# Understanding Accountability In Blockchain Systems

BRIDGET TYMA*

RINA DHILLON**

PRABHU SIVABALAN

BERNHARD WIEDER

ACCOUNTING DISCIPLINE GROUP

UTS BUSINESS SCHOOL

UNIVERSITY OF TECHNOLOGY SYDNEY

**September 2020**

Monforma 2020 submission

* Author currently holds a position as a Blockchain Assurance Specialist at Ernst and Young (EY). The views expressed in this paper are those of the authors and do not reflect the views of EY.

** Corresponding author: Email: rina.dhillon@uts.edu.au UTS Business School, Building 8, 14-28 Ultimo Road, Ultimo, NSW 2007, Sydney, Australia.

## ABSTRACT

**Purpose:** We examine how accountability is constructed in the context of different types of blockchain systems. With the aim of increasing knowledge on accountability across three different types of blockchains (public, private and consortium), we ask: how do blockchain systems construct accountability?

**Design/methodology/approach**: We draw on theorising in the accountability literature to study how blockchains relate to our construction and understanding of accountability. A qualitative field study of the Australian blockchain technology landscape is conducted, with insights garnered from eighteen blockchain experts across three types of blockchains.

**Findings**: Findings reveal that different types of blockchains employ different forms and mechanisms of accountability, and in novel ways previously less acknowledged in the literature. Importantly, we find that accountability increases with *less* pure applications of blockchain technology, contrary to that espoused in earlier exhortations of blockchain use in interdisciplinary literatures. We also find that similar subtypes of accountability operate very differently across public, private and consortium blockchains. We therefore offer novel explanations for the relevance of greater accountability in blockchains, especially when the assumptions of public blockchains are softened and applied as private and consortium blockchains.

**Originality/value**: We contribute to the accountability literature by addressing how blockchains reshape our understanding of traditional accounting and accountability practices. This speaks to the broader role and influence of accountability when systems are more closed and located, offering a counterpoint to the relevance and importance of trust and transparency as a key mechanisms of accountability.



**Keywords**: Accountability; Blockchain; Transparency; Trust

**Paper type**: Research paper

## Introduction

Over the last fifty years, methods of accountability have undergone extensive technological disruption (Ryan 2012; Schmitz & Leoni 2019; Scott & Orlikowski 2012). From the addition of computers into workplaces, to the development of accounting software packages, and acceptance of cloud computing (Dai et al. 2017; Kokina et al. 2017; Ryan 2012), the way people hold others accountable has changed with the advent of technology (Scott & Orlikowski 2012; Aste et al 2017). Whilst these technological advancements have contributed to significant changes in the business landscape in the last century (Aste et al 2017; Ryan 2012; Westerman et al. 2014), a new technology has emerged with the potential to not only induce change, but to revolutionise the way transactions are conducted (Huh et al. 2017; O'Dair 2016; Pilkington 2016).

Blockchain is a disruptive technology predicted to transform the traceability of transactions (Deloitte 2017; Dai et al. 2017; Dai & Vasarhelyi 2017; Fanning & Centers 2016; Hughes et al 2019; Kokina et al. 2017). Operating as a decentralised, definitive ledger which records transactions into blocks (Dai et al. 2017; Fanning & Centers 2016; Nakamoto 2008), blockchain technology boasts several characteristics that make it unique from existing accounting technologies (Hughes et al 2019; Schmitz & Leoni 2019). Whilst both the accounting and technology literatures have identified opportunities and challenges with blockchain systems (Deloitte 2017; Dai et al. 2017; Dai & Vasarhelyi 2017; Fanning & Centers 2016; Schmitz & Leoni 2019) research is yet to empirically examine the relationship between blockchain systems and the concept of accountability. Popular practitioner outlets cite the role of blockchain systems as increasing the visibility and accountability of actors – through its distribution, ubiquitous availability, and the availability of multiple records of proof (Deloitte, 2017; PwC Global, 2019). Accountability is touted as one of the major benefits of blockchain, yet we know little about whether and how accountability is constructed in blockchain technology.

Accountability refers to the responsibilities an entity is expected to uphold (Messner 2009; Mulgan 2000; Ribstein 2006; Roberts 2009). Requiring explanations and justifications for decisions (Lerner & Tetlock 1999; Messner 2009; Roberts 1991), accountability is a construct that creates a "relationship of responsibilities" (Mulgan 2000, p.87) between interacting entities. Playing a crucial role in a variety of fields, ranging from technology (Keller & Bichelmeyer 2004) to education (Petterson & Solstad, 2007) and health care (Emanuel & Emanuel 1996), accountability reflects a construct that affects not only organisations (Benston 1982) but also individuals (Lewis et al. 2019; Roberts 1991; Rus et al. 2012) and the wider society (McKernan & MacLullich 2004; Schweiker 1993).

The rise in interest in blockchain has led to the emergence of several blockchain-related papers within the accounting literature over the last few years (Cai 2018; Carlozo 2017; Dai et al. 2017; Dai & Vasarhelyi 2017; Kokina et al. 2017; Schmitz & Leoni 2019). Although prior literature has tended to focus on public blockchains such as Bitcoin (Cai 2018; Hughes et al 2019) and the potential of blockchain systems, with suggestions for the application of blockchain in voting, leasing, online gambling, supply chain, and auditing (Dai et al. 2017; Deloitte 2017; Fanning & Centers 2016; Kshetri 2018; Liu et al 2019; Swan 2016), the literature lacks an assessment of the accountability the technology provides in practice (Schmitz & Leoni 2019). Examining accountability in relation to blockchain systems is important because the nature of accountability within this platform remains unclear, and pure forms of blockchains are often claimed to be exemplary forms of accountability constructs; but how they do so (Batubara et al 2019), and their actual manner of working beyond cryptocurrency applications has not been studied yet. Thus, the objective of this study is to examine how blockchain systems construct accountability.

Our motivation is twofold. First, there is substantial interest at present in better understanding the role of accountability in blockchain systems (McBurney 2018). The Gartner Inc. '2019 Hype Cycle for Blockchain Technologies' depicted in Figure 1 below mirrors these results. Despite blockchain currently sitting in 'the trough of disillusionment', the technology is expected to advance to a 'plateau of productivity' in the next 2-5 years, before revolutionising business activity in the next 10 years (Gartner, Inc. 2019). Further, a majority of senior executives appreciate, but do not fully understand its potential (KPMG LLP, 2019). Therefore, our first motivation is to examine how blockchain technology is evolving to align with corporate practice, and the implications of this for the construction of accountability itself.

***[Insert Figure 1 here]***

The second motivation of this study is to build and extend the breadth of blockchain systems studied in accounting literature. Existing blockchain research in the accounting literature has centred upon blockchain technology as it is applied in the Bitcoin network (Cai 2018; Hughes et al 2019). In recent years, other academic literature has begun to move beyond research in Bitcoin cryptocurrency-related blockchain (Tapscott & Tapscott 2016), but a large gap still exists in the accounting literature regarding our understanding of the different types of blockchain systems. Illustrating that blockchain technology takes a variety of different forms that go beyond the public blockchain structure underlying Bitcoin (Asolo 2018b; DragonChain 2019; Khatwani 2018; Yafimava 2019; Zheng et al. 2018), we focus on the three types of blockchain systems most commonly found in practice: public, private and consortium blockchains. Transforming into variants that soften the assumptions of the original public blockchain,

private and consortium blockchains provoke central questions surrounding the monitoring and controlling of blockchain participants. Our second motivation is therefore to examine how these types of blockchain systems differ, and the implications of these differences for the construction of accountability.

Our central research question underpinning the abovementioned motivations are: how do blockchain systems construct accountability? Answering this question requires an examination of both the elements and mechanisms which form accountability across the three different types of blockchain systems – public, private and consortium blockchains (Bovens 2005; Roberts 1991; O'Neill 2004; Hyndman & McConville 2018; Roberts 2009). Our study is exploratory in nature owing to the relative infancy of blockchain practice, contributing to a lack of blockchain experts as well as organisations speaking of it at present. Yet, there are early adopters and experts working with industry to drive their use, and we sought to identify these individuals to explore our research question. This drove our selection of a more qualitative, exploratory field study method. Eighteen blockchain experts were interviewed over a ten-month period across private, public and consortium blockchains to better understand the construction of accountability in these blockchain systems.

We offer three key findings. First, while both private and consortium blockchains display elements of the principal-agent relationship (Lindberg 2009; Mulgan 2000), public blockchains eliminate the need for the separation of a principal and agent. Embedding accountability by design through consensus mechanisms and the alignment of incentives, public blockchains essentially remove the requirement for explanations and justifications for decisions as identified in Lerner & Tetlock (1999) and Messner (2009). They do not require a "relationship of responsibilities" (Mulgan 2000, p.87) to establish accountability.

Second, by expanding our study of public blockchains to include private and consortium blockchains, we note that the different types of blockchain systems employ different forms of blended accountability elements. While public blockchains emphasise individual accountability (Bovens, 2005), private blockchains rely on a mix of hierarchical (Roberts 1991) and individual (Bovens 2005) forms of accountability. Consortium blockchains, by contrast, construct a mix of socialising (Roberts 1991), corporate and individual (Bovens 2005) forms of accountability. Blockchains and their accountability potential cannot therefore be considered a unilateral construct. Also, individual accounts in public blockchains are constructed differently in its manner of application to private and consortium blockchains. This arises primarily because accountability in public blockchains emanates only from a self-accountability perspective.

Third, we explain how trust and transparency, as two mechanisms of accountability, are mobilised differently across the three blockchain types. As the underlying code of public blockchains is available in the public domain and adhere to consensus mechanisms, trust is placed in the code and consensus algorithm (Jeacle and Carter 2011), with transparency expressed by the fact that transactions are visible to everyone on the network. By contrast, users of private blockchains place their trust in a central authority, assuming the authority will not act in self-interest during transactions. While there is transparency of network participants who are provided access to the private blockchain by the central authority, there are limits to this transparency as private blockchains cannot be separated from the social and political drivers that constructed them (Roberts 2009; McKernan 2007; Power 2004; Robson 1992). Trust and transparency in consortium blockchains, on the other hand, differs from network to network. Dependent upon the access and rights permissions given to a user, trust is placed in the governing body, code and/or consensus algorithm instituted by network participants, with transparency ranging from full visibility over all transactions within the network, like in the context of public blockchains, to the restricted visibility similar in private blockchains.

From our findings, we claim three contributions to the accounting literature. First, public blockchains do not require many traditionally vital components of accountability to possess accountability itself. Prior literature depicts accountability as a construct which necessitates a "relationship of responsibilities" (Mulgan 2000, p.87) between a principal and an agent (Lindberg 2009; Mulgan 2000) to ensure its establishment. Public blockchains, however, do not require the same. Via consensus mechanisms and the alignment of incentives, public blockchains construct accountability in a way that removes the requirement for explaining and justifying decisions (an alternative view to Lerner & Tetlock 1999 and Messner 2009).

Second, we find that a 'blockchain' manifests in a multiplicity of forms, two of which mobilise distributed ledger technology in a softer way than in public blockchains. We advance Cai et al (2018) by expanding the analysis of blockchain types in accounting research. Also, advancing Hughes et al (2019), we explain how accountability relates to public, private and consortium blockchains. We also find that dichotomous classifications of accountability as either hierarchical or socialising, per Roberts (1991) or corporate or individual, per Bovens (2005), are somewhat incomplete and that different types of accountability can simultaneously exist in each of the three blockchain types.

Third, we show how the three types of blockchains, to varying extents, use code and algorithms to build reliance and consensus between users, ultimately removing (public blockchains), reducing (consortium blockchains) or transforming (private blockchains) how trust between individuals is implicated in a system characterised by distributed ledger architecture. Traditional accountability

settings in the literature have not considered consensus within accountability itself. We offer a novel, technology-driven setting to claim a contribution to accountability theory by highlighting the value of consensus mechanisms in constructing accountability, and illustrate how the greater their role, the less that trust between individuals is required for the system to function. Blockchain systems move trust to decentralised computers (DragonChain 2019; Khatwani 2018; Nakamoto 2008), demonstrating new ways in which trust, transparency, and consensus work to facilitate accountability in practice.

