Understanding Accountability

In Blockchain Systems

BRIDGET TYMA*

RINA DHILLON**

PRABHU SIVABALAN

BERNHARD WIEDER

ACCOUNTING DISCIPLINE GROUP

UTS BUSINESS SCHOOL

UNIVERSITY OF TECHNOLOGY SYDNEY

November 2021

* Author currently holds a position as a Digital Trust 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 for 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.

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 does not require a principal-agent relation and can still manifest in *less* pure applications of blockchain technology across a wide range of stakeholders, 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 and there exists an inverse relation between trust and consensus building through transparency as we progress from public to private blockchains. Overall, we 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 different blockchain systems reshape our understanding of traditional accounting and accountability practices. We question the very need for a principal-agent relation to facilitate accountability, and offer an additional perspective to how trust and transparency operate as key mechanisms of accountability.

Keywords: Accountability; Blockchain; Transparency; Trust

Paper type: Research paper

Introduction

Background

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, 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) – the blockchain.

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 (Bonsón and Bednárová 2019; Hughes et al. 2019; Schmitz & Leoni 2019). Both the accounting and technology literatures have identified opportunities and challenges with blockchain systems (Deloitte 2017; Dai & Vasarhelyi 2017; Fanning & Centers 2016) and popular practitioner outlets cite the role of blockchain systems as increasing the visibility and accountability of actors – through its distribution, ubiquitous availability, and availability of multiple records of proof (Deloitte 2017; PwC Global 2019). In summary, accountability is touted as one of the major benefits of blockchain, yet we know little about whether and how accountability is constructed in blockchains.

Briefly, a burgeoning interest in blockchain has led to a recent 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). These focus on public blockchains such as Bitcoin (Cai 2018; Hughes et al. 2019) and the application potential of blockchain systems 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). These studies consider the workability and operationalisation of public blockchain systems, but largely lack an assessment of the accountability that blockchain systems actually offer in practice (Schmitz & Leoni 2019). Examining accountability 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. Given the above, the objective of this study is to examine how blockchain systems construct accountability.

Our study is motivated in two ways. First we note a general practitioner call for better understanding the role of accountability in blockchain systems (McBurney 2018) in corporate society, which is currently in a 'trough of disillusionment' per practitioner reports highlighting the need to differentiate between the hype and reality associated to blockchain (Gartner Inc. 2019). Senior executives appreciate but do not fully understand its potential (Bonson and Bendarova 2019; KPMG LLP 2019).

Our second motivation is to theoretically incorporate blockchain systems beyond public blockchains (such as bitcoin, per Cai (2018) and Hughes et al. (2019)) into the accounting literature and understand its' consequent accountability implications. These have been discussed in the IT literatures (Asolo 2018b; DragonChain 2019; Khatwani 2018; Yafimava 2019; Zheng et al. 2018) and occasionally, the broader management literature (Tapscott and Tapscott 2016) individually (Bonsón and Bednárová 2019). However, the theorising and explanation of all three blockchain systems (public, private and consortium) as it relates to accountability remains elusive.

The above two motivations lead to our central research question underpinning the abovementioned motivations: *how do different blockchain systems construct accountability?*

Answering this question requires an exploratory examination of both the elements and mechanisms which form accountability (Bovens 2005; Roberts 1991; O'Neill 2004; Hyndman & McConville 2018; Roberts 2009) for the three dominant blockchain systems mentioned above. Over a ten month period, we identified and interviewed 18 blockchain experts who were early adopters or experts in industry that are driving their use, and sought their perspectives regarding our research question.

In seeking to answer the above research question, we find that public blockchains eliminate the need for principal-agent separation, indeed the very relationship itself (Lindberg 2009; Mulgan 2000) and are possibly impacted by a range of wider stakeholders (Allen and Berg 2020; Allen et al. 2020). We therefore do not need many traditional components of accountability to explain and justify decisions (Lerner and Tetlock 1999; Messner 2009) in certain blockchain systems. Second, we build on Cai et al. (2018) and Hughes et al. (2019) in explaining how different types of blockchain systems employ different forms of blended accountability elements, and offer an alternative view to the more dichotomous explanations advanced by Roberts (1991) and Bovens (2005). Third, we explain how trust and transparency, as two mechanisms of accountability, are mobilised differently across the three blockchain types, highlighting an inverse relationship between the prevalence of trust and the generation of transparency through consensus building, thereby advancing how we think about trust and transparency in relation to blockchains (furthering Coyne and McMickle 2017). While we will elaborate on these findings and contributions in the discussion section, their link to our motivations and underlying research question are succinctly summarised in Table 1 below.

[Insert Table 1 here]

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, highlighting avenues for future research.

Accountability and Blockchain

Background to Blockchain Research in the Accounting Literature

The increased 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). 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).

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). Indeed, the relevance of blockchain to accounting has been called into question (Coyne and McMickle 2017) – we argue that this question is a complex one, requiring the study of different types of blockchains in order to better understand how accountability impacts its design and use.

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. Of course, this notion of accountability has been contested in recent times, through the acknowledgement of a wider range of stakeholders impacting the working of governance in blockchain transactions (Woodside et al. 2017; Allen 2019). How they relate to accountability more broadly across multiple types of blockchain systems remain less explored.

