The Dynamic Effects of Blockchain-based Identity Management Adoption on Data Breaches

Sarah Mulombo Mulaji
University of Cape Town
mljsar001@myuct.ac.za

Irwin Brown
University of Cape Town
irwin.brown@uct.ac.za

Sumarie Roodt
University of Cape Town
sumarie.roodt@uct.ac.za

Abstract

The purpose of this research was to explore the dynamics associated with the adoption of blockchain-based identity management to illustrate its effects on data breach rates. A comprehensive literature review was conducted, and data was analysed using the system dynamics technique of causal loop diagram. The analysis identified key circular causal relationships which show how data breach rates could be reduced by adopting a blockchain-based identity management system like self-sovereign identity.

Keywords: blockchain-based identity management long-term effects, self-sovereign identity post-adoption dynamics, data breach, privacy and security, system circular causality.

1. Introduction

Organisations need to innovate with information and cybersecurity controls at the same pace as technological advancements to better support their businesses (Sung & Park, 2021). Blockchain-based identity is one such advancement in the field of identity management (IDM) (Satybaldy et al., 2020; Soltani et al., 2021). Within blockchain-based IDM, a distinction can be made between generic decentralised identity and Self-Sovereign Identity (SSI) (Zaeem & Barber, 2020). Decentralised identity tends to accommodate the reliance on a trusted service to validate transactions. In the SSI approach, the identity holder (i.e. user) "*owns* and *controls*" their identity without relying on a central authority and *consents* to which of their identity data can be shared with the verifier (service provider) under certain conditions (Soltani et al., 2021; Zaeem & Barber, 2020). SSI is gaining interest due to the growing rate of data breaches, identity fraud, and abuse of identity data by organizations (Soltani et al., 2021; Sung & Park, 2021).

Privacy protection regulations are increasing globally (Kuperberg, 2020; Satybaldy et al., 2020). Examples are the General Data Protection Regulation in the European Union, the Health Insurance Portability and Accountability Act in the United States, the Personal Data Protection Bill in India, and the Protection of Personal Information Act in South Africa (Singla et al., 2022). The growing security threats require information security managers to adopt innovative security strategies to address vulnerabilities in IDM systems (Demir et al., 2020; Nazareth & Choi, 2015). SSI has a privacy protection feature designed to overcome some of the challenges in traditional identity models that lead to identity abuse (Dewangan et al., 2023; Shao et al., 2020; Song et al., 2022). IDM systems deal with sensitive data known as Personal Identifiable Information (PII) (Whitman & Mattord, 2021). Unlike traditional centralised IDM, SSI is by design perceived to mitigate unauthorised PII disclosures (Ghaffari et al., 2022; Lim et al., 2023; Liu et al., 2020; Zaeem & Barber, 2020).

The adoption of blockchain-based IDM in the context of information and cybersecurity management in organisations is challenging due to the disruptiveness of the technology (Kussy et al., 2018; Sung & Park, 2021). SSI implementation might require highly skilled labour and adequate training for users to self-manage their identity data securely without third-party support (Naik et al., 2022; Liu et al., 2020; Soltani et al., 2021). Assembling a compelling business case for such a technology can be daunting. Understanding their long-term consequences might be a reasonable starting point in arguing for possible investment and proactiveness toward their smooth adoption in organisations. Post-adoption aspects of blockchain applications have not been given enough attention in research yet, especially concerning IDM use cases like SSI. Therefore, the paper attempts to answer the question: *What are the effects of SSI adoption on data breach rates in organisations?* The paper focuses on understanding the dynamic effects of SSI adoption on data breaches.

The next section details the methodology used in investigating the research question, followed by research results and a discussion including key

URI: https://hdl.handle.net/10125/107099
978-0-9981331-7-1

limitations of the research, ideas for future research and then a conclusion.

2. Research methodology

A literature review approach was adopted to investigate the phenomenon whereby existing published studies on the issue were treated as data. The procedure involved systematically searching and selecting literature before analysing and interpreting the data (Templier & Paré, 2018). The approach to analysing data involved employing the system dynamics technique of causal loop diagram (CLD) (Fang et al., 2018). Modelling a CLD involves identifying key variables associated with a phenomenon, identifying cause-effect relationships between these variables, and then applying the principle of circular causality which recognises that variables are interdependent, rather than being dependent and independent (Fang et al., 2018). Consequently, feedback loops can be identified between variables which may be positive (reinforcing) or negative (balancing). As illustrated in Figure 1, a reinforcing loop is symbolised by 'R' and a balancing loop by 'B'. (Fang et al., 2018). A combination of reinforcing and balancing loops helps explain dynamic behaviour, whereby an observed variable may increase or decrease in value depending on which loops are dominant at any point in time (Fang et al., 2018).

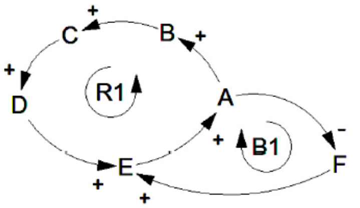

Figure 1. CLD illustration (Fang et al., 2018)

An iterative stance was adopted (Boell & Cecez-Kecmanovic, 2014) whereby cycles of reviews were conducted to familiarise with common themes on the topic and build a codebook while testing the themes through the drafting of a CLD. This allowed for scope maturation and the emergence of the research question. The initial review happened in September 2020, was updated in April 2021, then in November 2022. The CLD developed drew from existing theories and principles found in literature with the scope limited to the effects of SSI adoption on data breach rates in organisations. The final cycle of the literature review done in 2023 confirmed previously identified patterns in data and validated the final CLD. Figure 2 summarises the research process.

