The British Accounting Review xxx (xxxx) xxx

Contents lists available at ScienceDirect

The British Accounting Review

journal homepage: www.elsevier.com/locate/bar

Exploring dimensions of governance for different types of blockchain systems☆

Rina Dhillon, Prabhu Sivabalan *

UTS Business School, Australia

ABSTRACT

The rapid evolution of digital technologies has significantly reshaped governance. While much existing literature focuses on public blockchain governance, fewer investigate governance mechanisms of private and consortium blockchains, increasingly prevalent in society. We explore how blockchain systems enact governance using Beck et al.'s (2018) framework examining decision rights, accountability, and incentives. Interviews with eighteen blockchain experts reveal that public blockchains offer greater decision rights, less accountability and emphasise intrinsic incentives. In contrast, private and consortium blockchains adopt hierarchical governance where central entities regulate access, decision-making and behavioural norms. These systems prioritise extrinsic incentives and accountability than public blockchains. Our findings challenge the view of blockchain as purely decentralised, instead offering evidence of hybridised structures in practice. We also extend Beck et al.'s framework by studying three blockchain types and propose a systems and structure-based rationale for control in blockchains, as opposed to trust-based mechanisms (Pflueger et al. (2022)). Finally, we offer a variation on how responsibility and accountability depart, beyond extant MA studies (Burkert et al., 2011; Giraud et al., 2008) - suggesting that openness does not necessarily equate to enhanced accountability. These insights are crucial for understanding blockchain governance and have important implications for digital systems integration in organisations.

1. Introduction

The greatest challenge that new blockchains must evolve isn't speed or scaling - it's governance (Sedgwick, 2018).

Governance has undergone significant transformation with the rise of digital technologies (Bhimani & Willcocks, 2014; Brennan et al., 2019; Flyverbom et al., 2019; Möller et al., 2020; Yermack, 2017). These advancements have reshaped the ways in which organisations, institutions and individuals govern themselves and exercise control over various aspects of their operations. Among the technologies drawing significant attention from governments, businesses and academia is blockchain and distributed ledger technology. Blockchains, in particular, is increasingly impacting the conduct and nature of corporate transactions and exchange (Spanò et al., 2022).

Recent accounting literature has increasingly focused on blockchain technology, with studies exploring its applications in areas like accounting, auditing, finance and supply chain (Bellucci et al., 2022; Bonsón and Bednárová, 2019; Cai, 2018; Centobelli et al., 2022; Dai & Vasarhelyi, 2017; Fanning & Centers, 2016; Garanina et al., 2022; Han et al., 2023; Hughes et al., 2019; Kokina et al., 2017; Kshetri, 2017; Lardo et al., 2022, 2018; Liu et al., 2019; Pflueger et al., 2022; Schmitz & Leoni, 2019; Spanò et al., 2022; Tyma et al., 2022). Much of this research centres on public blockchains such as Bitcoin, evaluating their feasibility and potential uses. However, it often overlooks the development of private and consortium blockchains, which are more prevalent in business and society (Tyma et al.,

This article is part of a special issue entitled: Digital technologies & MA published in The British Accounting Review.☆ We thank the participants of the Monash Accounting Research 2023 seminar series, for their valuable feedback on a prior version of this study.

* Corresponding author.
E-mail address: Prabhu.Sivabalan@uts.edu.au (P. Sivabalan).

https://doi.org/10.1016/j.bar.2025.101588
Received 16 August 2023; Received in revised form 15 January 2025; Accepted 4 February 2025
Available online 5 February 2025

2022). These blockchains differ significantly from public blockchains, and their implications for governance and control in practice remain less explored.

The extant literature identifies two layers within blockchain governance structure. First is governance *by* blockchain, which focus on using a peer-to-peer decentralised blockchain networks to regulate user behaviours. Second is governance *of* blockchain, which relates to how the open-source community of developers design this infrastructure (De Filippi & Loveluck, 2016). Most researchers have focused on the former, aiming to achieve on-chain governance (Balcerzak et al., 2022; Dursun and Üstündağ, 2021; Ekal & Abdul-wahab, 2022; Ma et al., 2023; Reijers, 2021). However, there is limited understanding of the latter, especially how blockchain systems enact governance through controls and other elements implicit in their structure. We focus on how users engage in the design and development of the blockchain infrastructure itself.

This study is motivated by two factors. First, there has been increasing calls from academics and practitioners for a better understanding of how blockchain governance works in practice. Despite its importance (Laatikainen et al., 2023; Lardo et al., 2022) and governance being a significant challenge (Sedgwick, 2018; Zachariadis et al., 2019), "a governance framework for blockchain systems in general, for example, examining the roles, responsibilities, decision rights, or incentives of actors in a blockchain system is yet to be defined." (Ziolkowski et al., 2019, p.317).

Second, there is a need to expand the theoretical incorporation of blockchain systems into the accounting literature, particularly exploring the various types of blockchains found in society and their implications for governance and control. While these implications have been explored in the IT literature (Arrunada & Garicano, 2018; Atzori, 2015; De Filippi, 2019; Zachariadis et al., 2019), in the wider domain of management literature (Pereira et al., 2019), and recent accounting studies (Pflueger et al., 2022), direct investigation of blockchain governance *in practice* and its relation to control mechanisms remains lacking. This is crucial, as governance structures, once established, are difficult to change (Laatikainen et al., 2023). Understanding decision rights, accountability and incentives (Beck et al., 2018) of different blockchain systems enhances users' ability to select the most suitable blockchain system. Using Beck et al.'s (2018) three dimensions of governance – decision rights, accountability and incentives – as an analytical framework, we explore these dimensions within the context of public, private and consortium blockchain systems. Decision rights define who has control over governance, accountability measures how actors are held responsible for their actions, and incentives explain what motivates those actions.

The above motivations culminate in the following research question:

How do the decision rights, accountability and incentives of actors impact the governance of blockchain systems?

We interviewed 18 blockchain pioneers and industry experts, whose insights highlight that while public blockchains enable intrinsic (Tyma et al., 2022) and economic incentives, they do not offer accountability assurances from a governance standpoint (Spanò et al., 2022; Yermack, 2017). This gap drives the adoption of consortium and private blockchain governance structures in practice. These systems feature readily identifiable, hierarchy-based structures where a single central node (private blockchains) or a collection of identities (consortium blockchains) control the blockchain network through identity verification and consensus mechanisms to regulate the behavioural norms of all entities involved. While information is distributed across nodes, central actors/authorities regulate access and decision rights, aligning participant's accountability with their responsibilities. Consequently, incentives in private and consortium blockchains are more extrinsic. We argue that, though such commercially workable blockchain systems lose the pure openness and transparency of public blockchains, they create a more hybridised blockchain form that is more practical for governance and control in modern organisations.

Our findings offer three key contributions to the literature. First, we present a more hybridised form of blockchain governance than

Table 1
Expanded Beck et al. (2018) framework.

Beck's Dimensions	Public Blockchain	Private Blockchain	Consortium Blockchain
Decision rights	***Decision management:*** Distributed ***Decision control:*** De-centralised	Both decision management and control is centralised to an individual entity	Both decision management and control is centralised across a small collection of entities
Accountability	***Identity:*** Anonymous/Pseudo-anonymous	***Identity:*** Known/Verified to real entity by a single central stakeholder	***Identity:*** Known/verified by founding stakeholder group
	Resources invested: Breach results in risking loss of investment	***Resources invested:*** Breach results in risking loss of investment and reputation	***Resources invested:*** Breach results in risking loss of investment and position/reputation in consortium
	Regulatory/Legal: Responsible entities difficult to identify - anonymity	***Regulatory/Legal:*** Responsible entities identified and held responsible	***Regulatory/Legal:*** Responsible entities identified and held responsible
Incentives	***Intrinsic incentive:*** Involvement in consensus community	***Extrinsic incentive:*** Maintaining/growing resources invested	***Extrinsic incentive:*** Maintaining/growing resources invested
	Extrinsic incentive: Maintaining/growing resources invested	Reputation/brand damage from undesirable behaviours	Reputation/brand damage from undesirable behaviours

the commonly discussed public blockchain system, emphasising the role of traditional hierarchy and structural control in the practical advancement of blockchain, as opposed to the *"back-stage construction of communities relying on trust in individuals"* explained in Pflueger et al. (2022, p. 2). While Pflueger et al. (2022) relied on an archival analysis of secondary data, we offer primary empirical data encompassing experts in blockchain for three blockchain types.

Second, we advance and offer more nuance to the Beck et al. (2018) analytical framework by separately outlining how decision rights, accountability and incentives exist within public, private and consortium blockchains to facilitate blockchain governance and control. Beck et al. (2018) explain the same for a single case relating to a private blockchain. Our expanded analytical summary of Beck et al. (2018) is offered in Table 1 and discussed later in the study.

Third, we highlight the disconnect between responsibility and accountability in public blockchains, where openness and access do not necessarily enhance accountability, even when participants are identified as responsible actors (Ali et al., 2022; Ziolkowski et al., 2020). This issue, which has been overlooked in existing research, has important implications for blockchain governance and control in practice. While management accounting research to date addressed this disconnect in traditional organisations through controllability and its links to performance and reward (Burkert et al., 2011; Giraud et al., 2008), we offer a more systems-based rationale to address it, ensuring transaction integrity in digitised systems. This alternative view is less discussed and will only become more pertinent in the future.

The subsequent sections of this paper are organised as follows. We begin by presenting a review of key literature on blockchain, as well as an examination of governance from a blockchain perspective which includes the analytical framework that we use to make sense and integrate the results of our research. We explain our research method, present our findings and discuss their contributions to the literature. Finally, we offer conclusions, acknowledge limitations and suggest potential avenues for future research in this space.

2. Literature review

2.1. Blockchain – a background

Blockchain was first introduced to the world by Nakamoto in a 2008 white paper 'Bitcoin: A Peer-to-Peer Electronic Cash System'. Originally created to facilitate the use and dissemination of the well-known cryptocurrency Bitcoin, blockchain technology has since developed its use in various domains such as accounting, auditing, financial services, management and supply chain (Bellucci et al., 2022; Bonson and Bednarova, 2019; Cai, 2018; Fanning & Centers, 2016; Kshetri, 2018; Liu et al., 2019).