The remainder of this paper is structured as follows; the next section reviews the existing literature on accountability and the three blockchain system types – public, private and consortium – that underlie this paper. The research method section then outlines how the research question was investigated, including data collection and data analysis methods. Thereafter a presentation of the findings is provided, followed by a discussion around the construction of accountability in public, private and consortium blockchains. The final section discusses the conclusions and limitations, with promising avenues for future research.

## Accountability and Blockchain

### *Background to Blockchain Research in the Accounting Literature*

The rise in interest in blockchain has led to the generation of several blockchain-related papers within the accounting literature over the last few years (Cai 2018; Carlozo 2017; Dai et al. 2017; Dai & Vasarhelyi 2017; Hughes et al, 2019; Kokina et al. 2017). While prior literature has tended to focus on the potential of blockchain systems, the literature lacks an assessment of the accountability inherent in the structure of blockchain itself, and how the technology constructs accountability in practice. We examine the broad concept of accountability more closely.

### *Accountability*

The accounting literature is replete with a wide range of definitions of accountability (Bovens 2005; McKernan & MacLullich 2004; Sinclair 1995). Whilst the literature is broad and accountability has been defined in a multiplicity of ways, accountability definitions related to responsibility seem to be most appropriate for an application of the construct to blockchain systems. This is because blockchain is a technology which was created to remove the need to rely on an intermediary to process transactions between two parties (Nakamoto 2008). To this end, we define accountability as the responsibilities an entity is expected to uphold (Messner 2009; Mulgan 2000; Ribstein 2006; Roberts 2009).

As an obligation between a principal and agent/actor[1] (Lindberg 2009; Mulgan 2000), accountability creates a "relationship of responsibilities" (Mulgan 2000, p.87). Requiring explanations and justifications for decisions (Lerner & Tetlock 1999; Messner 2009, Roberts, 1991), principals can demand actors to account for their actions and impose sanctions (Lindberg 2009; Mulgan 2000). Accountability is a valued but notably elusive concept (Sinclair 1995) and has widely come to be understood as "the giving and demanding of reasons for conduct" (Roberts and Scapens 1985, p.447), with critical accounting researchers highlighting various forms (Roberts 1991; Sinclair 1995) and styles (Ahrens 1996) of accountability.

*Forms of Accountability*

Whilst the extant literature presents a range of ways to classify accountability (Bovens 2005; Roberts 1991; Kroon et al. 1991), the accounting literature traditionally differentiates between two forms of accountability: hierarchical and socialising (Roberts 1991). Identifying that accountability affects people on an intrinsic level, Roberts (1991) examines the effect that accountability has on one's sense of self. Firstly, he identifies that accountability can shape an individual's sense of identity. In providing people with an avenue to be acknowledged, accountability provides a mechanism that enables people to confirm their sense of self. Roberts (1991) refers to this type of accountability as hierarchical, emphasising "strict lines of command" (Bovens, 1998; p.74).

Following the examination of hierarchical accountability, Roberts (1991) identifies a second form of accountability which he refers to as socialising. This form of accountability contrasts hierarchical accountability and connotes an informal interdependence. Socialising accountability provides individuals with a richer sense of recognition than its power-driven hierarchical counterpart (Roberts 1991). Socialising accountability can be likened to the collective form of accountability explained in Bovens (2005).

As it is currently unclear in the extant literature which party assumes responsibility in blockchain settings and "who is to be held to account when unforeseen difficulties such as fraudulent transactions occur" (Schmitz & Leoni 2019, p.340), the classifications that Roberts (1991) and Bovens (2005) provide enable a paper examining accountability as a responsibility which is placed upon one to better understand "who qualifies as the accountor?" (p.189). Bovens (2005) provides insights into two other

[1] This paper' references to an 'actor' refers to a human actor only. Whilst acknowledging that the research methodology Actor Network Theory (Latour 1987, 1993; Callon 1984; Law & Callon 1992) also refers to technologies and systems as actors, this paper does not employ this methodology. As this paper conducts an exploration of accountability within the context of a technology, the technical system of interest (blockchain) is not considered an actor, but rather the context within which a human actor participates.

forms of accountability: individual and corporate accountability. Individual accountability refers to how individuals are judged on their actions rather than their relationship to or within an organisation (Bovens 2005). Recognising individual accountability as a form of accountability in which an individual should be held responsible for their actions, Bovens (2005) highlights the importance associated with imposing sanctions on responsible individuals. The corporate form of accountability contrasts individual accountability as it focuses on the organisation as an 'actor' (Bovens 2005).

As face-to-face interaction declines and becomes less significant in some contexts – especially with the advancement of technologies such as blockchain – the possibilities of socialising forms of accountability also decrease. This increases the need for calculating systems of accountability, which enable "more distanced forms of accountability" and control from a distance (Roberts and Scapens 1985, p.451). With distance, the relative importance of accounts increases because it becomes the primary and only source of information for actors to interpret and make judgements or decisions about the performance of the individual and the organisation (Roberts and Scapens 1985). However, these accounts "will be from a particular point of view, at a particular point in time … a partial, selective and potentially distorted reflection of the flow of events and practices that constitute organisational life" (Roberts and Scapens 1985, p.454). Thus, there is a risk that this particular point of view is taken to depict the only product of organisational reality. This illustrates that there are limits to accountability.

*Limits to Accountability*

To develop a greater understanding of what those limits are and the implications they may have on the construction of accountability, Messner (2009) explores the limits of accountability by asking whether more accountability is always beneficial. Identifying that the accountable self is constrained by its opacity, exposure to the principal and by the mediation required to be accountable, Messner (2009) demonstrates that these constraints limit the extent to which one can be accountable, a notion which is grounded in the work of Sinclair (1995) and Butler (2001, 2004, 2005). Showing that people can be held accountable for things outside of their control, Messner (2009) argues that there are ethical implications associated with greater accountability and that they impact not only the accountable self, but also the stakeholders that depend on their accountability. Considering the tensions Messner (2009) brings to the topic of accountability, it is vital to understand the mechanisms[2] of accountability that are constructed and utilised by principals to hold agents responsible.

[2] Bovens (2010) sees mechanisms of accountability as an institutional arrangement in which an agent can be held to account by a principal. The locus of accountability is not the behaviour of the principal-agents but the way in which these institutional arrangements operate.

*Mechanisms of Accountability*

Two key mechanisms of accountability explored by the extant literature are trust and transparency. Ammeter et al. (2004) draw strong parallels between the two constructs and demonstrate their significant impact on human behaviour in organisations. Playing a key role in blockchain systems, trust and transparency are constructs which are yet to be examined against a blockchain setting. Thus, this study, whilst acknowledging that there are other mechanisms of accountability such as performance measures, will more closely explore trust and transparency as mechanisms of accountability in blockchain systems.

*Trust as a Mechanism of Accountability*

One means which principals use to facilitate accountability is through trust (O'Neill 2004; Hyndman & McConville 2018). Defined as the "provider for the existence of relationships without the need for continual proof of legitimate intentions of the members" by Ammeter et al. (2004, p.49), trust is a social construct that offers organisations a range of benefits (Calnan & Rowe 2008). One such benefit that arises in employing trust emerges from principals being able to utilise pre-established notions of an agent to determine their ability to meet expectations (Ammeter et al. 2004; Rotter 1967). Jeacle & Carter (2011) reflect on this sentiment in their study of how interactive online forums, such as TripAdvisor, produce both personal and systems trust. They found that when a user saw that another user had made multiple contributions to the online forum, the former assumed that the contributing user had greater credibility and thus was more likely to trust the other's reviews.

Enabling a principal to rely on their existing knowledge and assumptions of an agent, trust as a mechanism for accountability lessens the amount of time a principal will spend verifying an agent's actions. Contributing to a reduction in a firm's monitoring and surveillance costs (Bromiley & Cummings 1992; Calnan & Rowe 2008), trust as a mechanism of accountability also leads to an increase in firm efficiency (Calnan & Rowe 2008). In addition to these advantages, De Cremer et al. (2001) found that trust leads to increased contributions from agents. As a result of a combination of high trust and accountability, De Cremer et al. (2001) shows that when actions are identifiable, agents become more engaged and motivated to meet expectations (Ammeter et al. 2004; Calnan & Rowe 2008).

However, despite the range of benefits produced through the employment of trust in organisations, researchers have identified several limitations that arise following the application of this construct to accountability. One such limitation results from how trust is implemented. Swift (2001) explains that trust is hard to enforce as often there are no formal contractual obligations which hold the agent

accountable. Consequently, as agents realise they are not being observed, some will choose to take advantage of the trust mechanism and will work less hard than they would if other mechanisms of accountability were employed (Rotter 1980). People generally require additional mechanisms of accountability to be motivated to engage in cooperative behaviour (Calnan & Rowe 2008; De Cremer et al. 2001). An additional limitation of employing trust as a mechanism of accountability stems around the inherent nature of one to act in their own self-interest. As O'Neill (2004) explains that it is "intrinsically immature" (p.269) for one to assume others will act in another's best interests, it becomes evident that trust can lead to lower levels of monitoring associated with accountability. Demonstrating that trust alone cannot act as a mechanism of accountability, the tensions within the literature highlight the importance of examining both the advantages and disadvantages of any construct that aims to form accountability.

*Transparency as a Mechanism of Accountability*

In addition to trust, transparency is another proposed mechanism for accountability (Roberts 2009) which also possesses a range of benefits and limitations. Defined as the result of making something visible from the outside (Hood 2010; Roberts 2009), transparency is argued as critical for accountability. One advantage that arises from employing transparency as a mechanism of accountability is that it encourages improved organisational performance (Fox 2007). Providing a mechanism to address deep-seated issues (Fox 2007), transparency as process visibility (Bernstein 2017) enables both internal and external stakeholders to review an organisation's processes and hold them accountable for their actions.

Resulting in greater "self-control and self-observation" (Roberts 2009, p.962; Power 2007), transparency forces agents to review their actions actively and repeatedly. This increased self-control and self-observation limits abuses of power (Fox 2007). As transparency is recognised as a means of surveillance (Bernstein 2017; Fox 2007), individuals looking to exploit systems have less capability and incentive to escape the consequences of nefarious actions.

Although transparency as a mechanism of accountability presents benefits, researchers have identified unintended consequences that can result from this construct. One such consequence stems from how transparency is created. Chua (1995) identified that to achieve transparency, one must conduct a complex and laborious process. However, once a transparent system is constructed, it can never be deemed to be fully transparent as the system itself cannot be separated from the social and political drivers that created them (Roberts 2009; McKernan 2007; Power 2004; Robson 1992). This in turn significantly affects the accountability that can be generated. As Roberts (2009) states,

"transparency becomes accountability by simply turning measures into targets" (p.962), it is evident that transparency provides a simplified view of an organisation's reality which arguably leads to self-censorship (O'Neill, 2002).

Despite the complex relationship between accountability and transparency, many accounting researchers have acknowledged that the rise of online technologies and digital accounting ecosystems, such as cloud accounting and blockchains, has become an increasingly important means for corporations to report financial and non-financial organisational information, communicate timely disclosures, and meet increasing corporate transparency and accountability demands (Koreto 1997; Cho et al 2009). This digital revolution has enabled democratic and "interactive possibilities for accountability" (Lowe et al. 2012, p.191), such that in recent years, methods of accountability have undergone extensive technological disruption (Ryan 2012; Scott & Orlikowski 2012; Dai et al, 2017). One of these latest technological disruptors – blockchain – is transforming the accounting world (Schmitz & Leoni 2019; Kshetri 2018; Aste et al. 2017), and yet our understanding of the construction of accountability in blockchains is limited. We proceed to introduce explanations for this technology, in its various forms.

**Blockchain**

Blockchain is essentially a decentralised ledger, which records transactions into blocks (Dai et al. 2017; Fanning & Centers 2016; Nakamoto 2008). These blocks are shared via a peer-to-peer (P2P) network, before being accepted and added to the chain (Fanning & Centers 2016; Kokina et al. 2017; Nakamoto 2008). The chain consists of interlocked blocks that enable observers to see the order and nature of previous transactions (Dai et al. 2017; Nakamoto 2008). Observers are unable to modify transactions on the blockchain, as the technology is tamper-resistant (Dai et al. 2017; Fanning & Centers 2016; Kokina et al. 2017). Data may only be appended to the blockchain via the generation of a new block (Nakamoto 2008).