Papers for the review were located on the Scopus database. Scopus was filtered through the Litbaskets tool using a basket of 187 IS-centric journals (3XL) (Boell & Wang, 2019). The search string used on Litbaskets was *"Identity management" AND blockchain OR "self-sovereign identity".* The concept of "*data breach*" was initially included but then dropped because it was narrowing the search unnecessarily. The search was limited to papers no older than five years due to the relative newness of blockchain as a technology. To ensure quality, only peer-reviewed papers were targeted. Journal articles were chosen for their completeness compared to conference papers and book chapters (Boell & Wang, 2019). Papers with a narrow use case (like SSI for IoT, cloud/fog, supply chain, etc.) were excluded as they diverged from the topic. Based on the titles and abstracts, 55 papers were exported for scrutiny to exclude irrelevant papers. Apart from relevance, preference was for papers with background sections on IDM, blockchain, and SSI fundamentals. The preliminary iterative review found that it was more effective to extract principles, theory, and links to data breaches from the background sections of papers than from the empirical sections. This explained why the final 16 included papers happened to be mostly conceptual.

Six reviews:
A1: Kuperberg (2020)
A2: Ghaffari et al. (2022)
A3: Liu et al. (2020)
A4: Mulaji and Roodt (2021)
A5: Shao et al. (2020)
A6: Sung and Park (2021)

Four essays:
A7: (Fdhila et al., 2021)
A8: Ishmaev (2021)
A9: Samir et al. (2022)
A10: Soltani et al. (2021)

Five design studies:
A11: Deng et al. (2021)
A12: Elisa et al. (2023)
A13: Lyu et al. (2022)
A14: Satybaldy et al. (2020)
A15: Zaeem and Barber 2020)

One longitudinal case study:
A16: Naik et al. (2022)

Abductive coding was executed to leverage the codebook built in the preliminary review while considering new codes that emerged during the final review. The main set of new emergent codes related to SSI challenges. The extracted data (the basics of IDM, blockchain, and SSI; and links among them) were broken into lower-order codes and then synthesised by classifying them into themes of either principles, challenges, theories, or links to data breaches (See Table 1). The themes' narratives are also reported. The synthesis, alongside narratives, was further analyzed and modelled using the CLD technique to "capture circular causality" (Fang et al., 2018, p. 1306) within the SSI post-adoption system.

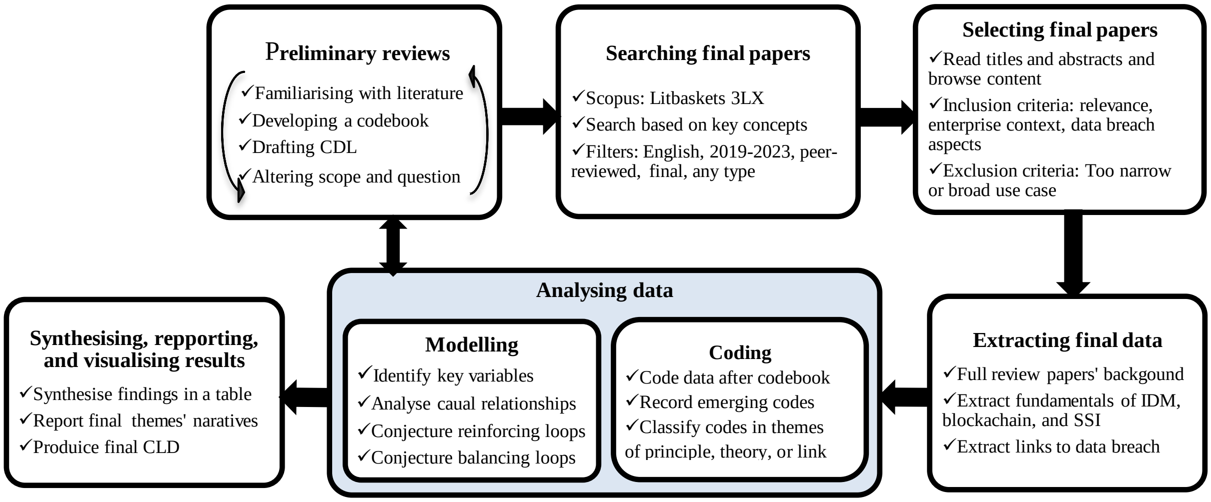
Preliminary reviews
✓Familiarising with literature
✓Developing a codebook
✓Drafting CDL
✓Altering scope and question
Searching final papers
✓Scopus: Litbaskets 3LX
✓Search based on key concepts
✓Filters: English, 2019-2023, peer-reviewed, final, any type
Selecting final papers
✓Read titles and abstracts and browse content
✓Inclusion criteria: relevance, enterprise context, data breach aspects
✓Exclusion criteria: Too narrow or broad use case
Analysing data
Modelling
✓Identify key variables
✓Analyse caual relationships
✓Conjecture reinforcing loops
✓Conjecture balancing loops
Coding
✓Code data after codebook
✓Record emerging codes
✓Classify codes in themes of principle, theory, or link
Extracting final data
✓Full review papers' backgound
✓Extract fundamentals of IDM, blockachain, and SSI
✓Extract links to data breach
Synthesising, repporting, and visualising results
✓Synthesise findings in a table
✓Report final themes' naratives
✓Produice final CLD

Figure 2. The research process followed in building a dynamic theory from literature

3. Results

3.1. Themes of principle (P), theory (T), link (L), and challenge (C)

Table 1 reports the details of three sets of principles (P1, P2, and P3), three theories (T1, T2, and T3), two sets of challenges (C1 and C2), and two sets of links (L1 and L2). The coding went from lower-order codes to higher-order codes and topic area, then also from lower-order codes to theme classification. The lower-order codes bolded and highlighted in blue are significant as they are drawn from more data incidences (greater frequency) and appear in more papers (files). Table 2 is an example of significant lower-order codes, illustrating some of the data excerpts that were coded, such as "Self-IDM reduces PIIs exposure" (the last lower-order code in Table 1). The following sub-sections provide the narrative associated with the themes as classified. These themes are interrelated.