Blockchain technology is a distributed ledger that records and stores transactions in blocks. These blocks are maintained and stored across a peer-to-peer (P2P) network, which are chained to previous transactions, comprising interconnected blocks that allow users to view the chronological order and details of transactions (Fanning & Centers, 2016; Nakamoto, 2008; Zheng et al., 2017). Importantly, users are not able to alter transactions on the blockchain and can only have new data appended through the creation of a new block (Fanning & Centers, 2016). To fully comprehend the role of governance in blockchain systems, it is essential to elaborate on the distinctions between different types of blockchains found in business and society (Tyma et al., 2022). The next section explores the three main blockchain types commonly observed in practice – namely public, private and consortium blockchains.

2.2. Public, private and consortium blockchains

In public blockchains, every node, also known as users or participants, can access the network to read, create and validate data blocks. Public blockchains are decentralised, giving users equal access to the most updated record of all transactions entered into the system (Angus, 2018; Khatwani, 2018; Nakamoto, 2008; Zheng et al., 2017). This transparency facilitates peer-to-peer interaction and participation, allowing transactions to be executed from any location and at any time (Hughes et al., 2019; Siba & Prakash, 2016; Zheng et al., 2017). By using a consensus mechanism, trust is decentralised, eliminating the need for centralised entities to approve and confirm transactions. Public blockchains also allow users to remain anonymous or pseudo-anonymous (Cai et al., 2021) when participating in the system.

In private blockchains, sometimes also called public permissioned blockchain, every node is able to read and create blocks of data, but the validation process is restricted to and done by authorised nodes rather than using a consensus mechanism (Ziolkowski et al., 2020). Private blockchains are designed to be owned and operated by a single entity (Khatwani, 2018), and controlled by a central authority that governs what is allowed to be published on the blockchain. These blockchains are centralised in structure and provide users within the organisation with transparency related to transactions (Khatwani, 2018; Zheng et al., 2017). To maintain transaction integrity, the central authority in private blockchains only allows verified parties to participate, exercising control over the network through access and rights permissions (Yafimava, 2019; Zheng et al., 2017).

Lastly, consortium blockchains, as also known as hybrid or federated blockchains, allow only authorised nodes to read, create and validate transactions. This blockchain type combines elements of both public and private blockchains to encourage collaboration among companies to address business challenges (Mendez, 2018; Tapscott & Tapscott, 2016; Yafimava, 2019). The validation process involves selective endorsement by authorised nodes (Ziolkowski et al., 2020), whereby a predetermined number of participants are needed to achieve consensus (Yafimava, 2019; Zheng et al., 2017). This blockchain type maintains a level of control over the network as noted in private blockchains, while also offering increased security akin to public blockchains by not requiring the need to trust a central entity to validate transactions (Yafimava, 2019; Zheng et al., 2017).

One of the essential components of blockchain technology is the integration of smart contracts. Smart contracts consist of code or source code that represents self-enforced and self-executed computational if-this-then-that (ITTT) agreements between parties (De

Filippi et al., 2021; Laatikainen et al., 2023; Pflueger et al., 2022). These contracts offer fundamental functionalities based on pre-defined conditions that expands the potential use cases, applications, and capabilities of blockchain technology, including token issuance and management and recurrent conditional transactions, among others (Laatikainen et al., 2023).

Tyma et al. (2022) offer a visualisation of the three blockchain types, originally sourced from ICOinRating.com (2018). We provide the same below to offer to visually explain the three different types of blockchains found in practice (Fig. 1).

2.3. Blockchain in practice – going beyond cryptocurrency

While blockchain technology is widely recognised for its applications in cryptocurrencies like Bitcoin, it has proven to be valuable in various other industries. Supply chains (Azzi et al., 2019; Chang & Chen, 2020; Francisco & Swanson, 2018), the energy sector (Andoni et al., 2019; Mika & Goudz, 2021), and finance (Tapscott & Tapscott, 2016; Treleaven et al., 2017) are some of the areas where blockchain has demonstrated its utility. One notable application is the emergence of decentralised finance (DeFi) built on blockchain, which operates without relying on central intermediaries such as banks. These services are very different to the more traditional financial services that are more commonly known due to their decentralised, inter-operable and transparent features (Chen & Bellavitis, 2020).

Blockchains also enable Decentralised Autonomous Organisations (DAOs), which presents a new decentralised governance form. DAOs are innovative blockchain systems that offer a range of benefits, including transparent decision-making processes, automated operations, formalised rules, and the decentralisation of power, among others (Faqir-Rhazoui et al., 2021). Members of a DAO can participate in voting on various matters, such as the allocation of resources within the organisation or changes to the DAO's code. In some blockchain systems, particularly in DAOs and DeFi applications, specific governance tokens are used for voting purposes. Typically, governance tokens adhere to the principle of one token, one vote, which promotes decentralised governance via the equal distribution of voting power among the community (Aramonte et al., 2021; Mondoh et al., 2022).

The next section summarises the extant literature on blockchain governance as investigated through the lens of various conceptual spaces, including corporate governance, IT governance, internet governance, open-source governance, organisational governance and platform governance (for a comprehensive review, see Liu et al., 2023).

2.4. Blockchain governance

Governance has been present since ancient times and is conceptually understood as the exercise of authority and control to ensure accountability and promote transparency (Mahanti, 2021, pp. 109–153). Its usage has significantly expanded, encompassing various contexts. In the context of accounting, according to the Institute of Management Accountants (2021), governance refers to:

> "the framework of policies, processes, and controls that guide the management and decision-making processes within an organisation"

More generally, the Institute on Governance (2023) determines governance as drawing on four key dimensions:

> "who has power, who makes decisions, how stakeholders make their voice heard and how account is rendered, i.e. how are decisions made, who has a voice in making these decisions and ultimately who is accountable."

Understanding blockchain governance is crucial for three key reasons. First, effective governance ensures the sustainability of

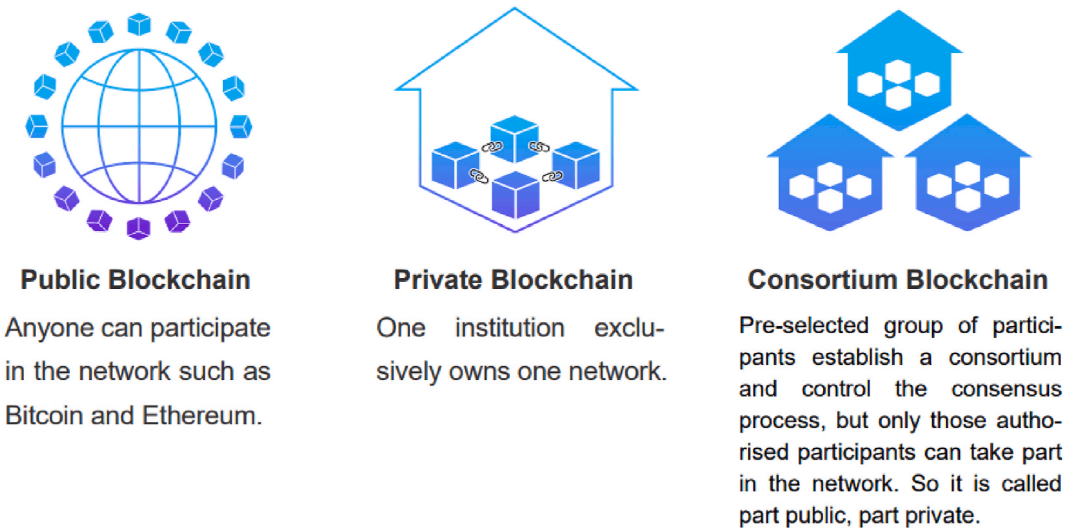

Fig. 1. Visualising Different Types of Blockchains (Tyma et al., 2022 *(p.1634)*; originally sourced from ICOinRating.com, 2018).

blockchain as a novel type of distributed ledger technology (Balcerzak et al., 2022) by enabling informed decisions on the technology's evolution (De Filippi & Loveluck, 2016). Second, it is essential for successful blockchain implementation, allowing systems to adapt, evolve and engage with users in business and society (Pelt et al., 2021). Third, given the distributed nature of blockchain technology, governance plays a critical role in managing and coordinating blockchain communities towards shared goals (Valdivia & Balcell, 2022). For businesses, blockchain governance must align with their expectations and needs, similar to how stock exchange regulations guide companies listing shares (Yermack, 2017). Understanding blockchain governance also provides policymakers with essential insights and relevant recommendations (De Filippi, 2019).

In delving into blockchain governance, it is essential to highlight two distinct coordination mechanism that governance can assume in the context of blockchain. These are governance *by* the blockchain infrastructure and governance *of* the blockchain infrastructure (De Filippi & Loveluck, 2016). Governance *by* the blockchain refers to the utilisation of blockchain technology to enhance the co-ordination of existing behaviours and actions (De Filippi & Loveluck, 2016). Within this context, blockchain technology serves as a support tool to optimise current governance processes. For instance, in Bitcoin, protocol or a blockchain may be employed to automate and implement governmental procedures.

On the other hand, the governance *of* blockchain requires developing, adapting and maintaining the blockchain technology itself, which is managed by the community of blockchain stakeholders (De Filippi & Loveluck, 2016). This latter mechanism of governance is the primary focus of interest in this research, which is interested in understanding the means and processes of governing and controlling the various actors utilising a blockchain system (De Filippi & Loveluck, 2016).

While there is no universal definition of blockchain governance, there are several key concepts that are commonly referred to in the extant research. Besides the fundamental distinctions between governance of the blockchain system and governance by the blockchain system described above, Reijers et al. (2021) differentiate between off-chain and on-chain governance. On-chain governance refers to the direct encoding of rules and decision-making processes into the blockchain system that cannot be easily bypassed due to the rule of the underlying blockchain code. Off-chain governance, on the other hand, refers to non-on-chain rules and decision-making processes that impact the operations and subsequent development of blockchain systems.

The literature also considers governance from an external as well as internal perspective. External governance involves decision-making processes made by *outside actors or outsiders of* the blockchain system (such as the community, media and general public), while internal governance relates to decision-making and governing processes involving inside actors or insiders of the blockchain system itself (Hsieh et al., 2017; Hsieh et al., 2017 (p.7) identified 3 levels of internal governance within a blockchain: (1) "owner control at the *blockchain level*"; (2) "formal voting on the *protocol level*"; and (3) "centralised funding at the *organisational level*".

