoming the problem. They have collaborated with a company called Aktiebolaget Trav och Galopp (ATG) in order to leverage their extensive network of shops across Sweden in which the customers can go through the identity verification process. **Tensions.** Countries worldwide may differ in their legal requirements, but universally, the initial identity verification process is concerned with linking the physical entity with the digital identifier, which requires a physical presence or done remotely with the help of software. The main distinction of bank-procured eID solutions is that the identity verification processes are regulated by law. One-time identity verification removes the need for consecutive visits to bank offices and enables not only online banking but also the use of identifiers in e-government and e-commerce services.

4. **eID chaining.** In order to create more competition in the market, Finland has mandated the eID chaining, i.e., creation of new eIDs based on existing ones. Obviously, this change has been received negatively by incumbent banks (that constitute more than 90% of all eID transactions) because the process is considered to subsidise newcomers. A few years ago, a similar situation was discussed in Sweden when universities used the “My messages” mailbox service provided by the tax agency to send out the passwords to university networks. In order to access the mailbox, students used a BankID solution to log in. “The banks were quite upset and said that [students] can’t use BankID and get an email to another eID that has a lower level of security. They called us and said that it is the tax agency that is running this message box, and said that if you don’t stop this we will stop delivering BankID to tax agencies. Of course the relationships were not so good afterwards.” The eID chaining in Sweden has not been in use since this incident. **Tensions.** Chaining of identifiers is a powerful way to overcome the challenge of onboarding and bootstrap user identities. However, some important issues arise from the chaining, including the identity theft threats and questions on responsibility. If business negotiations permit, the chaining can also help to expand the user base, include various customer groups and reduce exclusion.

5. **Ecosystem architecture.** Systems in the two countries are organised differently. The regulation in Finland that came into force in May 2017 introduced a number of changes (Ministry of Transport and Communications, 2016). First, banks have to implement changes to the TUPAS protocol because it no longer meets the requirements for strong customer authentication (SCA). Second, the new regulation makes it mandatory to integrate with Finnish BankID via service broker companies. Third, the regulation introduces a price cap for eID transactions, with the decrease for up to 70%, and allows eID chaining. These measures were aimed at increasing the competition as well as boosting the innovation in the market. Although Swedish regulators had similar objectives to widen the eID reuse, they chose a different approach. Nowadays, three optional systems cover the need for eID in the public sector (“E-ID Board,” n.d.).

- First is the electoral system 2018 that provides access to the most common eID methods in the Swedish market. BankID from Finansiell ID-Teknik BID AB is available currently, and more eID methods from the market are under review. The technical specifications in this electoral system are BankID Relying Party API and OCSP or SAML v2.0. These specifications are used by the dominant IdPs, while also technically facilitating the introduction of foreign e-credentials under the eIDAS Regulation (No. 910/2014).
- Second is the electoral system 2017 that is intended to increase the freedom of choice and provide access to new eIDs in the Swedish market. Currently, it includes the Freja eID solution from Verisec, and more eIDs have been registered and are currently under review. IdPs are required to be audited by the E-identification Board in accordance with the requirements of the Swedish Framework for eIDs and the technical specifications SAML v2.0. It is also important to note that, https://frejaeid.com/

---

³ https://frejaeid.com/
“these electoral systems are voluntary to use for [public] agencies. The agencies can also choose to go out by themselves and do procurement for eIDs, which makes situation a bit messy because you end up with some agencies just having a contract with one vendor and other with different”, comments the E-identification Board advisor.

- A third approach includes ad-hoc contractual forms for eIDs and digital signature services procurement. The regulators explain the existence of a number of options to choose from as a “... way to simulate the market, develop new and innovative solutions over time. And that we do not have just one vendor and we can change and stimulate the development & innovation in the market”, comments the E-identification Board advisor.

Together, the agreements provide a comprehensive supply of well-established and quality-reviewed eIDs in public sector e-services that does not prevent any existing solutions but rather create opportunities for the use of existing as well as future eID solutions. The eID and digital signing costs 17 ore (0.017 EUR) in Sweden. In Finland, the price decrease for eIDs has been regulated from approx. 0.5 to 0.1 EUR. As stated by Swedish regulators, the brokering concept from the Finnish case seems to be attractive and useful: “Well, we don’t have this dialogue very open with the private sector unfortunate-ly. That is something we lack in a current system - the support function. So there will be a support function now that the new agency is created.”

Tensions. In both cases, the BankID method is used as the main identification device in G2C and G2B use cases, which creates the need for governments to regulate the infrastructures. However, the governments’ involvement in regulating market-procured eID solutions differs significantly. The legislative environments in the two countries vary according to the ‘tenseness’ in relationships: Finland has decided to govern the ecosystem with a rigid framework and strict organising, while the Swedish eID ecosystem is a result of a gradually evolving heritage built over the years.