Table 1. Codes and theme classification

From lower-order codes to higher-order codes and topic area ←					**→ From lower-order codes to theme classification**				
Topic area	**Higher-order Codes**	**Lower-order codes**	**#File**	**Freq.**	**Principle**	**Challenge**	**Theory**	**Link**	**References (files labels)**
IDM	CIA triad	Availability	1	4	P1, P2		T1		A2
		Confidentiality	2	3	P1		T1		A2, A6
		Integrity	1	2	P1, P2		T1		A6
	IDM principles	**Authentication**	**7**	**9**	**P1**				**A1, A2, A4, A5, A6, A10, A15**
		Authorisation	3	5	P1				A2, A4, A10
		Identification	4	5	P1		T2		A2, A4, A15
		Nondenial (Accountability)	4	5	P1				A2, A13, A4, A5
	IDM models	**Centralised IDM**	**6**	**7**	**P1**		**T1**		**A2, A7, A11, A10, A12, A13**
		Distributed IDM	**5**	**5**	**P1**		**T2**		**A1, A3, A7, A12, A16**
		Federated IDM	3	3	P1				A2, A10, A16
	IDM components	Identity Provider	3	3	P1				A3, A10, A16
		Service provider	2	2	P1				A3, A10
		User	2	2	P1				A3, A10
	IDM challenges	Cost of identity verification	2	2		C1	T2	L1	A1, A10
		Credential Reuse	3	4		C1	T2	L1	A4, A13, A10
		Data ownership and control	3	7		C1	T2	L1	A1, A10, A6
		Fragmented identity data	**5**	**5**		**C1**	**T2**	**L1**	**A1, A2, A4, A6, A10**
		Growing data breach rates	3	5		C1		L1	A2, A6, A10
		Increased digitalisation and complexity	**5**	**5**		**C1**		**L1**	**A3, A4, A6, A10 A13**
		Legal Requirements	3	5		C1		L1	A2, A10, A16

		Security vs Privacy	**6**	**6**		**C1**		**L1**	**A2, A6, A10, A13, A15, A16**
		System vulnerabilities-SPOF	**8**	**13**		C1	**T2**	**L1**	**A1, A2, A6, A44, A10, A11, A12, A15**
		Vulnerabilities in authentication methods	4	6	P1	C1		L1	A1, A2, A4, A10
Blockchain	Blockchain key features	Consensus Protocol	3	4					A2, A10, A12
		Cryptography	3	4					A2, A6, A12
		Security by design	3	5			T2		A2, A6, A12
	Blockchain principles	Automation	1	2	P2				A4
		Decentralisation & disintermediation	**5**	**8**	**P2**		**T2**		**A2, A4, A5, A6 A12**
		Distribution	2	3	P2				A2, A12
		Immutability	4	9	P2				A2, A4, A6, A10
		Traceability & transparency	3	7	P2				A2, A4, A6
	Implementa-tion Types	Private permissioned	3	3	P2				A2, A4, A10
		Public permissionless	4	5	P2				A2, A6, A10, A12
		Public permissioned	3	3	P2				A2, A4, A5
SSI	SSI Features	Low transaction cost	4	5	P3			L1	A2, A3, A6, A16
		Self-IDM	**10**	**14**	**P3**			**L1**	**A2, A3, A4, A7, A8, A9, A11, A13, A14, A16**
		SPOF Resilience	**5**	**7**	**P3**		**T2**	**L1**	**A2, A3, A4, A7, A11**
	The Ten Principles of SSI	Access to services	2	3	P3			L1	A10, A16
		Consent to disclose identity data	3	5	P3			L1	A10, A6, A14
		Self-Control	**6**	**7**	**P3**			**L1**	**A2, A4, A9, A6, A10, A14**
		Existence of the individual	2	3	P3			L1	A10, A14
		Interoperability	2	5	P3			L1	A10, A14
		Minimalisation (disclose no more than necessary PIIs)	3	4	P3			L1	A10, A14, A16
		Persistence of the identity	4	6	P3			L1	A4, A10, A13, A14
		Portability (transportable)	**5**	**8**	**P3**			**L1**	**A4, A6, A10, A14, A16**
		Protection of privacy	**10**	**16**	**P3**		**T2**	**L1**	**A3, A4, A5, A8, A9, A10, A11, A12, A14, A16**
		Transparency of the IDM system	**6**	**6**	**P3**			**L1**	**A5, A6, A8, A9, A10, A14**
	SSI operational components	Holder	3	4	P1				A9, A10, A16
		Issuer	3	3	P1				A9, A10, A16
		Owner	1	1					A10
		Verifier	3	3	P1				A9, A10, A16
	SSI technical components	**Decentralised identifier**	**6**	**8**			**T2**		A6, A7, A8, A9, A10, A16
		Decentralised public key infrastructure - digital wallet	4	4			T2		A8, A9, A10, A16
		Verifiable credentials	**5**	**5**					**A1, A8, A9, A10, A16,**
	SSI challenges	Adoption resistance	1	2		C2			A10
		Caricatural decentralisation	1	1		C2			A10
		Consent fatigue	1	1		C2			A10
		Disruptiveness for the enterprise context	1	1		C2			A3
		Ethics about ID and privacy	1	1		C2			A8
		Anonymity conflicts with accountability	4	4		C2			A3, A4, A5, A11
		Misconceptions	1	1		C2			A8
		Standardisation	1	6		C2			A7, A8
		Trust decentralisation	**5**	**7**		**C2**			A1, A3, A4, A8, A10
		Undesirable consequences	4	4		C2			A1, A4, A8, A14
		User responsibility burdening	3	3		C2			A4, A10, A16
Adoption	Adoption	SSI adoption in Organisation	3	4				L2	A1, A4, A6
		Adoption theories	1	3			T3	L2	A4
		Role of government	1	3				L2	A6
Link to data breach	Link to data breach	Mitigate financial loss	1	1				L1	A15
		SSI addresses IDM challenges	**5**	**9**			**T2**	**L1**	**A4, A9, A6, A10, A15**
		IDM costs	4	5				L1	A4, A6, A15, A16
		Protect PIIs	2	3				L1	A6, A15
		Self-IDM reduces PIIs exposure	**5**	**7**				**L1**	**A2, A3, A4, A6, A15**