Like the 3 levels provided by Hsieh et al. (2017) within a blockchain, recent research has determined several blockchain governance components, depending on the analytical lens or research approach used by the authors. For instance, studies rooted in IT governance theory have highlighted decision rights, accountability, and incentives as key dimensions (Beck et al., 2018). On the other hand, researchers drawing from the theory of platform have identified 3 crucial components of blockchain governance relating to access, control, and lastly incentives (Schmeiss et al., 2019). More recently, Pelt et al. (2021) developed and proposed an integrative blockchain framework where blockchain governance encompasses six aspects, "namely formation and context, roles, incentives, membership, communication, and decision-making, which interact across three layers: off-chain community, off-chain development, and on-chain protocol" (p.29-30).

This section has provided several frameworks that offer varying lenses to view blockchain governance. While Pelt et al. (2021) highlight "on-chain protocol" and the "decision-making" category in blockchain governance, Beck et al. (2018) focus on "decision rights" (explained further below) which better aligns with blockchain contexts, where many participants have rights without necessarily making decisions about the blockchain. Further, Hsieh (2017) focuses on owner control, formal voting and funding, but overlooks incentives, which are central to blockchain governance according to our literature review and discussed in our empirics. Therefore, we find Beck et al. (2018)'s blockchain governance framework most relevant for our study, as it allows for a systematic analysis and interpretation of our empirical data. Given our interest in understanding the governance *of* blockchain systems in practice and synthesising the extant literature provided in the previous section, we draw on and seek to expand Beck et al. (2018)'s IT Governance Framework, which is detailed in the next section.

3. Analytical framework

In Beck et al. (2018), blockchain governance requires the interaction of the level of centralisation in *decision rights*, whether *accountability* is enacted institutionally or technically and the degree to which *incentives* are aligned to the system design's goals. This framework derives 3 key governance dimensions, namely: (i) *decision rights*, which pertain to the rights enabling one to govern and control actions; *accountability*, which assesses the extent to which actors can be held responsible for their (in)actions and lastly (iii) *incentives*, which highlight the motivations driving actors to take specific actions.

Decision rights refer to the entitlements governing control over specific assets. Beck et al. (2018) identified two types of decision rights: decision management rights, which enable the generation of decision proposals, and thereafter the implementation or execution of decision(s), and decision control rights, which involve making a decision about implementing a decision proposal and monitoring the decision agents' performance. In essence, decision rights ascertain the level of centralisation, whether the power to make a decision is concentrated in a single actor, a small group (centralised), or distributed among multiple entities (decentralised). Beck et al., 2018 illustrated that while the blockchain economy aims to prioritise decentralised forms of decision-making, currently, there remains a significant level of centralisation.

Decision-monitoring rights is intrinsically tied to accountability. Using accountability theories, Beck et al., 2018 argued that being called "to account" (p.1022) for one's actions forms the fundamental essence of accountability, although it represents only a facet of the accountability relationship. Accountees need to reflect on their choices and the resulting outcomes. "Enforcement mechanisms" (p.1022) play a vital role. To prevent self-review, self-interest and self-penalty, decision management and control rights are typically separated. Accountability is operationalised through contracts, legal frameworks and IT infrastructures, with blockchain technology shifting accountability towards technical mechanisms, like smart contracts. Beck et al. (2018) anticipate that institutions will remain key players in driving accountability in blockchain activities in the future.

Lastly, incentives motivate individuals or entities to act. Beck et al. (2018) described two types of incentives: "pecuniary incentives and non-pecuniary incentives" (p.1023). The former relates actions to monetary rewards (i.e. rewards that can be monetised) while the latter relates actions to non-monetary rewards such as "privileges, visibility, or reputation" (p.1023). Quoting Ba et al. (2001), Beck et al. (2018) explain that incentive alignment occurs "when the system's embedded features induce users to employ the system consistent with the design objective" (p. 227). Essentially, the alignment of incentives within a system allows actors to choose how they might behave, but at the same time, the use of incentives in systems make actors more inclined to choose actions that are more in line with the goals and interests of the system's design. Beck et al. (2018) highlighted that incentives play a pivotal role in the efficient functioning of the blockchain economy, as they are essential for achieving the consensus that underpins the blockchain.

Without proper alignment of incentives, blockchain nodes may not participate in consensus. Misaligned incentives could also jeopardise the blockchain system's integrity and cause blockchain practices to fail. Beck et al., 2018 argue that blockchain technology has the potential to produce a blockchain economy, which they refer to as a novel "economic system" (p.1020). While the digital economy has already become widespread, involving trade in digital goods and services, the blockchain economy surpasses its scope. With blockchain technology, "agreed-upon transactions" (p.1021) can be autonomously enforced or governed through smart contracts, following predefined rules. This could lead to the emergence of new organisational structures, which operate with governance rules aligned with the blockchain's logic and which challenge traditional concepts of governance.

We summarise Beck et al. (2018) three dimensions of governance in Fig. 2, which provide the analytical lens through which we analysed the research data and describe the research findings.

For each blockchain type found in practice, we wanted to better understand how decision-making and control works, and using Beck et al. (2018)'s distinctions between decision management rights and decision control rights, we interrogated whether these rights were held by fewer individuals/entities or separated across a wider range. Before doing so, we will first outline the research approach and data collection methods used in this study.

4. Research method

4.1. Research context

This study utilises qualitative research methods to investigate the Australian blockchain industry, incorporating perspectives from active, participating blockchain industry specialists. The Australian setting is particularly appropriate, as Australia holds a leadership

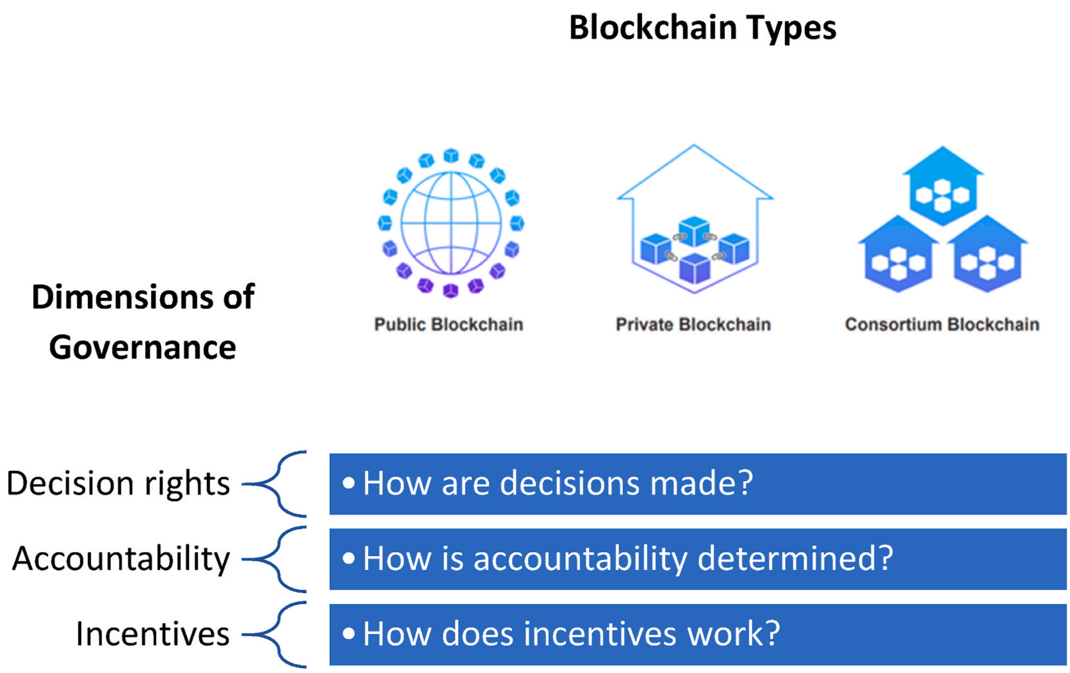

Fig. 2. Beck et al. (2018)'s blockchain governance framework (created by authors).

position in the development of blockchain and DLT standards within the International Standards Organisation (ISO). In addition, Australia possesses the necessary technical expertise and knowledge to gain profound insights into how governance and control is established through the practical application of blockchain technology (Eyers, 2018; Ølnes, 2017).

Secondly, Australia's pioneering role in the global financial landscape is exemplified by the Australian Securities Exchange (ASX), which has invested considerable funding to replace essential processes such as asset registration, clearing, settlement, and other post-trade services with a blockchain-based platform. This significant step is crucial for the smooth functioning of the Australian financial market (ASX, 2023). In addition, Australia's commitment to the adoption of blockchain technologies extends beyond the financial sector. The government has actively encouraged research and exploration of blockchain's potential applications in both the public and private sectors (Coyne & McMickle, 2017; Ølnes, 2017) through grants and incentives. This forward-thinking approach showcases Australia's leading position in implementing blockchain solutions across key sectors of the Australian economy.

Finally, the Australian government has taken a proactive approach towards advancing blockchain technology through the launch of The National Blockchain Roadmap (Commonwealth of Australia, 2020). This strategic initiative outlines the Australian government's commitment in investing, regulating and promoting innovation in the blockchain sector, with aims to foster widespread adoption throughout the country. The remarkable progress in blockchain implementation within various private and public entities in Australia serves as a testament to the nation's reputation as a world leader in this cutting-edge technology.

4.2. Research data and analysis

Our data collection occurred over ten months. To ensure a comprehensive understanding, data was gathered and analysed from diverse individuals working across various organisations in the blockchain sector (Appendix 1). Interviews were conducted with eighteen blockchain experts representing different sectors within Australia. The participants in our study represented a diverse set of industries encompassing communication services, consumer discretionary and staples, energy, financial services, health care, industrials, IT, materials and real estate.