6. Strategy. The governments in both countries understand the limitations of relying on an almost monopoly BankID solution. For example, as stated by the Swedish side: “There were suggestions from agencies for government eIDs, which we are looking into right now. It is about putting certificates in national ID cards. Officially approved ID cards and you put a certificate in it and use as a way to identify yourself digitally”. Similarly, Finland is currently in the process of investigating the right forms for government-issued eID solutions: “We will get the report soon and we need to wait for it before we can do anything”. The Finnish government sends a clear message that the BankID solution has become too expensive for the use in public services, which is why the strategies to change the de facto role of BankID were created (i.e., eID chaining), and state agencies are exploring the alternatives for citizens’ eID. However, Sweden’s approach to stimulating the market differs. A distinct example is the recent proposal about the police and banks collaborating in the process of the initial identification. As explained by the agency, “Banks would like to see that the government takes wider responsibility on the identification of people. Because now you do it in bank offices and banks are getting more and more digital and closing down their offices. For example, should you just do it [first time identification] at police or tax agency where you can also get a national ID card?” Although it is yet only a proposal, there are reasons to believe that decisions of cooperative nature between banks and the Swedish government would actually follow. Tensions. One explanation of cooperative and non-cooperative practices could be the maturity stages of two solutions; i.e., in Finland, the banks could not achieve the close collaboration and a common infrastructure that the banks have in Sweden. There is also less distance and more understanding between the BankID providers and regulators in Sweden than in Finland.

4.2  Design Choices for a Blockchain-Based eID Solution in Taiwan

In this section, we discuss how the tensions identified in Swedish and Finnish cases are mitigated in the design of BankID-like solution in Taiwan (see Table 4). The solution (YesID) is currently under development and undergoing initial tests.
Design choices | Taiwan | Tensions from SE and FI | Mitigation
--- | --- | --- | ---
1. Solution architecture | PKI + Blockchain | Deployment concerns | Federation architecture enables the sharing of eIDs, certificates enabling the economy of reuse, sharing costs and ease of deployability
2. Data control | User | Data stored in silos | User centricity
3. Initial identification | Physical and remote onboard- ing | Inclusiveness or exclusivity | Freedom of choice depending on assurance level, 3 different types of eIDs
4. eID chaining | Yes, multiple ways | Bootstrapping an identity | Bootstrapping identity by making use of existing eID methods, user experience
5. Ecosystem architecture | Hybrid (legacy + new approach) | G2BankID, Legacy systems | Inclusiveness of user groups that use existing eID methods and the use of platform strategies to move from the legacy ways to new blockchain-based
6. Strategy | Coopetition | Different ways of building a common infrastructure | Working on creating an ecosystem by cooperating with incumbent CAs in the private sector, with the long-term goal that the public sector will follow.

Table 4. Design choice overview in the Taiwanese case.

1. Solution architecture. Blockchain technology can prove that a particular transaction has occurred without the ability to attest the identity of the entity that conducted that transaction. PKI technology, which has been in use for more than 30 years, implements strong authentication. Despite being a cornerstone of most modern enterprise solutions, PKI has drawbacks, namely the cost and complexity of deployment (Davis, 1996). The certificate authorities (CAs, such as banks) need to understand the security policies, and resources for management of their private keys that they need to securely host and which require periodical auditing for policy compliance. The use of PKI in combination with blockchain results in a new trust-making mechanism. YesID solution is a decentralised trusted digital identity (Dunphy and Petitcolas, 2018) that aims to solve the problem of lack of reusability of digital identities. The solution seeks to utilise blockchain to replace the certificate revocation list (CRL) checking mechanism, so that CAs do not need to maintain their own CRLs but rely on the non-reputable and transparent ledger. By providing the cross-acceptable certificates to CAs, the YesID solution aims to create a shared economy for strong eIDs. As explained by one of the stakeholders: “There is a major difference between the [YesID] system we are trying to build now and the current certificate system in Taiwan. Like I said, if you want to have a certificate issued by a particular CA you can only use it in that CA. So there is no sharing involved between the institutions. What we are trying to create now is to create this the shared economy and the environment.” The system is built on the technology of Postchain developed by ChromaWay4. The Postchain turns an SQL database into a private blockchain that uses the Practical Byzantine Fault Tolerance (PBFT) algorithm as a consensus method (Castro and Liskov, 1999). The use of a familiar set of programming tools contributes to the ease of deployment and maintenance. Based on the consensus protocol, the blockchain needs 3n+1 nodes to tolerate the failures of n nodes, thus, the minimum number of nodes is 4 (Castro and Liskov, 1999). The YesID follows a consortium-based governance model in which the entities share common interests and maintain KYC procedures agreed upon to issue YesID.