Table 2. Example of data excerpts –lower-order code "Self-IDM reduces PIIs exposure"

From lower-order codes to higher-order codes to topic area			**From lower-order codes to theme classification**		
Topic area	**Higher -order code**	**Lower-order codes**	**Data excerpts**	**File label**	**Theme classifica -tion**
Link to data breach	Link to data breach	Mitigate financial loss	*…[Omitted]…*	A15	Link\L1
		SSI addresses IDM challenges	*…[Omitted]…*	**A4, A9, A6, A10, A15**	**Link\L1, Theory\ T2**
		IDM costs	*…[Omitted]…*	A4, A6, A15, A16	Link\L1
		Protect PIIs	*…[Omitted]…*	A6, A15	Link\L1
		Self-IDM reduces PIIs exposure	*“…the collection of PII makes the service providers primary target of attacks and results in security breaches and privacy exploitation. The recent work to eliminate the central service providers is one unique digital identity that is build, managed and controlled by identity owner (i.e., the user). Such identity that provides user centric data ownership is called Self-Sovereign Identity (SSI)” (Ghaffari et al., 2022, pp. 1-2)*	**A2**	**Link\L1**
			“The user in such a system acts as a node in the network; thus, allowing the storage of sensitive user data to shift from servers (in the conventional identity management solutions) to user devices/nodes (in the new blockchain-based paradigm). This facilitates self-sovereign identity (SSI), since the users will now have the capability to regain control of their own identity. Consequently, this minimizes various risks inherent of conventional identity management solutions (e.g. user identity abuse) (Liu et al., 2020, p. 1)	**A3**	
			…identity self-management could actually ‘lead to the practical advantage of reduced expenses’ for both users and organisations: users because of ‘the potential costs of identity theft and private data leaking of traditional centralised solutions’…” (Mulaji & Roodt, 2021, p. 12)	**A4**	
			“…a blockchain-based identity management system enables user-centered ID management, which directly transfers the management and control of ID information to individuals… increase users’ trust and control, and ease the maintenance burden” (Sung & Park, 2021, p. 1481)	**A6**	
			“…reducing the chance of exposure of these PII (Social Security Card, Healthcare ID and Driver’s License) would have saved identity theft victims from the highest amount of loss in the past 20 years” (Zaeem & Barber, 2020, p. 2)	**A15**	

3.1.1. Sets of IDM principles and challenges (P1 and C1)

At registration on a digital system, a typical centralised IDM system performs two distinctive security controls: *identification* and *authentication*, and stores identity data on a dedicated component (often a server) for future authentication. Identification labels each user with an identifier, usually in a human-friendly format like a meaningful string, while authentication provides a way for the user to prove they are legitimate, often by providing a secret (such as a password or PIN), their biometrics (such as a fingerprint), or a token (such as a smart/magnetic card) (Ghaffari et al., 2022; Soltani et al., 2021). These ways of proving identity are known as authentication methods. Identification and authentication are part of information security principles ensuring that access to a given digital system (such as a corporate website, a database, an application, etc.) is granted to legitimate users (Zaeem & Barber, 2020). To do so, additional principles are applied: *confidentiality* to prevent unauthorised disclosure of data, *authorisation* to prevent unauthorised access, *integrity* to safeguard against unauthorised modification of information, and *non-denial* to prevent a particular user from denying their action on the system (Zaeem & Barber, 2020; Lyu et al. 2022; Sung and Park, 2021). Unauthorised access to information is a security breach on data (i.e. data breach) (Naik et al., 2022).

Among IDM challenges is the fact that authentication methods have known *vulnerabilities* and can be compromised (Ghaffari et al., 2022; Mulaji & Roodt, 2021; Soltani et al., 2021). When a user’s credentials are compromised, the security of substantial systems relying on them to authorise access is breached, and identity data is exposed. This is how personal data (e.g. people’s account details, credit cards, mobile phone numbers, addresses, social security numbers, demographic information, etc.) can now be found on the internet (Sung & Park, 2021). The common IDM model includes centralised, federated, and distributed identity (which includes blockchain-based) (Fdhila et al., 2021; Ghaffari et al., 2022). In a traditional centralised IDM system, a user registers with every service they intend to use, leading to fragmented identity with *limited ID interoperability* across different domains (Ghaffari et al., 2022; Kuperberg, 2020). To overcome the inconvenience of remembering dozens of passwords, users adopt insecure practices like *reusing identical credentials* or choosing the ones that are easier for them to remember, unfortunately making it easier to guess by imposters (Lyu et al., 2022).