The concept of blockchain first appeared in the paper 'Bitcoin: A Peer-to-Peer Electronic Cash System' (Nakamoto 2008). Initially developed to operate the world's first cryptocurrency, commonly known as Bitcoin (Fanning & Centers 2016; Hughes et al 2019; Mendez 2018), blockchain has evolved to support numerous industries (Dai et al. 2017; Deloitte 2017; Fanning & Centers 2016). However, to understand the role accountability plays in those systems, the differences between the types of blockchains must first be elaborated.

*Public Blockchains*

The most well-known type of blockchain is the public blockchain. Created to move trust away from single centralised entities to groups of decentralised computers, public blockchains were developed to prevent censorship and corruption (DragonChain 2019; Khatwani 2018; Nakamoto 2008). To achieve this, public blockchains were designed to be publicly accessible and to provide each client with an up-to-date record of all past transactions (Angus 2018; Lin & Liao 2017; Mohammed 2018; Shiff 2018; Zheng et al. 2018). Ensuring that network transactions remain transparent to all, public blockchains establish security through peer participation (Shiff 2018; Zheng et al. 2018). The more the peers, the more difficult for one participant to manipulate the network (Angus 2018; Asolo 2018b; Thibodeau 2019). The decentralised structure of public blockchains enables anyone to transact any time, from any location (Asolo 2018b; Hughes et al 2019; Mohammed 2018; Shiff 2018; Siba & Prakash 2016; Zheng et al. 2018). This creates a system that does not require trust in a central authority (Davies 2019; Khatwani 2018).

A popular example of a public blockchain is Bitcoin, the world's first cryptocurrency (Fanning & Centers 2016; Hughes et al 2019; Mendez 2018). The fundamental benefit of Bitcoin is its decentralised structure. Bitcoin removes the need for a central authority and enables people globally to engage in transactions directly (Asolo 2018a; Siba & Prakash 2016; Lin & Liao 2017; Mohammed 2018; Shiff 2018). Another benefit is the privacy it affords. In collecting only a user's wallet address and no identifiable information (Hobson 2013; Thibodeau 2019), the network's transaction history can remain open and transparent for all (Shiff 2018; Zheng et al. 2018). This attribute ensures the network is rarely manipulated by any one actor (Angus 2018; Asolo 2018b; Thibodeau 2019; Zheng et al. 2018).

However, tensions exist around Bitcoin, and one issue is the network's design. Users are pseudo-anonymous, not anonymous. Identifying only a user's wallet address in the transaction history of the network, Bitcoin cannot assure that its users will inadvertently link themselves to their wallets (Hobson 2013). If this occurred, the user might be linked to their previous transactions. Additionally, the network characteristic of pseudo-anonymity has led to the trading of illicit goods on the dark web (Foley et al. 2019). As Bitcoin by design does not require identifying information of its users, authorities face difficulty in pursuing individuals purchasing illegal items with Bitcoin (Foley et al. 2019). Finally, as Bitcoin is not backed by a central authority, it is more volatile than fiat currencies (Hobson 2013; Shubber 2015). Evidently, there is increasing value but rising tensions surrounding the use of public blockchains such as Bitcoin, for regulators.

*Private Blockchains*

Private blockchains differ from public blockchains owing to its ownership structure. Created to remain the property of one entity (Khatwani 2018), private blockchains are operated by a central authority who controls what can be published on the blockchain (Khatwani 2018; Lin & Liao 2017; Mendez 2018; Siba & Prakash 2016; Zheng et al. 2018). Centralised in structure, this type of blockchain provides users with a more transparent database of transactions within their organisation (Davies 2019; Khatwani 2018; Zheng et al. 2018), to a closed group of participants. However, private blockchains are less secure than other blockchains due to its closed nature (Davies 2019; Yafimava 2019). Ensuring that only verified parties can participate in transactions, the central authority in private blockchains can utilise access and rights permissions to control the network (Lin & Liao 2017; Mohammed 2018; Yafimava 2019; Zheng et al. 2018). However, questions around the legitimacy of private blockchains continue to rise (Khatwani 2018; Thibodeau 2019).

One prominent example of a private blockchain is the forthcoming Australian Stock Exchange (ASX) distributed ledger technology (DLT) system. ASX DLT will replace the existing Clearing House Electronic Subregister System (CHESS) which is used to record share related transactions (ASX 2019a). Created in partnership with Digital Asset, an established DLT provider, DLT solution has been designed to operate a closed, private network where only permissioned participants can view the database (Angus 2018; ASX 2019a; ASX 2019b; Maxwell 2018; Nott 2018). DLT addresses privacy concerns whilst effectively distributing a single source of truth to all who require it (ASX 2019a; ASX 2019b; Nott 2018).

ASX DLT claims to offer greater benefits to the wider market than CHESS (ASX 2019a; Nott 2018). Ranging from "improved record-keeping; reduced need for reconciliation between multiple databases; more timely transactions and a better-quality source of truth data" (Nott 2018, para.12), each of these benefits reflect some of the key features of private blockchains. However, the ASX DLT solution contains limitations, primarily being the existence of a single point of failure (Khatwani 2018; Thibodeau 2019). If the DLT system or the ASX were to experience a technical failure post-implementation, all transfer and settlement of market transactions would cease immediately and would not resume until the failure is resolved (Shivang, 2019).

*Consortium Blockchains*

The final type of blockchain is consortium blockchains. Created to improve business processes through collaboration, consortium blockchains encourage companies to form collectives to develop solutions to shared problems (Asolo 2018a; Yafimava 2019). Consortium blockchains determine a pre-selected number of nodes (also known as participants) that are required to achieve consensus (Asolo 2018a;

Thibodeau 2019; Yafimava 2019; Zheng et al. 2018). Also known as a federated or hybrid blockchain, this type of blockchain combines elements of both public and private blockchains (Asolo 2018a; Mendez 2018; Thibodeau 2019; Yafimava 2019). Like private blockchains, consortium blockchains preserve a degree of control over the network, however, like public blockchains, the network is decentralised enough to enjoy greater security than private blockchains (Asolo 2018b). Operating as a permissioned, semi-decentralised network, consortium blockchains provide groups of companies with the opportunity to engage in a network that doesn't necessitate trust in a central authority (Asolo 2018a; DragonChain 2019; Ganne 2019; Yafimava 2019; Zheng et al. 2018).

Voltron is one example of a consortium blockchain. Developed as a trade finance blockchain, Voltron is designed to improve documentary trade by digitising the letter of credit process (Ganne 2019; Lundström & Öhman 2019; R3 2019; R3 2018; Voltron 2019; Wass 2019). Founded by eight banks, namely Bangkok Bank, BNP Paribas, CTBC Holding, HSBC, ING, NatWest, SEB and Standard Chartered, this consortium saw the process efficiencies a consortium blockchain could provide to their operations (Ganne 2019; Lundström & Öhman 2019; R3 2018; R3 2019; Voltron 2019; Wass 2019). Ensuring that all the parties involved in the letter of credit process can exchange and agree upon a single version of trade documents, Voltron effectively creates an open, yet secure network for competing organisations to engage in trade with each other (DragonChain 2019; R3 2018; R3 2019; Voltron 2019).

**Blockchains and the Construction of Accountability**

Existing blockchain research in the accounting literature has centred upon blockchain technology as it is applied in the Bitcoin network (Cai 2018; Hughes et al 2019). Whilst in recent years the academic literature has begun to move beyond research in the blockchain field which primarily focuses on cryptocurrencies such as Bitcoin (Tapscott & Tapscott 2016), a large gap still exists within the accounting literature when it comes to understanding the different types of blockchain systems. This distinction is important as the different types of blockchain systems are likely to have different implications in the way accountability is constructed.

As recognised above, blockchain technology takes a variety of different forms that go beyond the public blockchain structure of Bitcoin. Since the creation of Bitcoin in 2008, blockchain technology has evolved to take different forms as businesses and governments have realised a range of potential applications for the technology (Tapscott & Tapscott 2016). However, the blockchain system required for each of these applications will differ. Thus, we explore the recognition that not all applications of blockchain technology use the fully decentralised structure of public blockchains underlying the Bitcoin network described by Cai (2018). In addition to examining public blockchain systems, we

consider the workings of private blockchains and consortium blockchains, two less studied blockchain types. Having identified the three blockchain types, we explore how accountability relates to these different types of blockchains.

Within the IT literature, some research exists on the governance of decentralised autonomous organisations[3] (DAOs) (Beck et al. 2018). Examining decision rights, accountability, and incentives against a case study of an emerging DAO, Beck et al. (2018) aim to understand the implications for governance when DAOs form a blockchain economy in the future. Whilst this research is valuable for understanding governance within future applications of blockchain, the DAO being explored in Beck et al. (2018) is still undergoing development. With the existence of a range of blockchain applications across the different types of blockchains that are currently in use in society and the expected influx of applications projected to be employed in the near future (Gartner, Inc. 2019), it is now vital to understand accountability within existing blockchain applications. Thus, we examine how blockchain technology is evolving to align with corporate practice and the implications this has for the construction of accountability.

The next section continues the examination of how blockchain systems construct accountability by explaining the research method adopted to address this paper's research question.

## Research Method

This research is based on a qualitative field study of the Australian blockchain industry, drawing on insights from blockchain experts engaged in the digital economy through blockchain technology. Australia was chosen as the field site for this research for three reasons. First, Australia chairs the International Standards Organisation (ISO)'s development of blockchain and other Distributed Ledger Technology standards (Eyers 2018). Australia's role in chairing the ISO blockchain committee demonstrates that the country has the technical expertise and knowledge to better understand how accountability is constructed through the application of the blockchain technology in practice.

Second, the Australian Securities Exchange (ASX) is the first stock exchange in the world to invest several million Australian Dollars to replace the processes of clearing, settlement, asset registration, and some other post-trade services, which are critical to the orderly functioning of the Australian financial market, with a blockchain-based platform (ASX 2020). This illustrates that Australia is at the forefront of implementing blockchain technologies within key sectors of their economy, with the

[3] A DAO is a company which is comprised of blockchain technology. DAOs operate businesses by following rules established in smart contracts (Dai & Vasarhelyi 2017).

Australian government providing grants and incentives to study potential use cases of blockchain technology for the public sector and industry (Coyne 2016).

Lastly, the Australian government has also launched *The National Blockchain Roadmap* in Australia, focusing on the government's plans to invest, regulate and innovate the technology and boost wider adoption nationwide. Australia is recognised as a global leader in blockchain technology and this is evidenced by the rise in blockchain implementation across new and existing private and public organisations in Australia (Commonwealth of Australia 2020; Thompson 2019).

Data was collected over a period of 10 months. In exploring a phenomenon which is not bound by organisation, it was required to collect and analyse data from a range of individuals working across a range of organisations. As Table 1 illustrates, a total of twenty interviews were conducted with eighteen blockchain experts from various industries in Australia. The interviewees included solutions architects, lawyers, auditors, product managers and developers. Interviewees were approached through email, phone, direct messaging and/or attendance at industry forum events. A number of these individuals were identified through personal networks, whilst the rest were specifically selected following discussions at industry forum events. All interviewees were informed of the purpose of the study, assured that their identities would be anonymised and were provided with an introduction to the research aims alongside a participant information sheet and consent form before attending their interview. Interviews were semi-structured and were between half-an-hour to two hours in duration. Eighteen of the twenty interviews were conducted face-to-face and two were completed over Zoom[4] as the interviewees were based in another Australian city.

***[Insert Table 1 here]***

The main objective of interviews with blockchain experts was to understand the different types of blockchain systems and gain insights into how accountability was constructed within those systems. Each interview began with questions centred upon the professional background of the interviewee and their blockchain expertise. The information obtained from these first questions enabled the researchers to determine which type of blockchain system an interviewee specialised in. Following this, the researchers were able to tailor the accountability questions to focus upon the interviewee's area of expertise. As the interview progressed, the researchers asked the interviewee for examples to support their responses. This probing ensured that the interviewees were clear on their answers whilst providing the researchers with greater understanding of important concepts (Liamputtong 2013). At

[4] Zoom is a video conference call software. See https://zoom.us/ for more information.

the end of the interview, interviewees were asked if they wanted to share any further insights and, in most cases, interviewees volunteered additional thoughts around existing applications and the construction of accountability in blockchain systems. This discussion was followed up with additional questions that flowed from their line of thought as recommended in Kvale (2008).