To strengthen the credibility of our findings, we conducted a follow-up interview with two respondents to triangulate their perspectives with those of other participants. The contributing experts comprised auditors, developers, lawyers, product managers, and solutions architects. Various means of communication, such as sending emails, direct messaging, attending industry forum events, and call-calling via phone were utilised to approach the interviewees. Personal networks and industry forum events were used to identify and choose the final interviewees. Interviews were semi-structured, lasting between 30 and 120 min. Most interviews (eighteen out of twenty interviews conducted) were held face-to-face. The other two interviews were conducted over the web conferencing platform Zoom as the interviewees resided in another part of Australia.

The primary objective of the interviews was to gain a holistic understanding of the various blockchain types in practice, focusing on governance and control mechanisms. Each interview commenced by delving into the interviewee's professional background and blockchain expertise, which helped identify. The blockchain system the interviewee specialised in. Throughout the interview, the researchers utilised probing techniques to encourage examples that clarified key concepts (Bryman, 2019). Towards the conclusion of the interview, interviewees were invited to share any additional insights, often offering further thoughts on governance and control in blockchain systems. Occasionally, broad clarification questions were used to allow the conversation to flow naturally, as advocated in Kvale (2007).

At the beginning of each interview, every participant provided their expressed consent to record their session. During the interviews, the researchers recorded and captured the conversation using a mobile device, while simultaneously writing down notes to capture essential insights and thoughts shared by the interviewees. To transcribe the interviews accurately, the audio was processed using transcription services, Rev and Temi. The resulting transcripts were then carefully cross-referenced with the original audio to ensure consistency and accuracy in the transcription process.

The data coding process was conducted by the lead author and NVivo software (version 12) was utilised for coding the data, employing thematic analysis as a method for "identifying, analysing, and interpreting patterns of meaning ('themes') within qualitative data" (Clarke & Braun, 2017, p. 297). Thematic analysis facilitated the researchers in discovering common patterns within and across the interviews, enabling an assessment of key themes that emerged (Vaismoradi et al., 2013). During the coding process, the researchers inductively identified significant statements – paragraphs, phrases, or sentences – directly related to governance and control, depicting aspects of both these constructs as conveyed by each interviewee.

A comparison of these significant statements was then undertaken, with particular focus given to themes that emerged consistently among different participants. This iterative process continued until thematic saturation of key and related categories (Guest et al., 2020), providing a comprehensive understanding of how governance and control is enacted within the different types of blockchain systems, as identified by the interviewees and observed in practice. To complement our interview data and ensure corroboration and triangulation (Flick, 2018, pp. 527–544), we augment our study with an extensive analysis of blockchain use cases, white and yellow paper that are publicly documented and that relate blockchain to governance and control. The subsequent section presents our detailed results.

5. Results

Applying the Beck et al. (2018) conceptual dimensions, namely decision-rights, accountability and incentives, we organise and present our findings from blockchain experts regarding the governance and control of the three types of blockchains (public, private, consortium). We delve into the conceptual analytical elements of each across the three blockchain contexts separately, but will proceed to coalesce our learning across all three in our "Discussion" section, where Table 1 offers an expanded framework to Beck et al. (2018), incorporating all three conceptual dimensions for the three blockchain types.

5.1. Decision rights

5.1.1. Public blockchains

Blockchain systems are ostensibly organised in a decentralised manner. The nature of this decentralisation, however, is limited to decision rights in practice. As explained by blockchain experts, the aim of implementing public blockchains is to achieve the benefits of a higher level of decentralisation and autonomy for the code and application in practice – whereby no one is in control of the network. As a public blockchain includes both an open community and an open source code:

> *… anybody can see what the organisation is doing and see the code behind the* (public) *blockchain … you can see people contributing to the building of the blockchain and making features for the blockchain …* (Interviewee 10, Blockchain Developer)

> *… it depends on, you know, the governance process around the infrastructure side of things. So, in the case of an open public blockchain, like Ethereum or Bitcoin, the governance is somewhat decentralised, which means there's no central entity controlling the upgrades. There may be a central entity developing software for the upgrades, but that doesn't necessarily mean those upgrades need to be up taken by the network. … It's up to the network effectively to act as a collection of individuals to update their software based on effectively their own incentives …* (Interviewee 4, Solutions Architect)

Despite public blockchains not being perfectly decentralised, certain groups play a significant part in the advancement and endorsement of public blockchains in practice. In its current development phase, decision-making authority remains highly centralised given the level and permissions required to execute a change on the blockchain:

> *The ERC is Ethereum Request for Comments. It's publicly put out there, people could debate on it and comment on it. There's other forums out there, there's the Ethereum GitHub where people can have their proposals written up as the documentation side of things. The conversation side of things can happen in other forums … so it's a very open and decided upon. But in the end, it's those who have the means and the permissions to integrate that in the protocol who can actually do it* (Interviewee 16, Blockchain Developer)

> *… what a lot of smart contract makers will do is they will give themselves basically permissions for their smart contract. So, what this means is that if something goes wrong with the smart contract or it doesn't act behaviourally, they will basically re-control the contract and then do the changes they need to get it back to the correct state … they'll make these smart contracts that are fully decentralised, but then the owner of the contract in there they've coded into their smart contract that they still have permission to do whatever they want …* (Interviewee 12, Solutions Architect)

Many blockchain experts highlighted the issue of centralised decision rights, particularly after the 2016 hack of the Decentralised Autonomous Organisation (DAO) (Wang et al., 2019). The DAO, governed by code and smart contracts on the Ethereum (public) blockchain, raised a substantial amount of funds but had a vulnerability that allowed a cyber-attacker to steal millions of dollars' worth of Ether. This breach challenged the immutability principle of blockchain, prompting a tough decision within the Ethereum community. Eventually, a majority chose to perform a hard fork[1] to create a new blockchain, reversing the hack and returning the stolen funds to their rightful owners.

In narrating another blockchain breach example where decision rights were ultimately centralised, Interviewee 17, a very experienced developer in the blockchain space, alluded to the lengthy resolution time required to resolve complex issues and disputes in blockchain systems:

> *… I think there was a problem with that ZenCash. In the original paper, someone transcribed it, and there was a wrong formula somewhere. So, then they found that all the systems that were using it were potentially vulnerable. So, the developers or the people who found it and implementing the change, they had to go top secret for six months or something, to get all the other things* (systems) *synchronised. And then they released the fact that the algorithm was flawed, and these are the measures to counter it …*

An analysis of online records reveals that malicious actors gained control of over51% of the network's hash rate (Boukis, 2019), allowing them to manipulate the blockchain and double-spend ZEN coins. In response, the Horizen team and broader community made several security improvements, including changing. The network's consensus algorithm and switching from to Equihash-BTG to prevent future 51% attacks. They also enhanced network monitoring, collaborated with exchanges and mining pools to prevent the stolen coins from being traded, and activated an alert system to minimise the impact. In a media interview, Dr. Luca Carmelli, Country Manager of ZenCash, described these steps, which were praised as a high quality and effective response (Lugano, 2018).

The two blockchain breaches above and many since then highlight that public blockchain governance has been reactive to events of crises or dispute. While decision management is decentralised, allowing participants to initiate changes and improvements to the blockchain system, decision control is still very much centralised as the authority to ratify or approve decisions proposed through the decision management process lies in the hands of a designated group, such as blockchain developers. Although initial phases may

[1] A hard fork in blockchain refers to a significant and permanent divergence in the protocol of a blockchain network, resulting in the creation of a new block that follows a different set of rules from the original chain. This typically occurs when there are disagreements within the community about the direction of the blockchain's development or changes to its rules.

involve centralised decision rights, this centralisation can pave the way for later decentralisation; however, in practice, centralised control remains preferred by many entities. For example, as explained by a blockchain solutions architect:

> *… you may have a phase where you still have complete permission of the smart contract, and then in a future iteration once you have full faith that the smart contract is working, you may phase that out and remove yourself as the person who got permissions. You can put that into your smart contract that, "At a later date I can invoke this and will take away all my permissions." So, that's something you might try and do, but a lot of companies* (that I have dealt with) *what they do is they'll have themselves as the person who can change everything at will, so if something goes wrong, someone comes to you you'll be like, "I can fix this thing."* (Interviewee 12, Solutions Architect)

5.1.2. Private blockchains

Described as being controlled by access permissions, blockchain experts clarified that within private blockchains, a central entity, usually within a specific organisation, governs over the activities of nodes and transactions across the network. Control is fundamentally centralised under a single entity, where participants are known to each other, and a centralised authority sets the rules and oversees operations, typically through a governing charter (document) or body. As explained by one of the interviewees:

> *it's a permissioned system … there's someone making a decision on who does or doesn't get to access the blockchain and what rules they have to abide by … the private network is known to each other. Then I would say it's like the governing body that the people that brought them together …, like you think hyperledger or you think of private blockchain such as on ripple it's just, you know, they all know each other. So, they would all be bounded by some sort of governance document.* (Interviewee 4, Blockchain Lawyer)

The central authority in private blockchains set rules, manages access permissions, conducts transactions, and decides how transactions are validated, often involving selected users from the network or an independent entity chosen by the authority.