The main contrast between centralised and distributed IDM is respectively the presence and absence of a third-party service (a trusted central authority/component) (Fdhila et al., 2021; Satybaldy et al., 2020). Traditional centralised IDM stores a considerable number of PIIs linked to the identity on a central component to facilitate authentication. When that component is compromised, all stored identity data are exposed to imposters who can abuse or use it to gain unauthorised access to the substantial systems relying on them. This system vulnerability is known as *single point of failure (SPOF)* (Elisa et al., 2023; Ghaffari et al., 2022; Sung & Park, 2021; Zaeem & Barber, 2020). The criticality of SPOF is growing with claims of organisations (corporate, government, etc.) being the potential abusers of identity data by either selling it to third parties or by not investing enough in securing it against unauthorised access (Kuperberg, 2020). In response, SSI is a paradigm shift leveraging blockchain to achieve a user-centric approach in a distributed architecture and with a privacy-preserving propriety (Deng et al., 2021; Fdhila et al., 2021; Samir et al., 2022; Shao et al., 2020). Beyond the immediate need to address IDM challenges, blockchain-based IDM adoption might have long-term consequences on organisations' overall security posture, including the rate of data breaches (Ghaffari et al., 2022; Liu et al., 2020).

3.2.2. Set of blockchain principles (P2)

Blockchain is a peer-to-peer network securely *decentralized* that distributes cryptographically verifiable updates on transactions among participants, often without them necessarily trusting each other (Elisa et al., 2023; Shao et al., 2020). It is *transparent* because it links every block of updates with its previous and following block continually, creating an *immutable* record of updates (a chain of blocks) which cannot be tampered with without alerting substantial linked blocks and their interlinked blocks, and so on (Ghaffari et al., 2022; Sung & Park, 2021). The *traceable* distributed record of updates (i.e. distributed ledger) is irreversible in such a way that every single block must be compromised for the whole system (i.e. a chain of blocks) to fail (Shao et al., 2020; Sung & Park, 2021). The automated regulation of the network is based on a *consensus protocol* using *smart contracts* and secured based on cryptography, that is hash algorithms and digital signatures (Elisa et al., 2023; Soltani et al., 2021). *Distribution* ensures that all participants have the same copy of the database. Transparency could be achieved in a privacy-respectful manner through *anonymity* or *pseudonymity* to enable the auditability of transactions without disclosing participants' real identities (Shao et al., 2020; Sung & Park, 2021). In contrast with the traditional Client-Server network (where the server provides services for the clients to consume), a peer-to-peer network does not require a central authority since all participants are equal and can play the role of service provider and consumer (Satybaldy et al., 2020).

3.2.3. Sets of SSI principles and challenges (P3 and C2)

Within blockchain-based IDM, a distinction can be made between decentralised identity and SSI (Zaeem & Barber, 2020). Decentralised identity relies on a trusted service to validate transactions on the distributed ledger. In the SSI approach, the identity holder (i.e., user) "*owns* and *controls*" their identity without relying on a central authority and *consents* to which of their identity data can be shared with the verifier (service provider) under certain conditions (Soltani et al., 2021; Zaeem & Barber, 2020). During authentication, only *anonymised* cryptographic verifiable credentials are released on the public blockchain while the rest of the decentralised identifier data (DID) remains secure in the digital wallet, an app hosted on the user's device to *preserve the user's privacy* (Naik et al., 2022; Satybaldy et al., 2020). Hence, SSI enforces *minimal disclosure* of PIIS and *self-identity management (self-IDM)* supporting its claim of '*giving back to the user their power over their data*' (Kuperberg, 2020). In addition to privacy, SSI is claimed to be *interoperable* and *portable* (Naik et al., 2022; Satybaldy et al., 2020). The user no longer needs to create multiple accounts but can use their DID with any service provider they subscribe to, from work to online shopping. This mitigates the risks linked to credential reuse weakening traditional centralised IDM systems.

Blockchain-based identities are customisable and *less standardised*, making room for *misconceptions* about these IDM models (Fdhila et al., 2021; Ishmaev, 2021). For instance, the SSI principle of *anonymity may be problematic* since it tends to *conflict with accountability* (Shao et al., 2020). Due to its *disruptiveness*, including *power decentralisation*, SSI would require highly skilled labour to be properly implemented in organisations (Liu et al., 2020). Although SSI addresses the challenges of traditional

IDM, its inadequate implementation could lead to new sets of challenges (Soltani et al., 2021). Self-IDM puts a *significant responsibility on users* to safeguard their digital wallets and manage keys without third-party support (Naik et al., 2022). It is questioned whether SSI is *ethically* correct and there is a need to reflect on its potential *undesirable consequences* (Ishmaev, 2021).

3.1.4. Theories (T1, T2, andT3)

Some theories can make sense of claims about IDM, blockchain, SSI and their link to data breaches. They include the CIA triad (T1), SPOF (T2), and technology adoption frameworks (3), such as the technology-organisation-environment (TOE) framework. The *CIA triad* is an old standard in the computer security industry and government that traces back to mainframe development. It posits that a security breach results from an imbalance between confidentiality, integrity, and availability (Whitman & Mattord, 2021). The Trust Service Framework (TSF) (Romney et al., 2012), extends CIA by adding a fourth principle of privacy.

SPOF is a well-known theory in risk management suggesting that when the overall functionality of a system depends on a single node, there is a high risk of system collapse when that particular node fails (Deng et al., 2021; Soltani et al., 2021; Sung & Park, 2021; Zaeem & Barber, 2020). Redundancy can overcome SPOF vulnerability and achieve system resilience (Fdhila et al., 2021; Ghaffari et al., 2022). Redundancy consists of replicating the same copy of the database on every node of the system in such a way that an adversary must compromise all the nodes to breach system security. This is why a distributed system like SSI is considered SPOF-resilient (Mulaji & Roodt, 2021).