2. Ecosystem architecture. In Taiwan, nowadays, there exist two types of digital certificates: Citizen Digital Certificate Card (issued by MOICA, Ministry of Interior Certificate Authority) and financial

---

4 https://chromaway.com/
certificates issued by two companies, Taiwan CA (TWCA)\(^5\) and Chughua Telecom Financial Certification Authority (CTFCA). However, the government draws a strict line between public and private services; thus, a Citizen Digital Certificate can only be provided in G2G, G2B and G2C services. There is an exception that TWCA and CTFCA certificates are allowed to be used in tax reporting systems. There is a low take-up of TWCA, and it is reported that the solutions suffer from poor usability: of 3.75 million cases of income tax online reporting (i-TAX) in 2018, only 0.11 million were with the use of financial certificates. The approach of YesID is to integrate the legacy certificates with the new blockchain-based method. Such a hybrid solution that supports the legacy financial sector certificates from TWCA and new YesID certificates could help to gain traction, widen the use and increase the user base. Ongoing negotiations with Taiwanese banks (CAs) reveal that it is “not interesting to have yet another login function, there should be some more interesting application. Even if it [YesID] is more secure or with better user interface”. YesID stakeholders are currently thinking of the “killer app” to draw the attention of the users.

3. Data control. YesID aims to change the legacy way of using personal data by handing over the control to users. The users own their data and decide which relying party can access it and when. Users get their digital certificates issued and loaded on smartphones, which adds an inevitable layer of complexity and responsibility to users. No personal data are stored on the blockchain unencrypted; only the activities of issuing, verification and revocation are recorded. In addition, the YesID certificate supports self-attestation of attributes, i.e., private data fields created by users and those assigned by other entities, such as CAs. This feature of identity attribute sharing promotes the reuse of the attributes and enables minimal disclosure for constrained use, i.e., “need-to-know” or “need-to-retain” basis (Cameron, 2005). However, the mechanism relies upon ad-hoc trust between participants (Dunphy and Petitcolas, 2018).

4 and 5. Initial identification and eID chaining. YesID is planned to be classified into three different types of eID. The first and second ones do not involve TWCA; they are in specific certificate formats defined by YesID.

- In order to get the first type of YesID, the users need to verify their identities, either to the YesID RA or to any other RA that is part of the consortium. Alternatively, the initial identification could be done remotely with the use of optical character recognition (OCR) technology. Users first send their ID document pictures, and the second step is the interactive identity verification solution.

- The second type of YesID is created with the eID chaining; i.e., the user creates a YesID certificate on the basis of existing electronic means. “If customer already has TWCA we think they could use it chain it online with YesID on their phone. TWCA agrees with this model, because TWCA is behind the banks.” Another way of bootstrapping user identities is by using ATM cards. TWCA has another role authorised by the government; they operate so-called ‘KYC Hub’ for payment cards. With the use of a card reader connected to a computer, a software module reads the card and sends the data to TWCA Hub to query the cardholder’s identity. “TWCA could help us to verify the user’s personal ID so we could use the ATM card to exchange to YesID; you need a card reader of course. But maybe it is also possible to use the ATM machines in the future”. This approach differs from digital certificate chaining because the physical ATM card is used to verify the possession of a token.

- The third type of YesID is “to entrust TWCA to sign the YesID certificates and via our system to load it on our customers’ phone.” This type is required to support the users that are willing to use the government-recognised certificates in services that can only recognise TWCA signed certificates.

The user can be in possession of two certificate types: one of either type one or two, along with the type three. These certificates are based on different KYC and assurance levels and consequently can be used in different services. As stated by stakeholders, “In our previous design we limited the number of certificates to only one device and one certificate. But then we changed it to two: one of type 1 or 2 and type 3, TWCA signed. Type 1 verified by us and if verified remotely then type 2, type 3 is the legacy way. We believe that such a design will help us to penetrate into the market.” The revocation mechanism also relies on the initial chaining mechanism employed by the user.

6. **Strategy.** It seems that the Taiwan government’s interest in eID reuse in the private sector is limited for now. A similar attitude was observed in the Nordics before the establishment of the BankID infrastructure (Eaton et al., 2017). The YesID stakeholders’ approach is to coordinate the financial ecosystem actors to create a common infrastructure solution while competing on service levels. By engaging in cooperative competition with incumbent players, such as TWCA, the new eID method providers gain the opportunity to extend their reach and create a competitive marketplace in Taiwan.