Each interviewee provided the researchers with verbal and written consent to record their interview. The researchers used a mobile device in each interview to record the audio, whilst also taking hand-written notes of key thoughts and insights provided during the interview. Following completion of the interview, the researchers saved and uploaded the audio into a secure cloud storage system. Audio was then transcribed using Rev and Temi[5]. These transcripts were then read in conjunction with the audio to ensure the transcription was consistent with the recordings.

Data coding was carried out by the lead author and was reviewed by the second author. Data was coded using the NVivo software (version 12), with interview coding carried out using thematic analysis which is a "method for identifying, analysing and reporting themes within data" (Braun & Clarke 2006, p.79). The thematic form of data analysis enabled the researchers to find commonalities within and across the interviews and assess the prevalence of key themes (DeSantis & Ugarriza 2000; Vaismoradi et al. 2013). This involved identifying significant statements – paragraphs, sentences, or phrases – that related directly to accountability, to describe aspects of accountability within various blockchain systems as narrated by each participant. These significant statements from each interviewee were then compared across interviewees, paying particular attention to themes that were common across participants. Once these themes were identified, they were validated by reconciling each significant statement to its original narrative context. This process continued until key and related categories were sufficiently saturated to provide a connection of how accountability is constructed within different blockchain systems identified by research participants and present in practice. The next section narrates the key findings.

## Findings

### Public Blockchains

Public blockchains were defined as open, permission-less systems which anyone in any role could read, access, and participate in the network. Described as decentralised in nature, interviewees explained that in public blockchains, no one is in control of the network.

[5] Rev is an online transcription company and Temi is an online transcribing software which produces transcripts of audio files. See https://www.rev.com/ and https://www.temi.com/ for more information.

> Interviewee 3: "Blockchains are ledgers that record the ownership of assets. There must not be any centralised element. Anyone who wants to, should be able to participate in the network in any role that is possible. There must not be any privileged role that you cannot get to otherwise it's not open, not public."
>
> Interviewee 10: “I would define it (public blockchains) as obviously transparency, so anybody can see what the organisation is doing and see the code behind the blockchain. For example, Ethereum has an online open source repository where they store their code. There is also an open forum… you can see people contributing to the building of the blockchain and making features for the blockchain. …. so basically (a public blockchain) has an open source code and an open community…. another big benefit of public blockchains is that nobody really controls the blockchain…. its’ decentralisation is another big benefit as well.”

A public blockchain’s generation of distributed ledgers – a history which is visible and stored by all within the network – enables anyone to view and confirm any transaction that occurred within the blockchain, making it immutable in nature:

> Interviewee 10: “It (the ledger) has the history of everything that happens on the blockchain, and that history includes transactions between certain users, the amount of fees that are needed to transfer between user to user, and…. anybody can view that ledger. And it (the ledger) is a big part of accountability because this history can't be reversed and can't be changed.”

Additionally, certain groups play an important role in the transparent development and promotion of public blockchains:

> Interviewee 9: “Often a particular project will be backed by a group of people that will form a foundation… In the case of Ethereum there is the Ethereum Foundation - the group containing the code base. Developers are not responsible (for the public blockchain) because it (the code) is all published under the FLUX[6] license and well no one is accountable… I do not think anyone would really publish software in a public blockchain and assume liability. Pretty much everyone publishes under no liability (licenses). We (developers) make no guarantees about its (the blockchain’s) correctness or accuracy.”

Explaining that public blockchain technology is open source and published under no liability licenses[7], experts pointed out that users could not hold developers responsible for things that go wrong because the software is available in the public domain and employed at a user’s own discretion.

To understand at a deeper level who is responsible in public blockchains, interviewees were asked to reflect on their experiences with the networks and identify who had been held responsible in instances

[6] The name of the license has been changed for anonymity purposes.
[7] For example, on the Ethereum website, there is a limitation of no liability. https://ethereum.org/en/terms-of-use/

where something had gone wrong. Responses from this question were similar across the interviews, with numerous experts demonstrating that individuals were responsible for their own actions and could rarely impose sanctions on anyone but themselves.

> Interviewee 2: “The individual made the mistake… it’s personal responsibility. There is no authority to hold a central authority to hold account, so you have a personal responsibility to be responsible for every transaction that you send. You chose to do something without a trusted third party, so you take on that responsibility yourself.”

Experts showed that as holders of their own private keys, it is an individual’s responsibility to keep their key a secret and not allow anyone else to access it. Although it was highlighted that in instances where coin exchanges held an individual’s private key, ultimate responsibility lied with the individual.

> Interviewee 10: “You can blame the coin exchange, but you can also blame yourself for that because… you should be responsible for your own security. I mean, you should not be blaming people if you unlocked the front door and blame the locksmith. You should always be vigilant about your own security.”

Revealing that accountability within public blockchains lies with the holder of the private key, the experts showed that in most cases people could only have themselves to blame in instances where something did go wrong.

Participants were also asked who in their opinion *should be* accountable. While most working with public blockchains believed nobody should be held responsible in public blockchains as no one could control a public blockchain, accountability will ultimately be placed upon the one who has control over a user’s private key.

> Interviewee 2: “I don't think anybody should (be accountable) because if nobody is accountable, then no one or no group of people are empowered to make decisions based in their own interest that will result in their own interest.”

Embedding accountability by design through the utilisation of consensus mechanisms and the alignment of incentives amongst users based on game theory, public blockchains exclude the need for users to rely on and trust a central authority for accountability issues:

> Interviewee 2: “They're able to trust each other by essentially 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… There is only the integrity and the suitability and the validity of the consensus algorithm and the game theory that has been designed into the protocol. There is not anyone to be held accountable. There's just valid blockchain designs and there's invalid ones.”

> Interviewee 6: “You trust the consensus mechanism of the technology (in public blockchains). If you cannot hold an individual accountable, then you hope that the technology will do it for you.”

To participate in a blockchain’s consensus mechanism, a node (also known as participant) must stake something of value, for example electricity or some cryptocurrency (depends on the type of consensus mechanism employed in the blockchain), to keep the network running and to be eligible to receive the reward. When a node fails to achieve the outcome specified by the blockchain to reach consensus, the node will be forced to forfeit their stake with no chance of receiving the reward. Consensus mechanisms effectively align the incentives of blockchain participants to keep nodes accountable within public blockchains:

> Interviewee 11: “For example, in Bitcoin and most of the (public) chains nowadays…you have an incentive to mine because you get rewarded with newly issued Bitcoins. And as a result, because it is worth something then it is worthwhile to mine, and if it is worthwhile to mine then the network is stronger. So that is an alignment of incentives.”

> Interviewee 12: “…in the real world you will go to that participant and say, "Why did you act that way?" That is if you know their identity, and if you do not know their identity then you will have to look at other methods…such as consensus algorithms which are common to public blockchains. So, say for example if you acted maliciously in this validated pool and we do not know your identity, then there is no real way to hold you accountable in that sense. There are ways to basically make you incentivized to be a good actor… So, basically you have to have some sort of stake in the consensus and when you behave badly you lose that…you would not be a bad actor because you might lose your stake. That's of the belief that you value your stake enough and people are incentivized by monetary things, and your stake is monetary so you don't want to lose that and that's part of what keeps you accountable…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. So, I've already come up with a cost, I've already incurred a cost, but then I still get no reward for that cost… So, everyone who's involved in the consensus to validate a pool, they all have…a stake…”

Recognising that accountability within public blockchains is enforced through the consensus mechanism, experts reveal the implications this has on the level of trust that exists between individual users:

> Interviewee 4: “They don't necessarily trust one another, but they only trust each other to the extent that they agreed to perform consensus.”

**Private Blockchains**

Private blockchains were defined as closed, permissioned systems in which only preapproved nodes could read and request transactions on the network. Characterised as governed by access permissions,

interviewees explained that in private blockchains, a central authority, internal to an organisation, controls the conduct of all nodes and transactions on the network.

> Interviewee 6: “The way I would see a private blockchain would be like almost purely internal or where essentially one party holds all of the power.”
>
> Interviewee 8: “A private blockchain is when only permissioned users could see the transactions that have been written to blockchain… In a private blockchain because it's a permissioned system and because supposedly 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… in a private blockchain, you've just got a little bit more control theoretically over what your participants can and can't do.”

In terms of accountability within private blockchains, the experts explained that the accountability and control within the network are essentially centralised. Also identified as a notary, this central authority determines whether transactions on the network are valid:

> Interviewee 6: “(In a private blockchain)… you can restrict that (validation) to either one party or a series of parties operating together and they could either be parties that take part in the network itself, in like what it (the network) has been set up to do, or it could be an independent party who's writing that notarisation… so technically everyone is accountable to the notary.”

In a position to choose which nodes can participate in the network and which transactions to accept, the notary becomes the entity in private blockchains which holds users responsible.

Using a central authority to assure accountability, private blockchains were also stated to utilise the blockchain’s lack of anonymity to assess issues. As the identities behind all nodes within a private blockchain are known by the central authority, a notary can easily assess who is responsible for a certain transaction:

> Interviewee 6: “Typically in permissioned chains, you know, all of the parties who are on the platform, and that's probably one of the biggest differences between a permissioned chain and a public chain. If you (the notary) know something that is gone wrong, in a lot of cases you can very quickly see who it was that made it go wrong.”

Despite the identification of the governing role of the central authority within private blockchains, the experts presented differing opinions when it came to the recognition of who is responsible in the design and operation of private blockchains, spanning both developers (Interviewee 6) and regulators (Interviewee 5).

> Interviewee 6: “If the whole platform just fails, if there's like a massive security breach… then they're (developers) obviously accountable for that.”

> Interviewee 5: “We're developing a technical specification and that technical specification is supposed to guide how developers, enterprises, and governments develop smart contracts… So if you look at Ethereum in which some of their coins like the ERC20, they already have certain standards… and this technical specification that we're creating sits next to that, and it really considers the legal principles that these developers have to kind of be mindful of.”

In addition to encouraging developers to be mindful of legal principals, regulators can request businesses to employ auditors to assure their private blockchains:

> Interviewee 7: “Their (auditors) main job is just to be that source of trust that is going to say everything here is above board. You're trusting something that is automated with rules.”

As part of an organisation that conducts audits, Interviewee 6 provided further insights from his experience with regulators:

> Interviewee 6: “The government said (to a company looking to deploy their own private blockchain), we're (regulators) not letting you deploy your platform until you've gone to a major accounting firm and got them to give it the green light.”

Identifying three entities, namely developers, regulators and auditors, who can be argued to be responsible in the development and operation of private blockchains, the experts continued to present new insights into private blockchains when asked to reflect on their experiences with these networks. Like in public blockchains, where an individual form of accountability was identified, the experts of private blockchains identified individuals to be responsible in instances where something had gone wrong:

> Interviewee 6: “If you're putting the wrong stuff (data) in (the blockchain), then ultimately it's the responsibility of the party that did that.”

Furthermore, to gather further insights from the experts about the accountability within private blockchains, participants were also asked who in their opinion should be accountable. Interviewee 6 stated his thoughts as below:

> Interviewee 6: “Blockchain is meant to be a kind of trust-less technology where you should be able to trust everyone else on the network. So then why do you need an independent third party to provide trust to people? It is kind of counterintuitive. But until people trust the technology, there is still going to be demand for stuff (audit) that we do. Even if your actual blockchain platform is rock solid, that is just the bottom layer of a whole stack of tech… You've got to be able to trust the whole thing (system)…trust the data that's going on there in the first place…”

These insights into the relationship between blockchains, trust and transparency were supported by other experts:

> Interviewee 4: “Private blockchains rely on trust in the centralised authority, public (blockchains) don’t need trust in one entity because they trust in the code.”

> Interviewee 5: “With a private blockchain, if we have members in it and they're displaying it (manipulating transactions) to fit their agenda, then you can't really tell here. You can't really tell (if the transactions are accurate).”

Revealing that the centralised design structure and control of private blockchains reduce transparency with implications on trust, experts illustrated that the overall accountability of a private blockchain lies in the hands of the central authority.

**Consortium Blockchains**

Consortium blockchains were defined as permissioned systems in which control is distributed among selected nodes who can participate in the network:

> Interviewee 2: “(In a consortium blockchain) you have finite number of entities who have agreed to transact with each other and... if one of the participants wants to propose another entity to become a permissioned member of the network who can publish transactions or can propose blocks... then there's some sort of democratic process they might submit to.”