SSI adoption can be constrained or promoted by the firm contexts categorised as *technology, organisation and environment (TOE)* factors (Baker, 2012). In the organisational context, factors like firm financial resources, communication processes, and awareness would affect the decision to adopt or not adopt SSI. In the technological context, SSI characteristics like security, privacy, interoperability, etc. and the availability of IT skills and infrastructure may affect its adoption (Baker, 2012). In the environmental context, factors like industry characteristics, market structure, government regulation, and blockchain support and standardisation may affect the decision to adopt SSI. (Baker, 2012)

3.1.5. Set of links between IDM challenges, blockchain, and SSI features (L1)

IDM has known challenges: authentication vulnerabilities, system vulnerabilities (SPOF), the balance between security and privacy, credential reuse due to lack of ID interoperability etc. Identity data usually involve PIIs like name, date of birth, phone number, credit card number, medical status, ethnic group, etc. Due to the sensitivity and attractiveness of this information, a decentralized and user-centric approach is a better alternative IDM solution to preserve privacy (Deng et al., 2021; Fdhila et al., 2021; Samir et al., 2022; Shao et al., 2020. SSI, a decentralised IDM based on blockchain, which is SPOF-resilient and privacy-preserving through PII anonymisation, *mitigates multiple accounts by allowing identity interoperability*. Therefore, *SSI addresses IDM challenges*.

3.1.6. Set of links between SSI adoption and data breaches (L2)

Apart from the effect on user privacy, data breaches generate legal responsibility which generally involves financial loss and damage to the organisation's reputation (Liu et al., 2020). Depending on the motivation and skills of the adversary, data breaches may also disturb the availability of the IDM service, e.g., in the case of a Denial of Service (DOS) attack, which in turn affects the course of the business (Ghaffari et al., 2022). Adopting SSI may not only address IDM challenges but, in the long term, *mitigate the risks of data breaches by reducing the likelihood of a cyber threat agent exploiting vulnerabilities (such as SPOF, weak passwords, etc.) to perform a cyber-attack.* Although SSI adoption does not necessarily eradicate all IDM challenges and may not generate an immediate return on investment, *its self-IDM feature removes the need to store sensitive data on an insecure server*.

3.2. CLD of SSI post-adoption dynamic effect on data breaches

The above assumptions are reflected in the CLD in Figure 3. On the one hand, the diagram shows sets of variables circulating feedback that potentially increase the rate of data breaches. The effects over time are identified and labelled as reinforcing loops R1, R2, and R3. On the other hand, the diagram shows sets of variables circulating feedback with the potential to decrease the data breach rate. These long-term effects are termed balancing loops B1, B2, and B3. The following provides the narrative for these reinforcing and balancing loops.