5.1.3. Consortium blockchains

Like private blockchains, consortium blockchains are permissioned, but control is distributed among selected nodes with varying access and permission rights (Interviewee 7, Blockchain manager). A few can see all transactions, while the rest cannot. Decision rights within consortium blockchains are described by blockchain experts as being democratic, with a pre-selected group of participants – the consortium – collaboratively making decisions on the blockchain's development, operation, and governance. Consensus is required for decisions, including adding new members, which must be approved by a democratic vote of all consortium members (Interviewee 2, blockchain developer). Another interviewee also alluded to the fact that much governance and control relating to consortium blockchains are defined by the original consortium members:

> *… let's say you've got like a small technology house or a big technology house like an IBM who's building this thing and they've been kind of commissioned by two or three parties who say let's build a system … And then let's say they want to engage party number five or party number 20 to this thing. Like, if you're the 20th person, the 50th person that comes onto this, that governance that comes built, has already been predefined by those initial players … Is it defined by an original consortium? Is it defined by everyone who, who comes onto that? It's like the Libra model, right?.. It's a permissioned blockchain, like you can't just join it. You have to have permission from the Libra consortiums to join it. And so, you know, there's what, 33 participants or something in the first round, something like that. So, they define the governance model and then in two years' time someone else wants to join. Then that responsibility and that accountability model has already been defined by that original group.* (Interviewee 6, Blockchain Auditor and Product Manager)
>
> While decision rights are seemingly distributed in consortium blockchains in practice, many blockchain experts highlighted the fact that distributed decision rights can make decision making slow and hence very inefficient:
>
> *you could have a consortium model where, you know, you've got like a dozen banks coming together and then you are ruled by committee* (as opposed to a single authority). *The problem there is … 12 people, how do you get agreement and that things are just much slower.* (Interviewee 1, Blockchain Solutions Architect)

5.2. Accountability

5.2.1. Public blockchains

Public blockchain developers noted that blockchain systems do not take responsibility for the transactions or enforce users' adherence to legal requirements, as the technology is considered open source and experimental. Most interviewees who are developers put forth an argument that nobody would publish in a public blockchain, while assuming liability for it, and that most would interact with public blockchains and publish under no liability:

> *I think they* (initial developers) *were very careful to write it that way when they did the first launch, to say that we don't take any responsibility for this. It might work, it might not work, have a go … The big question would be even harder to answer because you don't know who the guy is who created it anyway, so how could you blame anyone exactly? It was like an open source project for them to make it, so if there was a problem there, then I don't think they'd be held accountable. (Interviewee 11, Blockchain Developer)*
>
> *… no, we are not responsible for it cause it's experimental software … it's all published under MIT license, so as an MIT license, it's experimental software and we're not liable for its use. Anyone …* (Interviewee 9, Blockchain developer)

Interviewee 9 specifically went on to explain that developers publish based on no liability. Also, as highlighted by Interviewee 11 above, the initial developers of the blockchain infrastructure are unknown and users can choose to use several public addresses or remain pseudonymous when transacting on the blockchain. As explained by Interviewee 16, a Blockchain Developer in a small blockchain company:

> People say that the blockchain is pseudonymous, meaning if you have an account address and you use it multiple times, no one will know it's necessarily you but they will see the history of that account if it's used again and again for different transactions. Some have the principle of using different accounts for each transaction such that it remains anonymous.

So, while blockchain technology provides a transparent, tamper-resistant ledger by linking transactions to their sources, blockchain experts noted that its focus on privacy and security prevents stakeholders from holding real identities accountable:

> *the thing that public blockchains give you is transparency, right? So, to the extent that you can link a blockchain identity to a real-world identity, then you can yeah, you have full transparency over their actions on chain … And then along with that, having a trail to verify off chain that, that identity is actually a real person and not some made up person. Then you get transparency over that set of actions. Um which means that you can be legally compliant and also comply with whatever regulations that relate to you. So, I think you know, the answer, the question of accountability is more in block chain, it's more question of transparency to the extent that things are transparent to a real-world identity that you can hold people with real world identities to account.* (Interviewee 4, Blockchain Solutions Architect)

> *And with a lot of the public blockchain systems out there, it's not like you can give someone a call and be like, hey, bitcoin foundation I lost my private keys, or you know, someone's taken money out of my wallet. There's no one that can do that. So that's kind of where the whole public private blockchain divide kind of comes. You know, where you could kind of an argument for, well, you know, public blockchains are great as a matter of principle and in theory, but maybe there aren't sufficient checks and balances to ensure their accountabilities.* (Interviewee 5, Blockchain Lawyer and Advisor)

As interviewee 4 and 5 highlighted, the question of accountability in public blockchains is more in the *on-chain* infrastructure given the lack of accountability *off-chain* with the anonymous or pseudo-anonymous identities granted to users in the blockchain network.

5.2.2. Private blockchains

In private blockchains, accountability is established and maintained through a combination of mechanisms that are typically defined by the central authority or the governing entity that controls the blockchain network, ensuring only authorised parties are involved in the network's activities. The use of a central authority by private blockchains to ensure accountability results in the absence of anonymity. This lack of anonymity contrasts with public blockchains, as the authority knows participants' identities, enabling quicker identification and resolution of issues, such as breaches, as noted by a Blockchain Auditor (Interviewee 6).

An important insight provided by one of the blockchain experts is that accountability in private blockchains is influenced, and can vary, by the blockchain's design, rules set by the central authority, and the legal/regulatory environment. Most private blockchains will provide common statements of responsibilities of its governing body to its users, where accountability is attributed to the centralised entity or provider, which is expected to address and remedy any issues that arise:

> *I think generally we tend to think of them the same way we think of a centralised bank or other* (centralised) *provider at this stage where we're like, it's your fault you fix it.* (Interviewee 7, Blockchain Product Manager)

Similar insights were provided in relation to private blockchain exchanges where the centralisation of control and trust afforded to a central authority such as a management team, along with the legal jurisdiction, made individuals like the Chief Executive Officer (CEO) of Mt Gox accountable when the cryptocurrency exchange collapsed in 2014 (Aubin, 2019; Pham, 2019):

> *It's an exchange, a centralised one. But if they lose your money, they are obligated to give it back, and they've been pretty good. Of course, some of them just go bust and disappear. But they're typically accountable. Even the Mt Gox, the big exchange that imploded in 2014, I think from memory, they went to court, they're still in court proceedings. It's taken ages. But they were liable at that point. They were holding users' money, and therefore they have to be a trusted custodian. Whereas the more decentralised* (a blockchain is)*, the less you can say that anyone is directly accountable.*

5.2.3. Consortium blockchains

As detailed above, in consortium blockchains, accountability is established through a combination of governance structures and predefined roles among vetted participants, typically organisations or institutions that have a vested interest in the network. These participants collaborate to develop rules, protocols, and decision-making mechanisms that ensure transactions and actions are traceable to specific individuals or entities, enhancing accountability. For example, as narrated by Interviewee 7, a Blockchain Product Manager, when a blockchain product in their organisation caused users to be locked out of their wallets, accountability rested with those overseeing the blockchain, who quickly disclosed the issue to the relevant community.

Experts noted that in consortium blockchains, accountability is established and allocated prior by primary stakeholders before system development, with individuals bearing responsibility to each other or those they transact with. As a result, every consortium participant holds a certain degree of accountability:

> *So, I know in the one* (consortium) *where there's like, you know, a company set it up like they're there, they're going to be the ones accountable. So, if something goes wrong, the members are going to come to them and say, well, I'm paying a fee for you to run this thing.*

> *It's busted, you know, fix it … which is why we think that one's* (consortium blockchains) *probably the best model because there is accountability …* (Interviewee 1, Blockchain Solutions Architect)

Given that consortium blockchains have a defined governance framework that outlines the roles, responsibilities, and decision-making processes of participating entities, it ensures that all participants adhere to agreed-upon rules and regulations that govern the network. This structure allows for identifying responsible actors when issues arise. However, whether that actor can provide an account – in other words provide an accurate record – of what or how something went wrong in the blockchain is still uncertain as highlighted by one of the blockchain experts:

> *I think it probably depends on how the governance is defined … who's responsible for that? Is it the software provider or is it the original consortium members? Does it go through reviews every six months where the current members go through a voting process on any changes?..Whether they're accountable, I think is a slightly different question. But you can sort of tell if they're responsible.* (Interviewee 6, Blockchain Auditor and Product Manager)

5.3. Incentives

5.3.1. Public blockchains

One of the novel ways in which public blockchain has ensured the increasing dissemination and use of its technology is through control mechanisms such as consensus alignment and incentives which are pre-programmed into the technology using computational logic. Public blockchain purports to cut out the need for centralised intermediaries, or middlemen, and reallocate the value currently held by established societal actors, such as banks, back to users (Pflueger et al., 2022). Users are able to place less reliance and trust on central entities because blockchains elicit trust in users via the consensus mechanism, and the algorithm, as opposed to individuals:

> *… trusting the protocol, not trusting in the accountability of any authority who's signing off on something or who is or has a reputation that is being relied on …* (Interviewee 2, Blockchain Developer)

The engagement with the consensus mechanism of a blockchain involves a node (also referred to as a user or participant) committing/investing a valuable asset, such as electricity or a specific cryptocurrency (depending on the consensus mechanism used by the blockchain). This commitment ensures the network's operation and qualifies the node for potential rewards. Failure to meet the consensus outcome results in the participant losing their stake and not being rewarded. Consensus mechanisms efficiently synchronise the motivations of blockchain participants to hold them accountable within the blockchain system, but in a manner that calls on them to be good actors, as opposed to directly identifying them as perpetrators of unsanctioned behaviours:

> *… I've put up all this work because I use my electricity and all that to do the mining, and if I'm not honest then my block is not going to be accepted and I'm not going to get the end reward … your stake is monetary so you don't want to lose that and that's part of what keeps you accountable but if … you didn't care about the incentive and you didn't care about losing that stake, then you can really do whatever you want because you're free of the bounds of the stake, you're willing to lose it and you can do* (act or behave in) *whatever you want.* (Interviewee 12, Blockchain Solutions Architect)

> *At the base protocol layer, which is Ethereum blockchain, they call it reaching consensus, the protocol mechanism, that's what it does. That is the key thing the blockchain does, it reaches consensus with certain data such as account balances. That is as far as that goes … When I talk about reaching consensus, it's not only on balances but also data inside smart contracts. Smart contract meaning executing code that stores variables as well, small amounts of data. You can extend trust from that smart contract out by allowing the smart contract to share extra data and to say, if the smart contract author has written something that says this is what this does in plain English to say here is a function, by calling this function it will take this and transfer the asset to this. The trust is coming from there* [consensus mechanism]. (Interviewee 16, Blockchain Developer)

As illustrated above, in public blockchains, incentives are crucial for motivating desirable behaviours and ensuring the blockchain functions optimally(such as Ethereum which is the infrastructure used by most public blockchains). Participants invest resources, such as cryptocurrency, and are driven by the desire to protect their investment. The fear and cost of losing this resource contribution serves as key motivator for responsible behaviour.