> Interviewee 7: “It (a consortium blockchain) is group of people who are collaborating with varying degrees of trust, and there's often a permissioned environment where some people may have more access to the initiation and orchestration of transactions. Some people may not be able to see one another's private transactions, whilst others may be able to.”

Comprised of a group of entities who have differing levels of access and read permissions, interviewees described consortium blockchains as networks where control over transactions can be established through a variety of means:

> Interviewee 7: “Sometimes there’s like a governance model where multiple people are elected, and they all govern the network together. Sometimes it is auditors that are the overseers. Generally, it's someone who has a stake but is not directly in competition or has an opposition in values.”

When asked about the role of accountability within consortium blockchains, the experts revealed that accountability within this type of blockchain is determined and distributed before the system is built by the main parties who commission the build:

> Interviewee 6: “The governance model that is defined, typically by the parties that developed it (the consortium blockchain) in the first place, tends to drive who is accountable to whom.”

Explaining that within a consortium blockchain, users are responsible to one another (i.e. users they are transacting with), the experts identified that within this type of network essentially everyone holds some level of accountability:

> Interviewee 5: “To really understand the role accountability plays in permissioned blockchains, you just got to figure out why you have it there in the first place. If it is established by consortium, and the consortium is working together in order to protect data, then it should all be super transparent, and everyone should really be accountable to each other.”

However, the experts also mentioned that an appointed governing body, referred to as the overseer of the network, can assist users in determining who is accountable. Referring to the ledger and an overseer’s ability to review all the transactions within the network:

> Interviewee 7: “They (the overseer) have this single source of truth that they can in theory, go back to. I guess a lot of them (users) like going back to the overseer of the network, a lot of them do rely on that for accountability and question one another for that.”

Interviewees shared insights as to who they thought is responsible in the design and operation of consortium blockchains. Citing developers, regulators and sometimes auditors to be responsible in these instances, interviewees presented similar responses to this question on consortium blockchains, as they did for private blockchains:

> Interviewee 1: “So it (accountability) is not just on the people developing it, it's also… (based upon) the regulatory obligations they've got to go meet.”

However, in addition to these entities, experts stated that the founding consortium members themselves play an important role in the design and operation of their networks:

> Interviewee 6: “It depends on how the governance is defined. Is it the software provider or is it the original consortium members? When there are changes in Ethereum, people vote, and everyone has an equal vote. Some permissioned chains may be set up in a similar way, but some might be set up by for example the original five members hold the voting rights and everyone else who joins has to just go with what they voted for.”

> Interviewee 7: “An auditor will always still have quite a bit of power, but they will also have the ability to track back and say, this is the exact point of failure.”

While auditors do still play an important role especially in instances of failure, founding consortium members were also found to be responsible in the design and operation of consortium blockchains. This was primarily due to the distributed control members had in defining and limiting what data is

accessible to each party on the blockchain from the network's inception, alongside being able to dispense voting rights.

To gauge whether these entities are responsible in any other instances in consortium blockchains, interviewees were asked to reflect on their experiences with the networks and identify who had been held responsible in instances where something had gone wrong:

> Interviewee 7: "The company, I think you might be able to find their statement about what they were going to do to be accountable to their users…. (This governing document describes) who is going to get in trouble for this, how are they going to make it up to you, is it them who is responsible to you, or do they just say it's this person's fault."

Following this explanation, Interviewee 7 shared an experience where things within the code her team had produced, had not gone as expected:

> Interviewee 7: "We've had a couple of vulnerabilities that someone luckily in our community found and flagged, but we had to tell our community about it to be transparent and accountable to them, which is hard."

Illustrating that when it comes to the construction of permissioned blockchains, developers do have a responsibility to be transparent with their users, Interviewee 7 showed that accountability can be promoted within the blockchain community through increased transparency.

To explore accountability in consortium blockchains more deeply, participants were also asked who in their opinion should be accountable. The experts recognised whilst everyone within that permissioned network should be responsible in a consortium blockchain, it is not currently the case:

> Interviewee 7: "I would normally say you should be accountable to everyone in that network, but I know for a fact that they are not. There is a lot of concern about not even showing everyone in your network what your transaction records are because then they could just be using that for competitive research... and be undermining you that way. There's just not enough trust to actually do it that way."

Revealing trust as a factor that is currently affecting the level of accountability within consortium blockchains, experts believed that the governing body or overseer plays a significant role in assuring transactions between individual consortium members are valid:

> Interviewee 7: "The two people transacting are accountable to one another and they just need that single source of truth to fall back on…. and people (auditors) come in and get paid to be the middleman and oversee the network."

Outlining the important roles played by individuals and governing bodies, the experts showed that both transacting and governing entities should be held accountable to some extent in consortium blockchains. The next section provides a discussion of the findings for this research.

## Discussion

From the findings, this research expands on how blockchain technology gives us cause to rethink the way accountability operates in organisational settings. The discussion is divided into three areas. First, accountability in the three different types of blockchain systems are considered, with a focus on theory relating to key accountability *elements*. Second, *forms* of accountability in the literature are related to the three blockchain systems to better understand how and when each applies in public, private or consortium blockchains. Lastly, we explain how two *mechanisms* of accountability, trust and transparency are used in constructing accountability within public, private and consortium blockchains.

### Accountability in Blockchain Systems

Examining the workings of accountability within public, private and consortium blockchain systems is important because the way accountability is constructed within this context is varied. To this end, this research emphasises that its manner of working is different for each of the three types of blockchain systems. Accountability has been recognised as the responsibilities that entities are expected to uphold to one another (Messner 2009; Mulgan 2000; Ribstein 2006; Roberts 2009). In private blockchains, the central authority is the entity tasked with the responsibility to hold network participants accountable for their actions. Provided with the ability to control who and what can be published on the blockchain (Khatwani 2018; Lin & Liao 2017; Mendez 2018; Siba & Prakash 2016; Zheng et al. 2018), the central authority can mobilise their position within the network to request explanations and justifications for decisions (Lerner & Tetlock 1999; Messner 2009) made by network participants. Demonstrating an application of the principal-agent interplay (Lindberg 2009; Mulgan 2000), private blockchains by design embed the traditional form of accountability identified within the accounting literature observed outside blockchain settings.

Like private blockchains, consortium blockchains enlist the principal-agent relationship (Lindberg 2009; Mulgan 2000) to assure accountability within the system. However, unlike private blockchains, the principal employed in consortium blockchains is usually not a single entity. Consortium blockchains are controlled by a group of companies rather than a single entity (Asolo 2018a; DragonChain 2019; Khatwani 2018; Yafimava 2019; Zheng et al. 2018). However, one or more (not always all) entities can be appointed to oversee others within the network. Consortium blockchains could also employ an

auditor to oversee network activity, or each party within the network could be considered both a principal and an agent as each user can hold the party they are transacting with accountable for their actions.

Differing from network to network, the principals within a consortium blockchain will nevertheless be able to demand network participants to account for their actions and could impose sanctions (Lindberg 2009; Mulgan 2000). Dependent upon "relationships of responsibilities" (Mulgan 2000, p.87), consortium blockchains require principals, whether they be a single entity or a group of entities or an external governing body, to assume the responsibility of holding network participants accountable. However, in having multiple entities acting as principals, consortium blockchains reveal softer forms of principal-agent interactions than that observed in private blockchains.

Whilst both private and consortium blockchains display elements of the principal-agent relationship (Lindberg 2009; Mulgan 2000), public blockchains eliminate the need for the separation of a principal and agent. Embedding accountability by design through consensus mechanisms and the alignment of incentives, public blockchains remove the requirement for explanations and justifications for decisions as discussed in Lerner & Tetlock (1999) and Messner (2009) and do not necessitate a "relationship of responsibilities" (Mulgan 2000, p.87) to establish accountability. The consensus mechanism employed within a blockchain ensures that issues of accountability do not arise post (trans)action as the agreement between what should be (i.e. expected performance) and what is (i.e. actual performance) is aligned through incentives that are only received if consensus is achieved. The incentive structure, unique to public blockchains, forces network participants to outlay an initial cost before having the opportunity to realise the reward for completing a (trans)action.

Advancing the work of Lindberg (2009) and Mulgan (2000) through the identification of a context in which accountability does not require a relationship between a principal and an agent, a key contribution of this paper is explaining how elements that were traditionally considered vital parts of accountability are not necessary to construct accountability in public blockchains. To this extent, these findings offer a conceptual explanation for how accountability might operate in a novel manner which departs from traditional notions of accountability, but in ways that conceptually depart from the explanations of Roberts (2009) and Messner (2009).

**Forms of Accountability in Blockchain Systems**

Accountability can be established in many forms, from hierarchical, to socialising, individual and corporate accountability (Bovens 2005; Roberts 1991). This paper looks at the accountability that is constructed in different blockchain systems. Whilst other forms of accountability could be argued to

be prevalent within entities that utilise blockchain systems, this paper focuses upon how blockchain systems construct accountability. Accordingly, we limit our discussion of accountability to focus on entities directly involved in the operation and use of blockchain systems.

Private blockchains' employment of a central authority enables companies to construct a hierarchical form of accountability. Created to remain the private property of a single entity (Khatwani 2018), private blockchains provide companies with the ability to decide who will control what can be published on the blockchain (Khatwani 2018; Lin & Liao 2017; Mendez 2018; Siba & Prakash 2016; Zheng et.al 2018) through the employment of a central authority. Providing one network participant with greater access and rights permissions than the rest, private blockchains provide a central authority with a superior position within the network. Subsequently establishing a form of accountability revolving around the hierarchical relationships established within organisations, a private blockchain can be argued to provide the hierarchical form of accountability described by Roberts (1991) which is prevalent in most traditional settings.

In addition to employing hierarchical accountability, private blockchains facilitate the individual form of accountability presented in Bovens (2005). The individual accountability produced in private blockchain falls upon the individuals given the responsibility to input and approve the data within the blockchain. Held accountable for any misconduct they personally contribute to, regardless of their position within the organisation (Bovens 2005), these individual actors are judged on their contributions to the blockchain by both external and internal significant others. The external significant others, an actor within a private blockchain, would have to account to could be any other individual within the company who can hold one to account and impose sanctions (Lindberg 2009; Mulgan 2000). The internal significant other, on the other hand, refers to one's own conscience which encourages the actor to conduct transactions within the blockchain in a morally acceptable way (Bovens 2005). Whilst the internal significant other tends to drive one's actions, it must be noted that the accountable self can be pressured by the external significant other and by the hierarchical relationships inherent in the design of private blockchains, to behave in immoral ways (Bovens 2005). Thus, whilst employing two forms of accountability, the hierarchical form of accountability generated by private blockchains is shown to play a more prominent role in providing accountability in private blockchains than other forms of accountability.

Consortium blockchains enlist the corporate, socialising, and individual forms of accountability (Bovens 2005; Roberts 1991) to assure that network participants are held responsible for their actions. A company takes on a level of responsibility as the organisation itself is participating in the blockchain as an 'actor' (Bovens 2005). Operating in a network in which other companies not only view but may

depend on the transactions being written to the blockchain, a company as an entity can be held accountable for their actions by other network participants and can have sanctions imposed upon them (Lindberg 2009; Mulgan 2000). With accountability depending upon the actions of individual corporations within the network, consortium blockchains can be argued to provide the corporate form of accountability described in Bovens (2005).

In addition to corporate accountability, consortium blockchains demonstrate the implementation of the socialising form of accountability examined in Roberts (1991). With some consortiums dependent upon a governing body made up of a group of companies (Asolo 2018a; DragonChain 2019; Khatwani 2018; Yafimava 2019; Zheng et al. 2018), an informal interdependence on others (Roberts 1991) may form, without precluding the existence of a socialising form of accountability.

Furthermore, an individual form of accountability (Bovens, 2005), is also prevalent in consortium blockchains. Like in private blockchains, the individual accountability generated in consortium blockchains falls upon the individuals given the responsibility to input and approve the data that goes onto the blockchain. Whilst emanating from both external and internal significant others, the individual accountability produced by consortium blockchains is generated by an additional external significant other to those identified in private blockchains. Other member companies within the consortium could also hold individual contributors to the blockchain accountable for their actions and impose sanctions upon them (Lindberg 2009; Mulgan 2000).