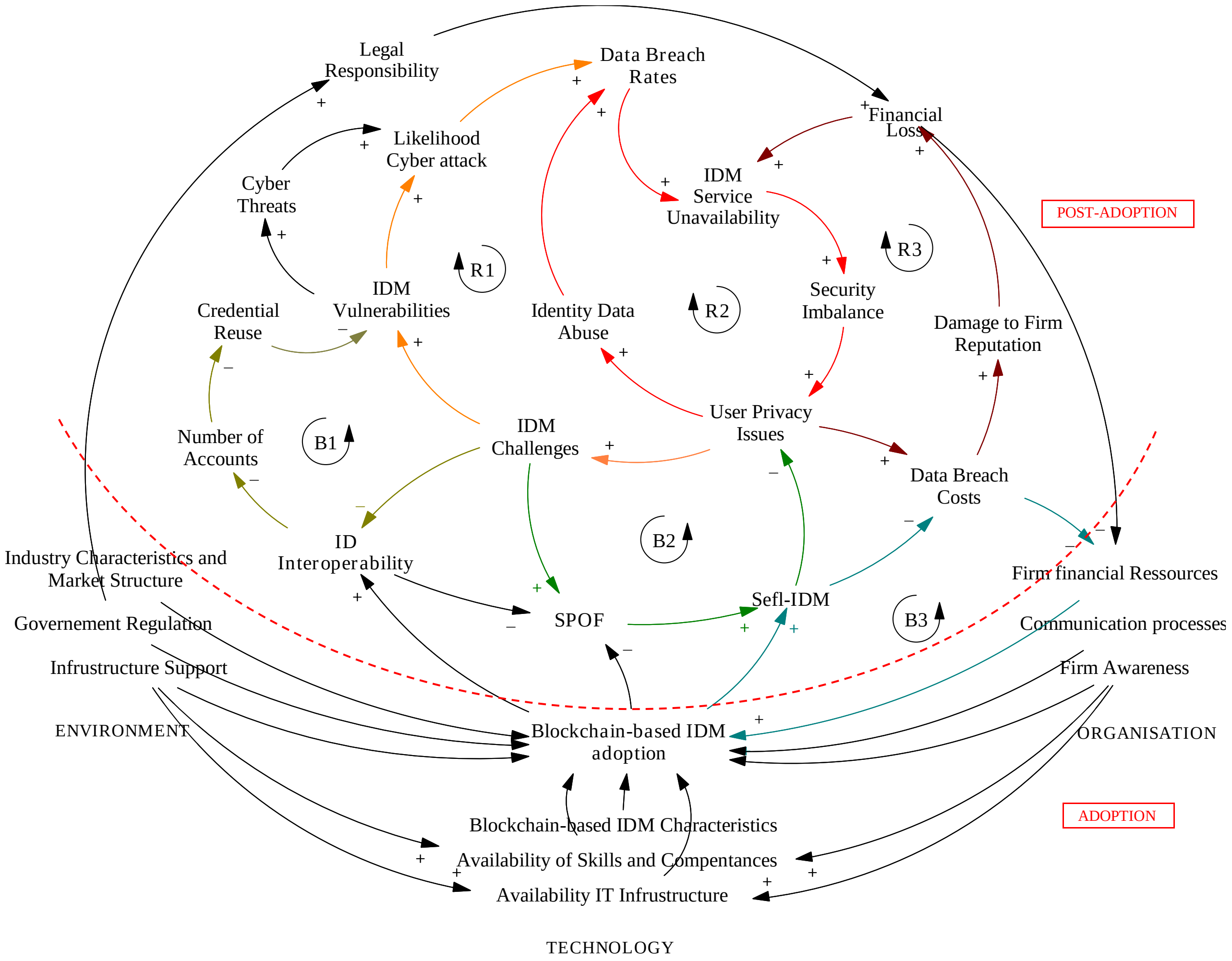

Figure 3. CLD of SSI post-adoption dynamic effect on data breaches

Loop R1 shows that IDM challenges mean added vulnerabilities in the IDM system. These vulnerabilities are likely to be exploited by a cyber threat agent to perform a cyber-attack which eventually results in a data breach occurrence (data breach rate increases). When a data breach occurs, the IDM service may become unavailable, which eventually leads to unbalanced security and infringement of user privacy. User privacy issues add more IDM challenges.

Loop R2 shows that data breaches lead to IDM service unavailability which leads to security imbalances and user privacy issues. User privacy issues give rise to identity data abuse and reinforcement of the data breach rate.

Loop, *R3* shows that infringement on user privacy leads to data breach costs and damage to the firm reputation. This in turn leads to financial losses which affects the availability of IDM services since it depends on financial resources to be properly implemented.

Loop B1 shows the effect of IDM interoperability enhanced by the adoption of blockchain-based IDM, i.e. SSI, which allows users to use their DIDs with any online service. This reduces the number of accounts per user and eventually diminishes credential reuse and hence vulnerabilities. Thus, B1 de-amplifies the effect of R1.

Loop B2 shows the effect of SPOF mitigation resulting from the adoption of blockchain-based IDM, i.e. SSI. Self-IDM negates the need to have a central authority, like a server hosting identity data, and decreases user privacy issues that occur when the server is compromised. Hence B2 de-amplifies the effect of R1 and R2.

Loop B3 shows the effect of Self-IDM resulting from the adoption of blockchain-based IDM, i.e. SSI. It represents a long-term return on investment by decreasing data breach costs as well as the overall IDM cost. This alleviates the effect on the firm’s financial resources, allowing for more investments in blockchain-based IDM (for instance by training users to self-manage their identity). The effect of B3 is to de-amplify R3.

4. Discussion

The CLD developed adds value to the knowledge area of blockchain applications, specifically the IDM use case, by revealing the dynamics of data breach rates and the effects of SSI adoption. It goes beyond simplistic claims of short-term return on investment of blockchain adoption (Lim et al., 2023), and considers post-adoption dynamics. It is challenging to assemble an accurate business case for a disruptive technology like SSI because it may not necessarily translate into immediate financial gain (Zaeem & Barber, 2020). Given the emergence of user-centric IDM approaches (Soltani et al., 2021; Sung & Park, 2021), proactive information security practitioners could use the cause-effect model proposed in this study to make a case for possible investments in their organisations. This explorative study also serves an illustrative purpose to help stakeholders better understand the long-term effects of SSI adoption on data breach rates in their organisations.

The CLD was based on theoretical assumptions and principles identified in the literature. Further studies could use the CLD to develop a stock and flow diagram (SFD) for further validation of the findings and development of a simulation model (Fang et al., 2018). Such simulation could be performed after determining through case studies variable estimates like the average rate of data breaches per day/week/month, the average number of new vulnerabilities discoverable per day/week/month, the practicality of blockchain-based IDM in terms of the number of vulnerabilities solved as a result of ID interoperability, SPOF mitigation, and Self-ID; etc. The review was limited to the effects on the data breach rate. Further research could address other areas of SSI's long-term effects like sustainable development, globalisation, ethical issues, etc. Future research could also investigate the unintended consequences of SSI adoption to reveal potential contradictions.

5. Conclusion

This explorative study investigated the dynamic effects of SSI adoption on data breaches by applying the technique of CLD. The results revealed that adopting a typical blockchain-based IDM in organisations results in layered causal relationships, which ultimately affect the data breach rate over time. Based on the CLD, it is inferred that blockchain-based IDM, specifically SSI, has the potential to reduce the data breach rates in organisations. This alleviation is due to the effect of SSI features such as interoperability, Self-IDM, and SPOF-less.

Funding acknowledgement

This work was financially supported by (1) Hasso Plattner Institute for Digital Engineering, through the HPI Research School at UCT, and (2) the Algorand Centres of Excellence programme managed by the Algorand Foundation. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the HPI or the Algorand Foundation.

References

Baker, J. (2012). The Technology–Organization–Environment framework. In *Information systems theory* (Vol. 28, pp. 231-253). Springer. https://doi.org/10.1007/978-1-4419-6108-2_12

Boell, S., & Wang, B. (2019). www.litbaskets.io, an IT artifact supporting exploratory literature searches for information systems research. *ACIS 2019 Proceedings*, Perth.

Boell, S. K., & Cecez-Kecmanovic, D. (2014). A hermeneutic approach for conducting literature reviews and literature searches. *Communications of the Association for Information Systems, 34*(1), 12.

Demir, M., Turetken, O., & Mashatan, A. (2020). An enterprise transformation guide for the inevitable blockchain disruption. *Computer, 53*(6), 34-43.