5.3.2. Private blockchains

In private blockchains, incentives differ from public ones due to the network's-controlled nature. Participants, typically within organisations, have a vested interest in the blockchain's success and influence governance and decision-making to align with their needs. This level of control can serve as an incentive in itself:

> *… the beauty with a private blockchain is that with a public one, I guess as well is that, you know, the creators get to choose, you know, either people that fall off a different blockchain or that start an entirely new blockchain system that is private. And its only permission is that you get to choose the rules of that network and how the participants operate. So again, it goes back to really good governance … a private blockchain, you've just got a little bit more control theoretically over what your participants can and can't do.* (Interviewee 5, Blockchain Lawyer and Advisor)

In addition to control and governance, incentives of cost reduction and efficiency of enhanced collaboration, data sharing, and improved decision-making ensures that the limited number of known participants in a private blockchain acts in alignment with the blockchain system's goals:

> *I think there is a mix of things there that, for some things it may be cheaper, for other things it may seem more expensive … The benefits that an industry like the supply chain can get from using blockchain technology, isn't necessarily the transaction costs, although that may be part of it, but I would say it's around sharing data with people that they may not trust and may not have a trusted third party … It's some way of reaching consensus on facts or on transaction data or other things in a way that's shared amongst them and no one can corrupt it. Whereas, currently, you might have silos of information between suppliers, transport and the recipients in the end and everywhere in between has their own data, their own transactions …* (Interviewee 16, Blockchain Developer)

Blockchain experts also pointed out that incentives in private blockchains are often aligned with specific objectives and goals of the participants, including non-monetary incentives such as building reputation. Consistently adhering to the rules, protocols, and agreements, fulfilling commitments, and actively participating in activities like voting can enhance one's reputation and demonstrate compliance and responsible behaviour:

> *… Going further with* (incentive) *mechanisms of accountability or, I'll say, reputation of individual addresses … You want to grow your reputation so you will reuse an account. Even if it's anonymous, you want that account to be doing good things …, or if that address is voting on certain issues and happens to, I'm not going to say vote correctly, but if they are often right with what they're predicting, then that's a good reputation for that address … There's other reputation systems out there … voting is the main one that will build reputation …* (Interviewee 16, Blockchain Developer)

5.3.3. Consortium blockchains

Like private blockchains, incentives play a crucial role in motivating participants to contribute positively to the consortium's network operation and success. Many of these incentives emerge from the emerging benefits of participating in a consortium blockchain as detailed by one blockchain expert:

> *… commercially popular use cases will emerge that allows entities that exist on the same level of a value chain in an industry, or which are very close to each other in the value chain, allow them to use* (permissioned consortium) *blockchain to interact with each other in a way that they are cooperating with each other that don't need to trust each other and derive further efficiencies in the commercial development of services and products. But then remain total bare-knuckle fierce competitors with each other at various stages … There are still data silos, there are economies of scale in which companies aren't forced to compete and offer or sell what they provide, they're able to put excessive mark-up margin on and they are in a position where they can extract more value at their position in the value chain than they are contributing to the development of the product service and value chain …* (consortium) *blockchain has the potential to allow … the second and third order competitors to the incumbent to cooperate with each other and to be sharing some aspects of the service in which they are providing in order to be more competitive, combining their market shares in order to reduce the discrepancy between the market share of the incumbent, which is often around 85% market penetration. And there might be two or three other competitors at something like 15%. And if the two or three other competitors were to cooperate, at some level in the value chain, they would reduce that discrepancy, which would place them in a far more competitive position against the incumbent.* (Interviewee 2, Blockchain Developer)

In a consortium blockchain, shared goals such as efficiency, access to services, and competitive advantage motivate participants to align their behaviours with the goals of the consortium.

The following section delves into a discussion of the above results, demonstrating how the insights garnered from blockchain experts advances our understanding of blockchain governance and control through the interplay of decision rights, accountability, and incentives.

6. Discussion

The findings above highlight how blockchain systems transcend public blockchains to include consortium and private blockchains in practice, and must do so owing to the natural shortcomings that arise from a control perspective when consensus-based control is created in a pure form, as is observed in a public blockchain (Ali et al., 2022). Analysing all three blockchain systems through the three dimensions of IT governance and control identified by Beck et al. (2018) - decision rights, accountability and incentives, our empirical data encompassing 18 interviews with blockchain experts, offer a broader encapsulation of this framework. Beck et al. (2018) had originally focused on a private blockchain alone. We offer the following table summarising the nature of relationships across the three blockchain systems:

We find that public blockchains offer access to all transactions and the ability to easily establish an identity and engage as a stakeholder with blockchain systems, but this identity is often anonymous and not easily traceable to an actual individual or entity (Tyma et al., 2022). Private and consortium blockchains, on the other hand, offer a more hierarchical governance and control structure, enabling an individual central entity (private blockchain) or collection of central entities (consortium blockchain) to drive the behavioural rules and norms within a blockchain system, verify the real identities of all stakeholders involved in the system, and facilitate a more coordinated and centralised transfer of information across nodes. They appear to be a rapidly growing and increasingly used blockchain form in business (Iredale, 2021).

The decision rights of participating stakeholders are greater in public blockchains than in private/consortium blockchains. In the latter, participation is regulated and driven by a central authority(ies). The distributed ledger technology still allows for all nodes to contain information, but centrally determined algorithms allow for information within nodes to be accessed and manipulated to different degrees, albeit with some element of traceability (Thylstrup et al., 2022), not unlike that observed in traditional hierarchical organisations. Thus, the governance of blockchains in practice does not differ drastically from pre-blockchain systems, but the use of DLT offers the advantage of more open information access, especially given the ability to execute smart contracts (De Filippi et al., 2021).

We also find that decision rights in private and consortium blockchains differ in terms of the control of, and access to the network. A private blockchain is governed by a single organisation or entity, which maintains complete control over the network's operations and governance. This centralised authority determines who can participate in the network, validate transactions, and maintain the ledger. In consortium blockchains, on the other hand, control is distributed among a group of pre-selected, trusted organisations, sharing decision making power and governance responsibilities. Like private blockchains, consortium blockchains are permissioned, but the difference is access is granted to a consortium of entities and thus control is more decentralised than a fully private blockchain. To operationalise this more decentralised form of centralised control in consortium blockchains, trust among participants is paramount, established through collaboration and mutual agreements between participants rather than controlled by one entity in the case of private blockchains.

Accountability reveals an inverse relationship to decision rights. Public blockchain participants tend to have lower accountability, relying on two assumptions: stakeholders' willingness to reveal their identity and their aversion to losing resources invested in a public blockchain. If either condition is unmet, little accountability remains. Many public blockchain developers assume that internal consensus governance is sufficient, ignoring the need for external accountability. Yet repeated examples of public blockchain breaches are observed, subsequently requiring intervention to remedy. In contrast, private and consortium blockchains demand higher levels of accountability from stakeholders through the direct identification of key stakeholders as a key control and governance process, immediately holding these individuals accountable notwithstanding their resources invested or individual attitudes to their accountability in a blockchain system. Accountability is also more collective in a consortium blockchain than a private blockchain given that decisions are often made collaboratively and thus consortium members may also be accountable to each other directly, in addition to the consortium governing body.

Finally, we find that the incentives for participating in a public blockchain system lie in the preservation of resources and the want to remain a part of a community (consensus). In private and consortium systems, these motivations are supplemented by the added incentive of legal and regulatory compliance, tied to the knowledge of participants' true identities. While these incentives are more extrinsic and easier to manage by central node founders or governing entities of private/consortium blockchains, they lack the purer intrinsic motivation found in pure public blockchain, where participants are often driven by a desire to self-regulate and resist traditional external regulatory governance and control norms observed in traditional commercial environments (Hytha et al., 2019; Manski & Manski, 2018). In private blockchains, incentives align with the goals of the central authority or organisation overseeing the network, whilst in consortium blockchains, incentives balance the interests of all members, addressing both collective success and individual organisational goals.

Overall, our empirics are organised using an expanded application of Beck et al. (2018) to offer a more nuanced encapsulation of how governance and control come to be enacted within alternative blockchain systems, highlighting the necessary trade-offs made between the pure application of a blockchain system, against the corporate realities relating to governing and controlling a commercial marketplace. While Beck et al. (2018) considered the operation of a single private blockchain system, we offer an expanded characterisation of how public, private and consortium blockchains achieve the same next to one another.

While other accounting studies have emphasised the importance of trust between actors to enable the working of a blockchain (Pflueger et al., 2022), and the role of transparency and accountability in driving different blockchain system activity (Tyma et al., 2022, Spanò et al., 2022), we find that decision rights and incentives alongside accountability assist in the explanation for alternative blockchain systems from a governance and control perspective. Public blockchains offer relatively more decision rights, lower accountability and demand relatively higher intrinsic incentives for governance and control. Private/consortium blockchain systems offer fewer decision rights, greater accountability and more extrinsically incentivise desirable behaviours from participants.

The demarcation of identity in public blockchains give rise to the possibility of a weakened relationship between *responsibility* and *accountability*. The absence of identification in public blockchains allows individuals or entities to be responsible for actions without being held accountable, which is often seen as a strength of the system. In traditional accounting studies, within more traditional organisational settings, responsibility is couched in notions of controllability, with studies investigating the strengths and weaknesses of individual controllability for actions rightly (or otherwise) affecting their accountability and reward for the same (Giraud et al., 2008). Notions of fairness are implicated in these debates, as well as the role of individual manager perception of their role (Burkert et al., 2011). We offer a very different rationale for this disconnect between responsibility and accountability, and present it as a key rationale for the development of alternative forms of blockchain that align responsibility with accountability, making commercial arrangements more workable in practice. This manner of capturing the occurrence and consequences of the disconnect between responsibility and accountability has not been previously offered in the literature.

7. Conclusions, limitations and suggestions for future research

We sought to understand how blockchain systems enact governance and control in practice, by offering empirical evidence from blockchain experts concerning the same. The expanded Beck et al. (2018) framework offered in Table 1 is a step forward in our understanding of these relationships, and our empirics offer an alternative hierarchy driven governance structural solution to the relationship and trust-based elements defining control in blockchains previously put forward in the literature (Pflueger et al., 2022). We also clarify how blockchains reveal different system level responses to address the disconnect between responsibility and accountability than that offered in the accounting literature in traditional organisational settings.

Essentially, this research demonstrates that public blockchains function under the governance of all participants having access to unalterable transaction records. These records are inherently resilient due to their presence on each node across the public blockchain. This decentralised ledger technology reaches its pinnacle in public blockchains, where users are motivated to act in the right manner through transparency facilitated by such access (Tyma et al., 2022). Additionally, the risk of losing investments due to violating consensus conditions within the blockchain further encourages compliant behaviour. This advantageous aspect of public blockchains has been acknowledged in previous research (Spanò et al., 2022; Yermack, 2017).