However, the individual accountability generated by consortium blockchains could be superseded by the corporate and socialising forms of accountability inherently possible in this type of blockchain because an actor may be pressured to perpetrate certain actions (Bovens 2005). Thus, whilst employing three forms of accountability, the corporate and socialising forms of accountability generated by consortium blockchains are shown to play a more prominent role in providing accountability in consortium blockchains than other forms of accountability.

Whilst private and consortium blockchains employ multiple accountability forms identified in Bovens (2005) and Roberts (1991), public blockchains necessitate only one type of accountability – individual accountability. Although producing a type of accountability that is established in both private and consortium blockchains, the individual accountability generated by public blockchains differs from the other blockchains because the accountability emanates only from self-accountability. As public blockchains are decentralised networks which assure every participant on the network has the same privileges (Fanning & Centers 2016; Kokina et al. 2017; Nakamoto 2008), there is no external entity that exists that can take on the responsibilities of another. Designed with the assumption that

participants within the network will act in self-interest, public blockchains lead to the creation of a system where no actor is required to trust any other actor on the network.

Overall, these findings demonstrate that the traditional understanding of accountability as either hierarchical or socialising, following Roberts (1991) or either corporate or individual, following Bovens (2005), is problematic and that these different forms of accountability can be intimately intertwined, enabled by and enabling the other, especially within the ever-increasing digital contexts by which everyday accountability is constructed. It also highlights that multi-faceted forms of accountability operate simultaneously and that the relative importance of individual accountability changes across alternative accountability forms in different blockchain systems.

**Mechanisms of Accountability in Blockchain Systems**

Trust and transparency were identified to facilitate accountability within blockchain systems (Schmitz & Leoni, 2019). In private blockchains, the central authority was the entity trusted to operate and control who and what can be published on the blockchain (Khatwani 2018; Lin & Liao 2017; Mendez 2018; Siba & Prakash 2016; Zheng et al. 2018). Given the ability to determine the access and rights permissions of new network participants (Lin & Liao 2017; Mohammed 2018; Yafimava 2019; Zheng et al. 2018), the central authority could utilise pre-established notions of an actor to determine how much of the network they should access (Ammeter et al. 2004; Rotter 1967). Following this provision of network access, network participants can conduct transactions within the private blockchain without needing to continually prove their legitimate intentions to the central authority (Ammeter et al. 2004). Leading to a reduction in the amount of time the central authority will spend verifying participant's actions within the network, the application of trust as a mechanism of accountability can lead to lower monitoring and surveillance costs (Bromiley & Cummings 1992; Calnan & Rowe 2008) for the firm. Utilising a central authority to ensure that only trusted parties can participate in transactions, private blockchains demonstrate the need for, and use of, trust as a mechanism to achieve accountability.

In addition to employing trust as a mechanism for accountability, private blockchains also used transparency within the network to assist the central authority in holding users responsible for their actions. Ensuring all users who access the network are known to the central authority, private blockchains use access and rights permissions to provide the central authority with visibility over all network activity (Lin & Liao 2017; Mohammed 2018; Yafimava 2019; Zheng et al. 2018). Whilst this permissioned nature of private blockchains could be used as a means to surveil participant activity (Bernstein 2017; Fox 2007), this 'transparency' produced in private blockchains cannot be deemed

fully transparent as the system itself cannot be separated from the social and political drivers that created them (Roberts 2009; McKernan 2007; Power 2004; Robson 1992).

Thus, whilst being an effective tool in encouraging actors to become more engaged and motivated to meet expectations (Ammeter et al. 2004; Calnan & Rowe 2008), the transparency used within private blockchains to facilitate accountability is inhibited by one actor that can override and delete transactions on the blockchain, and essentially the power to generate their own version of reality. Corroborating the work of Roberts (2009), this paper finds that transparency does not necessarily lead to greater accountability, particularly in instances where control is concentrated into one central entity.

Consortium blockchains, like private blockchains, also use trust and transparency as mechanisms of accountability. However, unlike in private blockchains, consortium blockchains offer network participants the choice in who their trust will be placed in. With options ranging from groups of companies to auditors (Asolo 2018b; Khatwani 2018; Yafimava 2019; Zheng et al. 2018), the trust used to facilitate accountability in consortium blockchains will differ from network to network. Regardless of which governing body is given the responsibility to hold network participants accountable for their actions, they will be able to govern the network with the notion that the network participants will be able to meet expectations (Ammeter et al. 2004; Rotter 1967). As consortium blockchains are permissioned networks in which only selected nodes can participate in the network, the governing body can reasonably trust that the members within the network do not need to continually prove that they have legitimate intentions for engaging with the network (Ammeter et al. 2004). However, governing bodies of consortium blockchains must be wary as people generally require additional mechanisms of accountability to be motivated to engage in cooperative behaviour (Calnan & Rowe 2008; De Cremer et al. 2001). As people may be engaging in consortium blockchains with their competitors, it would be "intrinsically immature" (O'Neill 2004, p.269) for one to assume network participants will act in another's best interests. Thus, consortium blockchains demonstrate that whilst trust is an important mechanism to facilitate accountability within this type of blockchain, trust alone cannot act as the sole mechanism of accountability.

To combat issues in employing trust as a mechanism for accountability, consortium blockchains also use transparency within the network to facilitate accountability. However, transparency in consortium blockchains, like trust, differs from network to network. Dependent upon the access and rights permissions given to a user, transparency within consortium blockchains can range from full visibility over all transactions within the network, to restricted visibility, where participants can only see transactions that they were involved in. Whilst enabling stakeholders to review their own and other's

actions, by making actions identifiable to other participants (De Cremer et al. 2001), and hold them accountable for them, transparency within consortium blockchains suffers from the same issue identified within private blockchains – an inability to separate the transparency within the network from the social and political drivers that created them (Roberts 2009; McKernan 2007; Power 2004; Robson 1992). Notwithstanding this, and utilising a mix of both trust and transparency to facilitate accountability, consortium blockchains illustrate the importance of using a combination of traditionally disparate mechanisms to reinforce accountability.

Public blockchains employ trust and transparency as mechanisms of accountability in ways which differ from traditional applications of the mechanisms. Through the implementation of a decentralised structure which enables anyone to access and participate in transactions within the network (Asolo 2018b; DragonChain 2019; Mohammed 2018; Shiff 2018; Zheng et al. 2018), public blockchains utilise robust consensus mechanisms and transaction transparency to facilitate accountability within the network. Differing from traditional systems, where trust as a mechanism of accountability emerges from principals being able to utilise pre-established notions of an actor to determine their ability to meet expectations (Ammeter et al. 2004; Rotter 1967), public blockchains enable a system where trust is placed in the code (Jeacle & Carter 2011). Advancing Jeacle and Carter (2011), we explain how trust is increasingly placed in codes and algorithms beyond popular culture contexts. Moving trust away from single centralised entities to groups of decentralised computers (DragonChain 2019; Khatwani 2018; Nakamoto 2008), public blockchains reveal a systems-driven accountability that reduces the need for trust, but does not explicitly counter trust; rather, it is independent of it.

A public blockchain also uses a decentralised ledger to generate accountability. Ensuring all transactions that occur on the network are visible to all on the network (Shiff 2018; Zheng et al. 2018), a public blockchain utilises its ledger's transparency to provide users assurance that their transaction was performed correctly and successfully. This activates “self-control and self-observation” (Roberts 2009, p.962; Power 2007) from network participants. One of the consequences of pseudo-anonymous identities and immutable transactions (Hobson 2013; Thibodeau 2019; Dai et al. 2017; Fanning & Centers 2016; Kokina et al. 2017) is that the ledger in public blockchains compels actors to take responsibility for the transactions they undertake. Using trusted code, that is constructed via consensus mechanisms and the alignment of incentives to distribute immutable transactions to all in the network, public blockchains demonstrate new ways trust and transparency can be used to facilitate accountability.

The findings from this sub-section are summarised in Table 2 below.

***[Insert Table 2 here]***

## Conclusion

This study examined how accountability is constructed in the context of different types of blockchain systems. To increase knowledge on the accountability within these different types of blockchains, this paper asked: how do blockchain systems construct accountability? To answer this question, an exploratory field study was conducted which examined the insights of eighteen blockchain experts across three types – public, private and consortium – of blockchains over a ten-month period, and contributes to the accounting literature in three ways. First, we find that public blockchains do not require many traditionally vital components of accountability to possess accountability itself. Prior literature depicts accountability as a construct which necessitates a "relationship of responsibilities" (Mulgan 2000, p.87) between a principal and an agent (Lindberg 2009; Mulgan 2000) to ensure its establishment. Public blockchains, however, do not require the same, reducing the requirement for explanations and justifications for decisions as discussed in Lerner & Tetlock (1999) and Messner (2009).

Second, we demonstrate that a 'blockchain' is not a unitary construct, but can manifest and be reflected in a multiplicity of forms, two of whom possess softer characteristics of the distributed ledger technology than those mobilised in public blockchains. By doing so, we further contribute to the accounting literature by demonstrating the relative importance of the simultaneous consideration of multi-faceted forms of accountability, to fully capture accountability effects on practice technologies (such as blockchains).

Third, we highlight the usefulness of consensus mechanisms in constructing accountability and their inverse relationship with trust. Moving trust away from single centralised entities to groups of decentralised computers (DragonChain 2019; Khatwani 2018; Nakamoto 2008), blockchain systems demonstrate new ways in which trust, transparency and consensus can be used to facilitate accountability in practice.

There are several implications of this research for broader society. First, regulators will need to consider the accountability implications this technology will have on businesses and consumers as blockchain is a technology that is forecast to revolutionise business activity. Second, auditors will likely revisit their auditing of financial transactions and internal controls of companies that run private blockchains, are a part of consortium blockchains or utilise public blockchains to conduct transactions.

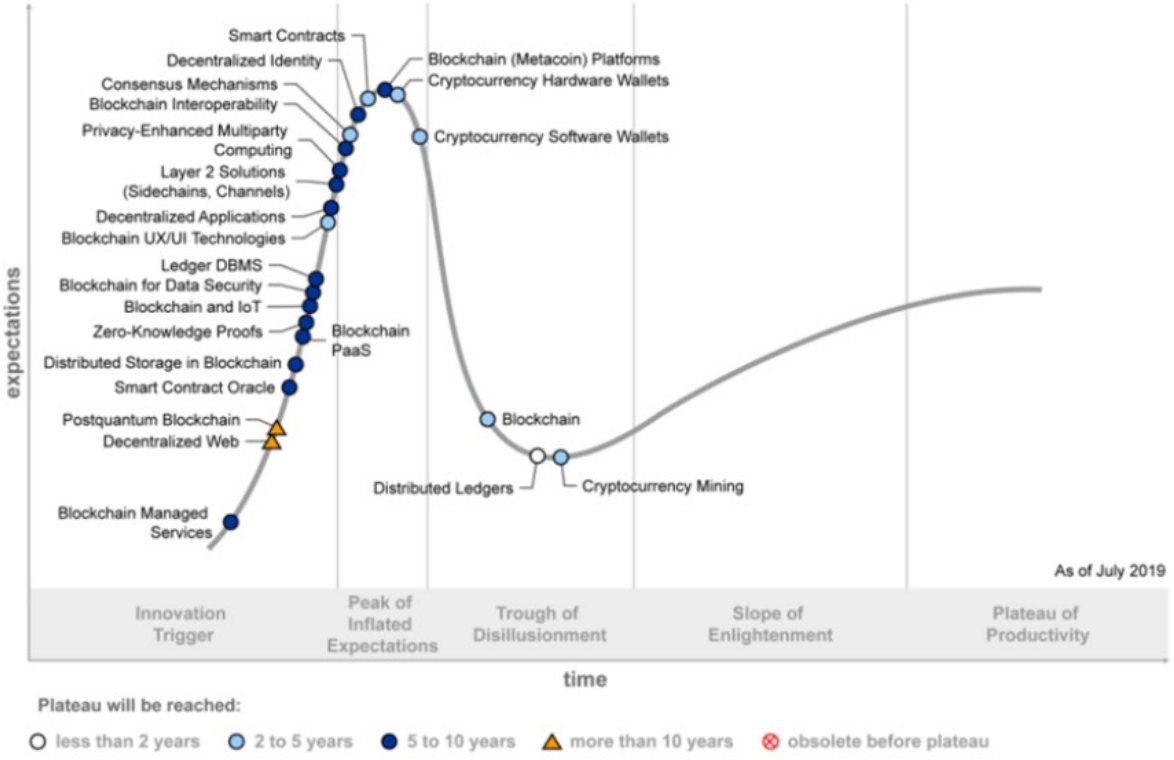
Third, or study has legal implications for the developers of blockchain systems. Though experts within public blockchains developers can publish their code under no liability licenses, how this relationship operates for developers of private and consortium blockchains remains less clear. Our findings hold the potential to guide this legal debate.