5 Discussion and Conclusion

As seen in the Results section, the two initial (Sweden and Finland) cases of existing eID solutions display a difference in approach in the chosen dimensions. On the basis of this, we will now offer a discussion in terms of design choices made in the Taiwanese eID solutions.

![Diagram](image)

Figure 1. Consummate illustration of design choices in the three cases.

The pattern that emerges from our analysis is one of clear differentiation between the three cases, see Figure 1. First, the difference between the two centralised initiatives is substantial, with a diametrical approach to solution architecture, eID chaining and strategy. The Finnish case avoids utilizing PKI, allows for eID chaining and is based on a strategy of competition rather than cooperation, in direct contrast to the Swedish case. This opens up interesting avenues of interpretation, where we hypothesise that there is a causal hierarchy of factors in the underlying model of analysis. For instance, will the choice in strategy be contingent upon the choice of chaining, or vice versa? Without room for additional analysis, we will refrain from discussing this further and instead push this to the call for continued research.
Second, the differences between the centralised versus the decentralised cases are similarly substantial. Through utilising the blockchain in combination with PKI, the data control is shifted to the user rather than the banks/IdPs. This constitutes the most significant consequence of the blockchain design for eID solutions. Instead of continuing to amass user data in the banks or IdPs, the Taiwanese case illustrates a new approach to how we use eID solutions and how the spoils in terms of user data get distributed. This is regarded to be in line with recent European regulations, such as GDPR and PSD2. The implications of this for privacy are expected to be substantial yet fall outside the scope of this paper. In addition to this, the choice of a higher degree of loose coupling in the ecosystem architecture as displayed by the Taiwanese example shows the second implication of blockchain technology as a novel approach to handling the digital heritage. Rather than complete agnosticism and separateness, the design choice signals a clearly scoped utilizing of the existing infrastructure with the desire to avoid lock-in effects. As a consequence of this, the strategy employed is one of co-opetition rather than choosing between cooperation and competition. As in the comparison of the centralised solutions above, this opens up the question of casual relationships between dimensions.

There are three implications for future research that emerge from our study. First, the analysis shows that the design choices for eID solutions differ between countries and technological regimes. Following a centralised technology, we were surprised to see such a high degree of variation in terms of the design choices made in the Swedish and Finnish cases. This has not been amply captured in previous studies of individual initiatives (see Söderström and Melin (2012), Eaton et al. (2017), Bazarhanova et al. (2018) for example). At the same time, the pattern of design choices for the decentralised Taiwanese case showed that in most dimensions, the design choices displayed a combinatory approach; i.e., they involved combining two options from the centralised cases into one. In two dimensions, data control and eID chaining, the design choices were not combinatory but novel. Hence, we see these two dimensions as being of particular interest to future studies.

Second, following the discussion of the causal relationships between design choices in the dimensions, the use of coopetition in the Taiwanese case offers a potential avenue for continued research. Looking at the recent contributions within the platform literature, we see an increased interest in coopetition as a mode of coordination in platform settings (Basole, Park and Barnett, 2015; Adner, 2017). As found by Tiwana et al. (2010), this increases the complexity of market coordination activities, and puts a significant emphasis on governance. Hence, the issue of how the design choice of coopetition impacts governance becomes relevant for future studies, see (Svahn, Mathiassen and Lindgren, 2017; Beck et al., 2018). Third, because the Taiwanese case is contemporary, there is a lack of insight into the potential success of the initiative. The adoption of blockchain per se, however, may not be a panacea for the next generation of digital identity architectures. The research shows (Dunphy et al., 2018) that often blockchain-based eID solutions reach the decentralization that rely not upon eliminating intermediaries but “reshaping” them (e.g., trust anchors in Sovrin) using a consortium-based governance structure as in Taiwanese case. Thus, it is an important challenge to evaluate how decentralization can overcome the challenges present in centralised frameworks such as the issues of trust, confidentiality and privacy. Depending on how the initiative pans out, there is still a strong need for additional empirical studies within this field, where the case will form a relevant basis for future studies.

Our study offers two main implications for practice. First, the variation in design choices made within and between the centralised and decentralised solutions opens up indications for future design choices. This implies that the level of design freedom in terms of the dimensions analysed in this study are substantial and increase with the adoption of blockchain technology. We suggest that practitioners involved in designing eID solutions consider the described dimensions and utilise the variation displayed as inspiration for design. Our study also offers one implication for policy. With increased user-centrism in terms of data control being pushed through legislation and regulation, blockchain technology is currently still uncharted territory. Few studies have empirically described the regulative implications of the blockchain design space and design choices. We hence recommend that prior to continued legislative action, a thorough analysis of the implication of blockchain design choices be conducted.
References