Nevertheless, our findings uncover a significant concern related to the accountability of stakeholders in public blockchains. This concern arises from the challenges of pinpointing the true identities of responsible parties (Ali et al., 2022). Moreover, responsibility tends to be attributed more to the blockchain system itself than to individual actors within the blockchain. Individuals responsible for developing, mining, or engaging in other blockchain processes in public blockchains often operate under aliases or anonymous identities that are exceedingly hard to trace. Even when they operate openly, these developers struggle to grasp the rationale behind their personal accountability. Consequently, although a node's responsibility for a task can be determined, practically enforcing and assigning accountability to the individuals or entities performing the task within public blockchains remains deficient.

Furthermore, this study reveals that the majority of operational commercial blockchains have more hierarchical structures, with a central authority – either a single node in private blockchains or a consortium of identities in consortium blockchains – overseeing and regulating the system. These central entities verify identities, enforce controls, and manage participant access, while information remains distributed across all nodes., This centralised oversight aligns tasks and accountability more clearly in private and consortium blockchain systems. While these systems deviate from the complete openness and transparency of public blockchains, they form a hybridised blockchain model that proves functional and essential for modern organisational governance and control.

This research makes three key contributions to the existing literature. Firstly, this study sheds light on a more hybrid form of blockchain governance, which contrasts with the widely discussed public blockchain system. We attribute a more traditional hierarchical and structural control framework to the practical evolution of blockchain, diverging from the "back-stage construction of communities relying on trust in individuals" as elucidated by Pflueger et al. (2022, p. 2).

Secondly, we expand upon Beck et al. (2018)'s work by systematically delineating how decision rights, accountability, and incentives manifest within the contexts of public, private, and consortium blockchains. Our approach involves interviewing a diverse set of experts with exposure to all three blockchain variants, in contrast to Beck et al. (2018)'s focus on a singular type of blockchain. We find that public blockchains provide a higher degree of decision rights, accompanied by reduced accountability, and require a greater emphasis on inherent incentives for effective governance and control. On the other hand, private and consortium blockchain systems allocate fewer decision rights, increases accountability, and rely more on external incentives to encourage users to behave in alignment to the goals of the blockchain system.

Thirdly, we underscore the disparity between responsibility and accountability that can arise in public blockchains, where participants may be identified as responsible but remain accountable due to the inherent weakness of identity validation processes in public blockchains, where anonymity is often encouraged (Ali et al., 2022). In contrast, private and consortium blockchains rely on identity verification (Ziolkowski et al., 2020). This specific disjunction between responsibility and accountability, largely overlooked in existing research (Spanò et al., 2022; Tyma et al., 2022), has significant implications for our comprehension of practical blockchain governance and control. It further elucidates the shift from public to private and consortium blockchains across various industries. In the realm of management accounting research, the examination of the disconnect between responsibility and accountability has primarily revolved around controllability and its associations with performance and rewards in traditional organisational settings (Burkert et al., 2011; Giraud et al., 2008). In our study, we present a more system-oriented rationale for addressing this issue, aimed at preserving transaction integrity within a digitised system.

This study has several practical and policy implications. Firstly, our findings show that responsibility is often attributed to the blockchain system itself, rather than individual actors, making governance and operational issues critical during the blockchain planning and design phases. Governance models for public blockchains are not easily transferable, and governance challenges vary across different types of blockchain systems observed in practice. There are important governance policy implications for organisations to decide which blockchain system to choose when implementing the technology, keeping in mind how the interplay of decision rights, accountability and incentives may influence the adaptability, resilience and scalability of governance models. For example, in private and consortium blockchains, there are challenges related to what entity or entities will govern and operate the blockchain network and its intended users, with impact of this decision rights allocation on the efficiency, security and decentralisation of the blockchain system.

Secondly, blockchain governance involves the processes, practices and rules that control and direct the network, with developers, nodes and network users all playing a role. It is essential to analyse the control mechanisms in place to ensure accountability of actors within blockchain systems. However, power and control vary by blockchain type; for example, developers typically have more control in public blockchains like Ethereum, while in whereas in permissioned systems (private and consortium blockchains), accountability and control mechanisms are determined by members who govern access and consensus conditions for smart contracts. Policymakers and system developers need to reflect on the interlinkages between the level of control and assess the implications of the level of governance afforded by different blockchain types to prevent fraud, collusion and other malicious activities. Here it is also essential for practitioners and researchers to evaluate the impact of various incentive models, for example rewards, penalties, staking, on actor behaviour and system stability.

Lastly, the conceptualisation of blockchain governance in the extant literature is fragmented, highlighting the need for a more cohesive framework to analyse governance implications in blockchain design. By expanding Beck's governance dimensions, decision rights (decision management and control), accountability (identity, resources invested and regulatory) and incentives (intrinsic and extrinsic) across different blockchain types, we offer a primer for policymakers, developers, stakeholders and researchers to create a more robust and effective governance model for blockchain systems. This paper applies these governance dimensions to public, private and consortium blockchains, but suggest they can also inform governance frameworks in other sectors, such as the public sector, by examining decision rights allocation, evaluating accountability mechanisms and incentive structures to identify best practices and potential pitfalls in designing governance frameworks for public sector blockchain networks.

There are several limitations to this study that present opportunities for further research exploration. This study comprised the analysis of a range of qualitative interviews with blockchain experts. While difficult to obtain sample sizes, future studies might apply a survey methodology to offer more aggregate statistical testing and validation of our qualitative findings.

In addition, our empirical setting was the Australian corporate setting, which broadly mirrors modern economic environments. Yet we know that blockchain has grown enormously in developing markets such as Asia. Studies that explore the impact of cultural differences on the operationalisation of many of the decision rights, accountability and incentives findings in this study will strengthen or shed light on alternative governance and control responses to different blockchain systems. Furthermore, and while we received no such feedback from our respondents, it is possible that cryptocurrency blockchains might systematically vary in their responses to non-crypto blockchains, as the industry matures and higher volumes of different blockchain types proliferate.

Finally, our findings reflect a broad range of perspectives from various blockchain stakeholders, rather than an in-depth examination of a single case. Future studies focusing on in-depth case studies of individual blockchain systems could provide richer insights, revealing deviations in practice that might be observed from those theoretically espoused in popular media and opinion pieces. For example, research may uncover that consortium blockchains are dominated by a single entity, making them resemble private blockchains. These subtleties require deeper exploration in future research.

Accounting will be inexorably altered by the conduct of transactions in digital marketplaces, and blockchains systems appear to be a structure that has become a dominant vehicle through which this digitisation is being enacted. The future study of the antecedent organisational and individual variables driving variation in its practice, and the consequences of doing so, are imperative to ensure these new forms of digitised coordination mechanism are enacted in a manner that protects the decision rights, justifiably accounts for and incentivises all relevant stakeholders effectively.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.bar.2025.101588.

Data availability

The authors do not have permission to share data.

References

Ali, S., Shin, W. S., & Song, H. (2022). Blockchain-enabled open quality system for smart manufacturing: Applications and challenges. *Sustainability, 14*(18), Article 11677.

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable & Sustainable Energy Reviews, 100*, 143–174.

Angus, C. (2018). *Blockchain technology, parliament of NSW, NSW*.

Aramonte, S., Huang, W., & Schrimpf, A. (2021). DeFi risks and the decentralisation illusion. *Last accessed 1st august 2023*. https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf.

Arrunada, B., & Garicano, L. (2018). Blockchain: The birth of decentralized governance. *Pompeu Fabra University, Economics and business working paper series,*, Article 1608.

ASX. (2023). Chess replacement, last viewed 1st august 2023. https://www.asx.com.au/services/chess-replacement.htm.

Atzori, M. (2015). *Blockchain technology and decentralized governance: Is the state still necessary?*. Available at SSRN 2709713.

Aubin, D. (2019). Former Mt Gox CEO must face lawsuit over bitcoin exchange collapse – ruling. *Last accessed 3rd august 2023*. https://www.reuters.com/article/idUSL2N24U1EB/.

Azzi, R., Chamoun, R. K., & Sokhn, M. (2019). The power of a blockchain-based supply chain. *Computers & Industrial Engineering, 135*, 582–592.

Balcerzak, A. P., Nica, E., Rogalska, E., Poliak, M., Klieštik, T., & Sabie, O.-M. (2022). Blockchain technology and smart contracts in decentralized governance systems. *Administrative Sciences, 12*(3), 96.

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the Association for Information Systems, 19*(10), 1.

Bellucci, M., Cesa Bianchi, D., & Manetti, G. (2022). Blockchain in accounting practice and research: Systematic literature review. *Meditari Accountancy Research, 30*(7), 121–146.

Bhimani, A., & Willcocks, L. (2014). Digitisation, 'Big Data'and the transformation of accounting information. *Accounting and Business Research, 44*(4), 469–490.

Bonsón, E., & Bednárová, M. (2019). Blockchain and its implications for accounting and auditing. *Meditari Accountancy Research, 27*(5), 725–740.

Boukis, A. (2019). *Exploring the implications of blockchain technology for brand-consumer relationships: A future research agenda*. University of Sussex. Journal contribution. https://hdl.handle.net/10779/uos.23470295.v1.

Brennan, N. M., Subramaniam, N., & Van Staden, C. J. (2019). Corporate governance implications of disruptive technology: An overview. *The British Accounting Review, 51*(6), Article 100860.

Bryman, A. (2019). *Social research methods* (5th ed.). Oxford University Press Canada.

Burkert, M., Fischer, F. M., & Schäffer, U. (2011). Application of the controllability principle and managerial performance: The role of role perceptions. *Management Accounting Research, 22*(3), 143–159.