There are several limitations to this study, which do however offer new avenues for research. First, we sourced a range of experts in blockchains across the three types of blockchain systems investigated. Undoubtedly, the availability of even more blockchain experts, not just in Australia but globally, for interviews would have provided more insights and further strengthened the identification of patterns in the findings. While we believe sufficient information from those respondents was obtained to generate the findings, future research might consider collaborating with international institutions. In doing so, a broader range of views and perceptions around accountability and blockchain systems beyond Australia could be captured.

Second, had this paper organised a different selection of individuals or combination of individuals to interview, different views might have been expressed. This is a natural limitation associated with qualitative research and we mitigated this concern by capturing a broad cross-section of blockchain experts. Future research might conduct broad-based survey studies regarding the views and perceptions around accountability and blockchain systems, as blockchain practice increases and large-scale survey data can be captured from a wider range of practitioners.

Lastly, whilst this paper identifies public, private and consortium blockchains as being the three types of blockchains currently used in practice, this research is limited to the knowledge of the types of blockchain systems that might come into being in the future. In the same way, this work advances Cai (2018) and answers Hughes et al (2019)'s call to study blockchains beyond bitcoin, future research may advance the findings from this paper to identify new types of blockchains that may develop in the future.

**Figure 1: The Gartner Hype Cycle for Blockchain Technologies, 2019**




**Source: Gartner, Inc. 2019**

| Interviewee ID | Occupation and Organisation | Length of Time in Industry | Specialty Type of Blockchain | Length of Interview (hour: minutes: seconds) |
|---|---|---|---|---|
| Interviewee 1 | Solutions architect in medium-sized blockchain software company. | 20 years in IT | Public and Consortium | 0:54:52 |
| Interviewee 2 | Developer in contractor role. | 30 years in IT | Public | 1:10:58 |
| Interviewee 3 | Developer in small research and development lab. | 5 years in IT | Public | 1:11:45 |
| Interviewee 4 | Solutions architect and executive in small blockchain software firm. | 15 years in Engineering and 3 years in IT | Public | 1:00:48 |
| Interviewee 5 | Lawyer in medium-sized law firm. | 4 years in Law | Public and Private | 0:45:25 |
| Interviewee 6 | Blockchain auditor and product manager in blockchain services in a big four accounting firm. | 4 years in IT | Private and Consortium | 0:58:35 |
| Interviewee 7 | Product manager in medium-sized blockchain software company. | 5 years in IT | Public and Consortium | 0:55:18<br>0:53:26 |
| Interviewee 8 | Lawyer, business advisor and executive of small freelance law firm. | 8 years in Law | Public and Consortium | 0:48:11 |
| Interviewee 9 | Developer, executive and co-founder of small blockchain security firm. | 15 years in IT | Public | 1:06:24<br>1:18:33 |
| Interviewee 10 | Developer in contractor role. | 6 years in IT | Public | 0:35:41 |
| Interviewee 11 | Developer and co-founder of small blockchain development company. | 4 years in IT | Public and Private | 1:16:18 |
| Interviewee 12 | Solutions architect in small blockchain development company. | 3 years in IT | Public and Private | 0:46:57 |
| Interviewee 13 | Developer in medium-sized blockchain software company. | 12 years in Engineering and 7 years in IT | Public | 1:57:06 |
| Interviewee 14 | Solutions architect in blockchain services in a big four accounting firm. | 9 years in Engineering and 5 years in IT | Private | 1:20:30 |

| | | | | |
|---|---|---|---|---|
| Interviewee 15 | Developer in small blockchain software company. | 38 years in IT | Public | 1:02:54 |
| Interviewee 16 | Developer in small blockchain development company. | 21 years in Engineering and 8 years in IT | Public and Private | 1:19:07 |
| Interviewee 17 | Developer in small blockchain software company. | 28 years in IT | Public | 1:15:14 |
| Interviewee 18 | Head of blockchain technology at digital travel company. | 23 years in Engineering and 13 years in IT | Public, Private and Consortium | 0:42:24 |

**Table 1: Interview Details**

| | Public Blockchains | Private Blockchains | Consortium Blockchains |
|---|---|---|---|
| Trust in… **(Ammeter et al. 2004; O'Neill 2004; Hyndman & McConville 2018)** | Code/consensus algorithm | Central authority | Differs network to network: Governing body /code/consensus algorithm |
| Transparency of… **(Hood 2010; Roberts 2009)** | Transactions | Network participants | Differs network to network<br>Network participants and/or transactions |

**Table 2: Comparison of the Mechanisms of Accountability in Public, Private and Consortium Blockchains**

## References


Ahrens, T., 1996. 'Styles of accountability'. *Accounting, Organizations and Society*, 21(2-3), pp.139-173.

Ammeter, A.P., Douglas, C., Ferris, G.R. & Goka, H. 2004, 'A social relationship conceptualization of trust and accountability in organizations', *Human Resource Management Review,* vol. 14, no. 1, pp. 47-65.

Angus, C. 2018, *Blockchain technology,* Parliament of NSW, NSW.

Asolo, B. 2018a, *Consortium Blockchain Explained,* viewed 25th July 2019, <https://www.mycryptopedia.com/consortium-blockchain-explained/>.

Asolo, B. 2018b, *Private Blockchain Explained,* viewed 27th July 2019, <https://www.mycryptopedia.com/private-blockchain-explained/>.

Aste, T., Tasca, P. and Di Matteo, T., 2017. 'Blockchain technologies: The foreseeable impact on society and industry.' *Computer*, vol.50, no.9, pp.18-28.

ASX 2019a, *CHESS Replacement: Latest Updates,* viewed 25th July 2019, <https://www.asx.com.au/services/chess-replacement.htm>.

ASX 2019b, *Distributed Ledger Technology solution,* viewed 25th July 2019, <https://www.asx.com.au/services/technology-solution.htm>.

ASX, 2020, *Chess Replacement*, viewed 1st June 2020, <https://www.asx.com.au/services/chess-replacement.htm>

Batubara, F.R., Ubacht, J. and Janssen, M. (2019) Unravelling Transparency and Accountability in Blockchain, Proceedings of the 20th Annual International Conference on Digital Government Research, pp. 204-213, https://doi.org/10.1145/3325112.3325262

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,* vol. 19, no. 10, pp.1020-34.

Benston, G.J., 1982. 'Accounting and corporate accountability'. *Accounting, Organizations and Society*, vol. 7, no.2, pp.87-105.

Bernstein, E.S. 2017, 'Making transparency transparent: The evolution of observation in management theory', *Academy of Management Annals,* vol. 11, no. 1, pp. 217-66.

Bovens, M. 1998, *The quest for responsibility: Accountability and citizenship in complex organisations,* Cambridge university press, Cambridge University.

Bovens, M. 2005, 'Public Accountability', in E. Ferlie, L. Lynn Jr. & C. Pollitt(eds), *The Oxford Handbook of Public Management,* Oxford University Press Inc., United States, pp. 182-208.

Bovens, M., 2010. 'Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism.' *West European Politics*, vol. 33, no.5, pp.946-967.

Braun, V. & Clarke, V. 2006, 'Using thematic analysis in psychology', *Qualitative Research in Psychology,* vol. 3, no. 2, pp. 77-101.

Bromiley, P. & Cummings, L.L. 1992, *Transactions costs in organizations with trust,* Strategic Management Research Center, University of Minnesota Minneapolis, Minneapolis.

Butler, J. 2005, *Giving an account of oneself,* Fordham University Press, New York.

Butler, J. 2004, *Precarious life: The powers of violence and mourning,* Verso.

Butler, J. 2001, 'Giving an account of oneself', *Diacritics,* vol. 31, no. 4, pp. 22-40.

Cai, C.W. 2018, 'Disruption of financial intermediation by FinTech: a review on crowdfunding and blockchain', *Accounting & Finance,* vol. 58, no. 4, pp. 965-92.

Callon, M. 1984, 'Some elements of a sociology of translation: domestication of the scallops and the fishermen of St Brieuc Bay', *The Sociological Review,* vol. 32, no. 1, pp. 196-233.

Calnan, M. & Rowe, R. 2008, 'Trust, accountability and choice', *Health, Risk and Society,* vol. 10, no.3, pp. 201-206.

Carlozo, L. 2017, 'What is blockchain?', *Journal of Accountancy,* vol. 224, no. 1, pp. 29.

Cho, C.H., Phillips, J.R., Hageman, A.M. and Patten, D.M., 2009. 'Media richness, user trust, and perceptions of corporate social responsibility.' *Accounting, Auditing & Accountability Journal*, vol. 22, no.6, p.933.

Chua, W.F. 1995, *Experts, networks and inscriptions in the fabrication of accounting images: A story of the representation of three public hospitals,* vol. 20, no. 2, <www.sciencedirect.com.ezproxy.lib.uts.edu.au/science/article/pii/036136829595744H>.

Commonwealth of Australia, 2020, *the National Blockchain Roadmap: Progressing towards a blockchain-empowered future*, viewed 1st June 2020 <https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf>

Coyne, 2016, Australia to take global lead on blockchain standards, *IT News*, viewed on 1st June 2020, <https://www.itnews.com.au/news/australia-to-take-global-lead-on-blockchain-standards-437342>

Dai, J. & Vasarhelyi, M.A. 2017, 'Toward blockchain-based accounting and assurance', *Journal of Information Systems,* vol. 31, no. 3, pp. 5-21.

Dai, J., Wang, Y. & Vasarhelyi, M.A. 2017, 'Blockchain: an emerging solution for fraud prevention', *The CPA Journal,* vol. 87, no. 6, pp. 12-4.

Davies, A. 2019, *Public vs Private (Permissioned) Blockchain Comparison,* viewed 24th July 2019, <https://www.devteam.space/blog/public-vs-private-permissioned-blockchain-comparison/>.

De Cremer, D., Snyder, M. & Dewitte, S. 2001, ''The less I trust, the less I contribute (or not)?'The effects of trust, accountability and self-monitoring in social dilemmas', *European Journal of Social Psychology,* vol. 31, no. 1, pp. 93-107.

Deloitte 2017, *Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession,* Deloitte, viewed 17th August 2019, <https://www2.deloitte.com/za/en/pages/audit/articles/impact-of-blockchain-in-accounting.html>.

DeSantis, L. & Ugarriza, D.N. 2000, 'The concept of theme as used in qualitative nursing research', *Western Journal of Nursing Research,* vol. 22, no. 3, pp. 351-72.

DragonChain 2019, *What Different Types of Blockchains are There?* viewed 20th July 2019, <https://dragonchain.com/blog/differences-between-public-private-blockchains>.

Emanuel, E.J. & Emanuel, L.L. 1996, 'What is accountability in health care?', *Annals of Internal Medicine,* vol. 124, no. 2, pp. 229-39.

Eyers, 2018, Australia in driving seat as global blockchain standards take shape, *Australian Financial Review*, viewed 1st June 2020, <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,* vol. 27, no. 5, pp. 53-7.

Foley, S., Karlsen, J.R. & Putniņš, T.J. 2019, 'Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?', *The Review of Financial Studies,* vol. 32, no. 5, pp.1798-1853.

Fox, J. 2007, 'The uncertain relationship between transparency and accountability', *Development in Practice,* vol. 17, no. 4-5, pp. 663-71.

Ganne, E. 2019, 'Why blockchain could become the new container of international trade', *International Trade Forum,* vol. 1, no. 1, pp. 16-7.

Gartner, I. 2019, *Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact,* viewed 14th October 2019, <https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-from-transformational-impact>.

Hobson, D. 2013, 'What is Bitcoin?', *XRDS: Crossroads, The ACM Magazine for Students,* vol.20, pp.40-4.

Hood, C. 2010, 'Accountability and transparency: Siamese twins, matching parts, awkward couple?', *West European Politics,* vol. 33, no. 5, pp. 989-1009.