Deng, Tian, C., Chen, F., & Xian, H. (2021). Designated-verifier anonymous credential for identity management in decentralized systems. *Mobile Information Systems, 2021*. https://doi.org/10.1155/2021/2807395

Dewangan, N. K., Chandrakar, P., Kumari, S., & Rodrigues, J. J. P. C. (2023). Enhanced privacy-preserving in student certificate management in blockchain and interplanetary file system. *Multimedia Tools and Applications, 82*(8), 12595-12614. https://doi.org/10.1007/s11042-022-13915-8

Elisa, N., Yang, L., Chao, F., & Cao, Y. (2023). A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless Networks*, *29*(3), 1005-1015. https://doi.org/10.1007/s11276-018-1883-0

Fang, Y., Lim, K. H., Qian, Y., & Feng, B. (2018). System dynamics modeling for information systems research: Theory of development and practical application. *MIS Quarterly*, *42*(4), 1303-1329.

Fdhila, W., Stifter, N., Kostal, K., Saglam, C., & Sabadello, M. (2021). Methods for decentralized identities: Evaluation and insights. In *Proceedings of the International Conference on Business Process Management*.

Ghaffari, Gilani, K., Bertin, E., & Crespi, N. (2022). Identity and access management using distributed ledger technology: A survey. *International Journal of Network Management, 32*(2). https://doi.org/10.1002/nem.2180

Ghaffari, F., Gilani, K., Bertin, E., & Crespi, N. (2022). Identity and access management using distributed ledger technology: A survey. *International Journal of Network Management, 32*(2), 1-19. https://doi.org/10.1002/nem.2180

Ishmaev, G. (2021). Sovereignty, privacy, and ethics in blockchain-based identity management systems. *Ethics and Information Technology, 23*(3), 239-252. https://doi.org/10.1007/s10676-020-09563-x

Kuperberg, M. (2020). Blockchain-based identity management: A survey from the enterprise and ecosystem perspective. *IEEE Transactions on Engineering Management, 67*(4), 1008-1027. https://doi.org/10.1109/TEM.2019.2926471

Kussy, M. Y., Pobirchenko, V. V., Shutaieva, E. A., & Kakutich, Y. Y. (2018). Blockchain technologies as a stimulator of institutional transformations of the world financial system. *International Journal of Engineering and Technology (UAE), 7*(3.14), 354-359.

Lim, J.-H., Chiu, T.-T., & Traini, S. (2023). Blockchain adoption and investment efficiency. In *Proceedings of the 56th Hawaii International Conference on System Sciences*.

Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Raymond Choo, K.-K. (2020). Blockchain-based identity management systems: A review. *Journal of Network and Computer Applications*, *166*, 102731. https://doi.org/10.1016/j.jnca.2020.102731

Lyu, Q., Cheng, S., Li, H., Liu, J., Shen, Y., & Wang, Z. (2022). NSSIA: a new Self-Sovereign Identity scheme with accountability. *Security and Communication Networks, 2022*. https://doi.org/10.1155/2022/1607996

Mulaji, S. M., & Roodt, S. (2021). The practicality of adopting blockchain-based distributed identity management in organisations: a meta-synthesis. *Security and Communication Networks, 2021*, 9910078. https://doi.org/10.1155/2021/9910078

Naik, Grace, P., Jenkins, P., Naik, K., & Song, J. (2022). An evaluation of potential attack surfaces based on attack tree modeling and risk matrix applied to self-sovereign identity. *Computers and Security, 120*. https://doi.org/10.1016/j.cose.2022.102808

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management, 52*(1), 123-134.

Romney, M., Steinbart, P., Mula, J., McNamara, R., & Tonkin, T. (2012). *Accounting Information Systems Australasian Edition*. Pearson Higher Education AU.

Samir, E., Wu, H., Azab, M., Xin, C., & Zhang, Q. (2022). DT-SSIM: A decentralized trustworthy Self-Sovereign Identity management framework. *IEEE Internet of Things Journal, 9*(11), 7972-7988. https://doi.org/10.1109/JIOT.2021.3112537

Satybaldy, A., Nowostawski, M., & Ellingsen, J. (2020). Self-Sovereign Identity systems: Evaluation framework. In *Lecture Notes in Computer Science, Vol. 576, pp. 447-461*.

Shao, W., Jia, C., Xu, Y., Qiu, K., Gao, Y., & He, Y. (2020). AttriChain: Decentralized traceable anonymous identities in privacy-preserving permissioned blockchain. *Computers and Security, 99*. https://doi.org/10.1016/j.cose.2020.102069

Singla, A., Gupta, N., Aeron, P., Jain, A., Sharma, D., & Bharadwaj, S. S. (2022). Decentralized identity management using blockchain: Cube framework for secure usage of IS resources. *Journal of Global Information Management, 31*(2). https://doi.org/10.4018/JGIM.315283

Soltani, R., Nguyen, U. T., & An, A. (2021). A Survey of Self-Sovereign Identity ecosystem. *Security and Communication Networks, 2021*. https://doi.org/10.1155/2021/8873429

Song, Z., Wang, G., Yu, Y., & Chen, T. (2022). Digital identity verification and management system of blockchain-based verifiable certificate with the privacy protection of identity and behavior. *Security and Communication Networks, 2022*. https://doi.org/10.1155/2022/6800938

Sung, C. S., & Park, J. Y. (2021). Understanding of blockchain-based identity management system adoption in the public sector. *Journal of Enterprise Information Management, 34*(5), 1481-1505. https://doi.org/10.1108/JEIM-12-2020-0532

Templier, M., & Paré, G. (2018). Transparency in literature reviews: an assessment of reporting practices across review types and genres in top IS journals. European *Journal of Information Systems, 27*(5), 503-550. https://doi.org/10.1080/0960085X.2017.1398880

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage Learning.

Zaeem, R., Nokhbeh, & Barber, K. S. (2020). How much identity management with blockchain would have saved us? A longitudinal study of identity theft. In *Business Information Systems Workshops: BIS 2020 International Workshops, Colorado Springs, CO, USA, June 8–10, 2020, Revised Selected Papers 23* (pp. 158-168). Springer International Publishing.