Cai, C. W. (2018). Disruption of financial intermediation by FinTech: A review on crowdfunding and blockchain. *Accounting and Finance, 58*(4), 965–992.
Cai, C., Xu, L., Zhou, A., & Wang, C. (2021). Toward a secure, rich, and fair query service for light clients on public blockchains. *IEEE Transactions on Dependable and Secure Computing, 19*(6), 3640–3655.
Centobelli, P., Cerchione, R., Del Vecchio, P., Oropallo, E., & Secundo, G. (2022). Blockchain technology design in accounting: Game changer to tackle fraud or technological fairy tale? *Accounting, Auditing & Accountability Journal, 35*(7), 1566–1597.
Chang, S. E., & Chen, Y. (2020). When blockchain meets supply chain: A systematic literature review on current development and potential applications. *IEEE Access, 8*, 62478–62494.
Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights, 13*, Article e00151.
Clarke, V., & Braun, V. (2017). Thematic analysis. *The Journal of Positive Psychology, 12*(3), 297–298.
Commonwealth of Australia. (2020). The national blockchain Roadmap: Progressing towards a blockchain-empowered future. https://apo.org.au/sites/default/files/resource-files/2020-02/apo-nid276541.pdf.
Coyne, J. G., & McMickle, P. L. (2017). Can blockchains serve an accounting purpose? *Journal of Emerging Technologies in Accounting, 14*(2), 101–111.
Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems, 31*(3), 5–21.
De Filippi, P. (2019). Blockchain technology and decentralized governance: The pitfalls of a trustless dream. In *Decentralized thriving: Governance and community on the web* (Vol. 3).
De Filippi, P., & Loveluck, B. (2016). The invisible politics of bitcoin: Governance crisis of a decentralized infrastructure. *Internet policy review, 5*(4).
De Filippi, P., Wray, C., & Sileno, G. (2021). Smart contracts. *Internet Policy Review, 10*(2).
Dursun, T., & Üstündağ, B. B. (2021). A novel framework for policy based on-chain governance of blockchain networks. *Information Processing & Management, 58*(4), Article 102556.
Ekal, H. H., & Abdul-wahab, S. N. (2022). DeFi governance and decision-making on blockchain. *Mesopotamian Journal of Computer Science, 2022*, 10–17.
Eyers. (2018). Australia in driving seat as global blockchain standards take shape. *The Australian Financial Review, 9*. https://www.afr.com/technology/australia-in-driving-seat-as-global-blockchain-standards-take-shape-20180907-h151w7.
Fanning, K., & Centers, D. P. (2016). Blockchain and its coming impact on financial services. *Journal of Corporate Accounting & Finance, 27*(5), 53–57.
Faqir-Rhazoui, Y., Arroyo, J., & Hassan, S. (2021). A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain. *Journal of Internet Services and Applications, 12*(1), 1–20.
Flick, U. (2018). Triangulation in data collection. *The SAGE handbook of qualitative data collection*.
Flyverbom, M., Deibert, R., & Matten, D. (2019). The governance of digital technology, big data, and the internet: New roles and responsibilities for business. *Business & Society, 58*(1), 3–19.
Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics, 2*(1), 2.
Garanina, T., Ranta, M., & Dumay, J. (2022). Blockchain in accounting research: Current trends and emerging topics. *Accounting, Auditing & Accountability Journal, 35*(7), 1507–1533.
Giraud, F., Langevin, P., & Mendoza, C. (2008). Justice as a rationale for the controllability principle: A study of managers' opinions. *Management Accounting Research, 19*(1), 32–44.
Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PLoS One, 15*(5), Article e0232076.
Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial intelligence: A literature review. *International Journal of Accounting Information Systems, 48*, Article 100598.
Hsieh, Y. Y., Vergne, J. P. J., & Wang, S. (2017). The internal and external governance of blockchain-based organizations: Evidence from cryptocurrencies. In *In bitcoin and beyond* (pp. 48–68). Routledge.
Hughes, A., Park, A., Kietzmann, J., & Archer-Brown, C. (2019). Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms. *Business Horizons, 62*(3), 273–281.
Hytha, D. A., Aronson, J. D., & Eng, A. (2019). Technology innovation and the rebirth of self-regulation: How the internet of things, cloud computing, blockchain, and artificial intelligence solve big problems managing environmental regulation and resources. *International Journal of Communication, 13*, 5.
ICOinRating.com. (2018). Ozex. https://icoinrating.com/ozex/.
Institute of Management Accountants. (2021). *Governance*. https://asiapac.imanet.org/.
Institute on Governance. (2023). What is Governance. https://iog.ca/what-is-governance/.
Iredale, G. (2021). The rise of private blockchain technologies. https://101blockchains.com/private-blockchain/.
Khatwani, S. (2018). Different types of blockchains in the market and why we need them. https://coinsutra.com/different-types-blockchains/.
Kokina, J., Mancha, R., & Pachamanova, D. (2017). Blockchain: Emergent industry adoption and implications for accounting. *Journal of Emerging Technologies in Accounting, 14*(2), 91–100.
Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80–89.
Kvale, S. (2007). *Doing interviews*. London: SAGE.
Laatikainen, G., Li, M., & Abrahamsson, P. (2023). A system-based view of blockchain governance. *Information and Software Technology, 157*, Article 107149.
Lardo, A., Corsi, K., Varma, A., & Mancini, D. (2022). Exploring blockchain in the accounting domain: A bibliometric analysis. *Accounting, Auditing & Accountability Journal, 35*(9), 204–233.
Liu, Y., Lu, Q., Zhu, L., Paik, H. Y., & Staples, M. (2023). A systematic literature review on blockchain governance. *Journal of Systems and Software, 197*, Article 111576.
Liu, M., Wu, K., & Xu, J. J. (2019). How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. *Current Issues in Auditing, 13*(2), 19–29.
Lugano, F. (2018). Zencash: "We want to make 51% attack impossible". https://en.cryptonomist.ch/2018/06/11/51-attack/.
Ma, W., Zhu, C., Liu, Y., Xie, X., & Li, Y. (2023). A comprehensive study of governance issues in decentralized finance applications. *arXiv preprint arXiv:2311.01433*.
Mahanti, R. (2021). *Data governance and compliance*. Singapore: Springer.
Manski, S., & Manski, B. (2018). No gods, no masters, no coders? The future of sovereignty in a blockchain world. *Law and Critique, 29*, 151–162.
Mendez, J. (2018). Current state of blockchain technology A literature review, research gate. https://www.researchgate.net/publication/329622321_Current_State_of_Blockchain_Technology_A_Literature_Review. last accessed on 1st August 2023.
Mika, B., & Goudz, A. (2021). Blockchain-technology in the energy industry: Blockchain as a driver of the energy revolution? With focus on the situation in Germany. *Energy Systems, 12*, 285–355.
Möller, K., Schäffer, U., & Verbeeten, F. (2020). Digitalization in management accounting and control: An editorial. *Journal of Management Control, 31*, 1–8.
Mondoh, B. S., Johnson, S. M., Green, M., & Georgopoulos, A. (2022). Decentralised autonomous organisations: The future of corporate governance or an illusion? *Aris (Aristeidis), Decentralised Autonomous Organisations: The Future of Corporate Governance or an Illusion*.
Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic Cash system*.
Ølnes, S. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly, 34*(3), 355–364.
Pelt, R. V., Jansen, S., Baars, D., & Overbeek, S. (2021). Defining blockchain governance: A framework for analysis and comparison. *Information Systems Management, 38*(1), 21–41.
Pereira, J., Tavalaei, M. M., & Ozalp, H. (2019). Blockchain-based platforms: Decentralized infrastructures and its boundary conditions. *Technological Forecasting and Social Change, 146*, 94–102.
Pflueger, D., Kornberger, M., & Mouritsen, J. (2022). What is blockchain accounting? A critical examination in relation to organizing, governance, and trust. *European Accounting Review*, 1–26.

Pham, S. (2019). Former Mt. Gox chief Mark Karpeles acquitted of most charges in major bitcoin case. https://edition.cnn.com/2019/03/14/tech/mark-karpeles-mt-gox/index.html.

Reijers, W., Wuisman, I., Mannan, M., De Filippi, P., Wray, C., Rae-Looi, V., & Orgad, L. (2021). Now the code runs itself: On-chain and off-chain governance of blockchain technologies. *Topoi, 40*, 821–831.

Schmeiss, J., Hoelzle, K., & Tech, R. P. (2019). Designing governance mechanisms in platform ecosystems: Addressing the paradox of openness through blockchain technology. *California Management Review, 62*(1), 121–143.

Schmitz, J., & Leoni, G. (2019). Accounting and auditing at the time of blockchain technology: A research agenda. *Australian Accounting Review, 29*(2), 331–342.

Sedgwick, K. (2018). Why governance is the greatest problem for blockchains to solve. *Bitcoin.com*. July 15 https://news.bitcoin.com/why-governance-is-the-greatest-problem-that-blockchains-must-solve/.

Siba, T. K., & Prakash, A. (2016). Block-Chain: An evolving technology. *Global Journal of Enterprise Information System, 8*(4), 29–35.

Spanò, R., Massaro, M., Ferri, L., Dumay, J., & Schmitz, J. (2022). Blockchain in accounting, accountability and assurance: An overview. *Accounting, Auditing & Accountability Journal, 35*(7), 1493–1506.

Tapscott, D., & Tapscott, A. (2016). The impact of the blockchain goes beyond financial services. *Harvard Business Review, 10*, 2–5.

Thylstrup, N. B., Archer, M., & Ravn, L. (2022). Traceability. *Internet Policy Review, 11*(1), 1–12.

Treleaven, P., Brown, R. G., & Yang, D. (2017). Blockchain technology in finance. *Computer, 50*(9), 14–17.

Tyma, B., Dhillon, R., Sivabalan, P., & Wieder, B. (2022). Understanding accountability in blockchain systems. *Accounting, Auditing & Accountability Journal, 35*(7), 1625–1655.

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing and Health Sciences, 15*(3), 398–405.

Valdivia, A. D., & Balcell, M. P. (2022). Connecting the grids: A review of blockchain governance in distributed energy transitions. *Energy Research & Social Science, 84*, Article 102383.

Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for internet of things. *Computer Communications, 136*, 10–29.

Yafimava, D. (2019). What are consortium blockchains, and what purpose do they serve?. https://openledger.info/insights/consortium-blockchains/#Shared_Platforms.

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance, 21*(1), 7–31.

Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and Organization, 29*(2), 105–117.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557–564).

Ziolkowski, R., Miscione, G., & Schwabe, G. (2020). Decision problems in blockchain governance: Old wine in new bottles or walking in someone else's shoes? *Journal of Management Information Systems, 37*(2), 316–348.