Hughes, A., Park, A., Kietzmann, J. and Archer-Brown, C., 2019. 'Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms.' *Business Horizons*, vol. 62, no. 3, pp.273-281.

Huh, S., Cho, S. & Kim, S. 2017, 'Managing IoT devices using blockchain platform', *2017 19th International Conference on Advanced Communication Technology (ICACT)* IEEE, Bongpyeong, South Korea, pp. 464-7.

Hyndman, N. & McConville, D. 2018, 'Trust and accountability in UK charities: Exploring the virtuous circle', *The British Accounting Review,* vol. 50, no. 2, pp. 227-37.
Jeacle, I. & Carter, C. 2011, 'In TripAdvisor we trust: Rankings, calculative regimes and abstract systems', *Accounting, Organizations and Society,* vol. 36, no. 4-5, pp. 293-309.
Keller, J.B. & Bichelmeyer, B.A. 2004, 'What happens when accountability meets technology integration', *TechTrends,* vol. 48, no. 3, pp. 17.
Khatwani, S. 2018, *Different Types Of Blockchains In The Market and Why We Need Them,* viewed 24th July 2019, <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,* vol. 14, no. 2, pp.91-100.
Koreto, R.J., 1997. 'When the bottom line is online.' *Journal of Accountancy*, vol. 183, no.3, p.63.
KPMG LLP 2019, *KPMG Technology Industry Innovation Survey: Blockchain,* viewed 15th October 2019, <https://assets.kpmg/content/dam/kpmg/us/pdf/2019/02/blockchain-tech-survey-2019-infographic.pdf>.
Kroon, M.B., Hart, P. & Van Kreveld, D. 1991, 'Managing group decision making processes: Individual versus collective accountability and groupthink', *International Journal of Conflict Management,* vol. 2, no. 2, pp. 91-115.
Kshetri, N., 2018. 'Blockchain's roles in meeting key supply chain management objectives' *International Journal of Information Management*, vol. 39, pp.80-89.
Kvale, S. 2008, *Doing interviews,* SAGE, London.
Latour, B. 1993, *We have never been modern,* Hemel Hempstead, Harvester Wheatsheaf.
Latour, B. 1987, *Science in action: How to follow scientists and engineers through society,* Harvard University Press, Cambridge, Mass.
Law, J. & Callon, M. 1992, 'The life and death of an aircraft: a network analysis of technical change', in W.E. Biker & J. Law(eds), *Shaping technology/building society: Studies in sociotechnical change,* MIT Press Cambridge, M.A.
Lerner, J.S. & Tetlock, P.E. 1999, 'Accounting for the effects of accountability.', *Psychological Bulletin,* vol. 125, no. 2, pp. 255.
Lewis, R.L., Brown, D.A. & Sutton, N.C. 2019, 'Control and empowerment as an organising paradox: implications for management control systems', *Accounting, Auditing & Accountability Journal,* vol. 32, no. 2, pp. 483-507.
Liamputtong, P. 2013, *Qualitative research methods,* 4th edn, Oxford University Press, South Melbourne, Vic.
Lin, I. & Liao, T. 2017, 'A Survey of Blockchain Security Issues and Challenges.', *IJ Network Security,* vol. 19, no. 5, pp. 653-9.
Lindberg, S.I. 2009, 'Accountability: the core concept and its subtypes', *Africa Power and Politics Programme Working Paper,* vol. 1.
Liu, M, Wu, K. & Xu, J.J. 2019, 'How will Blockchain Technology Impact Auditing and Accounting: Permissionless versus Permissioned Blockchain', *Current Issues in Auditing*, vol.13, no.2, p.19-29.
Lowe, A., Locke, J. and Lymer, A., 2012. 'The SEC's retail investor 2.0: Interactive data and the rise of calculative accountability.' *Critical Perspectives on Accounting*, vol. 23, no.3, pp.183-200.
Lundström, S. & Öhman, S. 2019, *Generating Value Through Blockchain Technology: The Case of Trade Finance,* KTH, School of Industrial Engineering and Management (ITM).
Maxwell, C. 2018, 'Acting for you, July 2018', *Governance Directions,* vol. 70, no. 6, pp. 361.
McBurney, P. 2018. 'The blockchain buzz', *Accountancy Futures,* pp. 20-1.
McKernan, J.F. 2007, 'Objectivity in accounting', *Accounting, Organizations and Society,* vol. 32, no. 1, pp. 155-180.
McKernan, J.F. & MacLullich, K.K. 2004, 'Accounting, love and justice', *Accounting, Auditing & Accountability Journal,* vol. 17, no. 3, pp. 327-60.

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>.

Messner, M. 2009, 'The limits of accountability', *Accounting, Organizations and Society,* vol. 34, no.8, pp. 918-38.

Mohammed, S. 2018, *Public vs. Private Blockchain,* viewed 27th July 2019, <https://hackernoon.com/public-vs-private-blockchain-4b4aa9326168>.

Mulgan, R. 2000, 'Comparing Accountability in the Public and Private Sectors', *Australian Journal of Public Administration,* vol. 59, no. 1, pp. 87-97.

Munro, A. 2019, *KPMG survey: Blockchain enthusiasm grew rapidly in 2018,* viewed 10th October 2019, <www.finder.com.au/kpmg-survey-blockchain-enthusiasm-grew-rapidly-in-2018>.

Nakamoto, S. 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Nott, G. 2018, *ASX pushes back roll-out of blockchain-based CHESS replacement,* viewed 25th July 2019, <https://www.cio.com.au/article/663423/exclusive-rob-james-resigns-qantas-cto/>.

O'Dair, M. 2016, *The networked record industry: how blockchain technology could transform the consumption and monetisation of recorded music,* NEMODE, viewed 12th August 2019, <alresearchonline.arts.ac.uk/14652/1/ODair-The-networked-record-industry-REPORT-1.pdf>.

O'Neill, O. 2002, *A question of trust: The BBC Reith Lectures 2002,* Cambridge University Press, United Kingdom.

O'Neill, O. 2004, 'Accountability, trust and informed consent in medical practice and research', *Clinical Medicine,* vol. 4, no. 3, pp. 269-76.

Pettersen, I.J. and Solstad, E., 2007. 'The role of accounting information in a reforming area: a study of higher education institutions.' *Financial Accountability & Management*, vol. 23, no.2, pp.133-154.

Pilkington, M. 2016, '11 Blockchain technology: principles and applications', *Research Handbook on Digital Transformations,* vol. 225.

Power, M. 2007, *Organized Uncertainty : Designing a World of Risk Management,* Oxford University Press, Oxford <http://ebookcentral.proquest.com/lib/uts/detail.action?docID=415614>.

Power, M. 2004, 'Counting, Control and Calculation: Reflections on Measuring and Management', *Human Relations,* vol. 57, no. 6, pp. 765-83.

PwC Global 2019, Blockchain is here. What's your next move?, *www.pwc.com/blockchainsurvey*

R3 2018, *Trade finance solution Voltron launches open platform on Corda blockchain,* viewed 27th July 2019, <https://www.r3.com/press-media/trade-finance-solution-voltron-launches-open-platform-on-corda-blockchain/>.

R3 2019, *Voltron Description,* viewed 27th July 2019, <https://marketplace.r3.com/solutions/voltron>.

Ribstein, L.E. 2006, 'Accountability and responsibility in corporate governance', *Notre Dame L.Rev.,* vol. 81, pp. 1431.

Roberts, J. 1991, 'The possibilities of accountability', *Accounting, Organizations and Society,* vol. 16, no. 4, pp. 355-68.

Roberts, J. 2009, *No one is perfect: The limits of transparency and an ethic for 'intelligent' accountability,* vol. 34, no. 8, <www.sciencedirect.com.ezproxy.lib.uts.edu.au/science/article/pii/S0361368209000452>.

Roberts, J. and Scapens, R., 1985. 'Accounting systems and systems of accountability—understanding accounting practices in their organisational contexts.' *Accounting, Organizations and Society*, vol.10, no.4, pp.443-456.

Robson, K., 1992. 'Accounting numbers as "inscription": Action at a distance and the development of accounting.' *Accounting, Organizations and Society*, vol.17, no.7, pp.685-708.

Rotter, J.B. 1980, 'Interpersonal trust, trustworthiness, and gullibility', *American Psychologist,* vol.35, no. 1, pp. 1.

Rotter, J.B. 1967, 'A new scale for the measurement of interpersonal trust 1', *Journal of Personality,* vol. 35, no. 4, pp. 651-65.

Rus, D., van Knippenberg, D. and Wisse, B., 2012. Leader power and self-serving behavior: The moderating role of accountability. *The Leadership Quarterly*, vol. *23*, no.1, pp.13-26.

Ryan, E. 2012, The Evolution of Accounting Software: Past, Present and Future. *The Journal of the Global Accounting Alliance,* viewed 12th July 2019, <http://www.gaaaccounting.com/the-evolution-of-accounting-software-past-present-and-future/>.

Schmitz, J., & Leoni, G. 2019. Accounting and auditing at the time of blockchain technology: a research agenda. *Australian Accounting Review*, vol. 29, no.2, pp. 331-342.

Schweiker, W. 1993, 'Accounting for ourselves: accounting practice and the discourse of ethics', *Accounting, Organizations and Society,* vol. 18, no. 2-3, pp. 231-52.

Scott, S.V. & Orlikowski, W.J. 2012, 'Reconfiguring relations of accountability: Materialization of social media in the travel sector', *Accounting, Organizations and Society,* vol.37, no.1, pp.26-40.

Shiff, L. 2018, *Public vs Private Blockchains: What's the Difference?* viewed 24th July 2019, <https://www.bmc.com/blogs/public-vs-private-blockchain/>.

Shivang 2019, *Difference Between Centralized, Decentralized & Distributed Systems Oversimplified,* viewed 28th July 2019, <https://www.8bitmen.com/difference-between-centralized-decentralized-distributed-systems-explained/>.

Shubber, K. 2015, 'The regulators', *New Scientist,* vol. 225, no. 3006, pp. 1.

Siba, T.K. & Prakash, A. 2016, 'Block-Chain: An Evolving Technology', *Global Journal of Enterprise Information System,* vol. 8, no. 4, pp. 29-35.

Sinclair, A. 1995, 'The chameleon of accountability: forms and discourses', *Accounting, Organizations and Society,* vol. 20, no. 2-3, pp. 219-37.

Swan, M. 2016, 'Blockchain Temporality: Smart Contract Time Specifiability with Blocktime', *Research,* Springer International Publishing, Cham, pp. 184-96.

Swift, T. 2001, 'Trust, reputation and corporate accountability to stakeholders', *Business Ethics: A European Review,* vol. 10, no. 1, pp. 16-26.

Tapscott, D. & Tapscott, A. 2016, 'The impact of the blockchain goes beyond financial services', *Harvard Business Review,* vol. 10, pp. 2-5.

Thibodeau, M. 2019, *3 Types of Blockchain Explained,* viewed 24th July 2019, <https://hedgetrade.com/3-types-of-blockchain-explained/>.

Thompson, 2019, Australia has launched a blockchain strategy: What can other countries learn?, *Coin Rivet*, viewed 1st June 2020, <https://coinrivet.com/australia-has-launched-a-blockchain-strategy-what-can-other-countries-learn/>

Vaismoradi, M., Turunen, H. & Bondas, T. 2013, 'Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study', *Nursing & Health Sciences,* vol. 15, no. 3, pp.398-405.

Voltron 2019, *Voltron,* viewed 27th July 2019, <https://www.voltron.trade/>.

Wass, S. 2019, *Voltron blockchain consortium to create independent company ahead of commercial launch,* viewed 27th July 2019, <https://www.gtreview.com/news/fintech/voltron-blockchain-consortium-to-create-independent-company-ahead-of-commercial-launch/>.

Westerman, G., Bonnet, D. & McAfee, A. 2014, *Leading digital: Turning technology into business transformation,* Harvard Business Press, United States.

Yafimava, D. 2019, *What are Consortium Blockchains, and What Purpose do They Serve?,* viewed 26th July 2019, <https://openledger.info/insights/consortium-blockchains/#Shared_Platforms>.

Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. 2018, 'Blockchain challenges and opportunities: A survey', *International Journal of Web and Grid Services,* vol. 14, no. 4, pp. 352-75.