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" (Roberts 1991, p.74).

[1] This paper' references to an 'actor' refers to a human being only, not as espoused in Actor Network Theory (Latour 1987, 1993)

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 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. Indeed, how these arguments work across a broader range of stakeholders in novel arrangements such as blockchains, remain less explored (Allen and Berg (2020)).

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

[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.

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 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;). 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). Bitcoin is decentralised – it removes the need for a central authority and enables direct transactions with addresses anywhere in the globe (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 remains open and transparent for all (Shiff 2018; Zheng et al. 2018), ensuring the network is rarely manipulated by an actor (Angus 2018; Asolo 2018b; Zheng et al. 2018). However, whilst users do not provide identifiable information to engage with Bitcoin, they are not completely anonymous, but rather are pseudo-anonymous. Users could be identified if they inadvertently link themselves to their wallet address as a user (Hobson 2013).

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 controlling what the blockchain publishes (Khatwani 2018; Lin & Liao 2017; Mendez 2018; Siba & Prakash 2016; Zheng et al. 2018). Being centralised, private blockchains provide users a more transparent database of transactions within their organisation (Davies 2019; Khatwani 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). Given this, questions around the legitimacy of private blockchains continue to rise (Khatwani 2018; Thibodeau 2019).

One prominent private blockchain example is the Australian Stock Exchange (ASX) distributed ledger technology (DLT) system. It replaces the existing Clearing House Electronic Subregister System (CHESS) used to record share related transactions (ASX 2019a). DLT is designed to operate a private network where only permissioned participants view the database (Angus 2018; ASX 2019b; Maxwell 2018). This addresses privacy concerns whilst effectively distributing a single source of truth to all requiring it (ASX 2019a; Nott 2018).

The ASX DLT solution offers 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), these features relate to private blockchains. However, the ASX DLT solution is limited by a single point of failure (Khatwani 2018; Thibodeau 2019). If the system were to experience a technical failure post-implementation, all market transactions cease and only resume when 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; Zheng et al. 2018). Also known as a federated or hybrid blockchain, they combine elements of both public and private blockchains (Asolo 2018a; Mendez 2018; Tapscott and Tapscott 2016; Thibodeau 2019; Yafimava 2019). Like private blockchains, consortium blockchains preserve some 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 companies with the opportunity to engage in a network that doesn't necessitate trust in a single central authority (Asolo 2018a; DragonChain 2019; Ganne 2019; Yafimava 2019; Zheng et al. 2018). As sub-categories of interactions can be separate from others within the same system, consortium blockchains may possibly have implications for the public sector (Ølnes 2017).

Voltron is one example of a consortium blockchain. Developed as a trade finance blockchain, Voltron improves documentary trade by digitising the letter of credit process (Ganne 2019; Lundström & Öhman 2019; R3 2019; R3 2018; Voltron 2019). Founded by eight banks, this consortium saw process efficiencies a consortium blockchain for their operations (Lundström & Öhman 2019; R3 2018; R3 2019; Wass 2019). Ensuring that all the parties in the letter of credit process can agree upon a single version of trade documents, Voltron creates an open, yet secure network for competing organisations trade with each other (Voltron 2019).

A visual summary of the three different types of blockchain systems from ICOinRating.com (2018) is provided below:

[Insert Figure 1 here]

Blockchains and the Construction of Accountability

Having identified three blockchain types, we explore how accountability relates to their operationalisation. Within IT literature, some research exists on decentralised autonomous organisations[3] (DAOs) (Beck et al. 2018). Examining decision rights, accountability, and incentives

[3] A DAO is a company which is comprised of blockchain technology, utilising smart contracts (Dai & Vasarhelyi 2017).

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. Allen and Berg (2020) take a broader stakeholder view to blockchain governance, clarifying governance as processes through which users posture their bargaining power in the network at the construction stage and permissions/operation stages of blockchain practice, beyond principals (owners) and agents (managers/central authorities/overseers). Allen and Berg (2020) explain that even regulators, auditors and developers and not merely users are implicated in the negotiation for stakeholder influence in blockchain systems. Similar arguments are put forward by Woodside et al. (2017) in citing this broadening of key stakeholders as a deliberate strategy organically driving the growth of blockchains. Chen (2018) similarly associates this broader stakeholder influence, identifying public blockchains as opening up (democratizing) innovation beyond owners with wealth and traditional capital more generally. However, the implications for these for how accountability manifests different across the three major types of blockchains remain unresolved (Allen et al. 2020). Finally, Allen (2019) offers an institutional view to the development and management of blockchains, highlighting the role of broader markets and hierarchies in affecting how blockchains operate. Multiple, different entities therefore can impact the workings of blockchain. However, studies empirically marshalling evidence (quantitative or qualitative) to explore accountability, trust and transparency, remain sparse.

With the existence of a range of blockchain applications across different blockchain types in society and the expected influx of blockchain applications in the 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 our 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; Ølnes 2017), revealing the technical expertise and knowledge existing to better understand how accountability is constructed in this context.

Second, the Australian Securities Exchange (ASX) is the first stock exchange in the world to invest financial processes critical to the orderly functioning of the Australian financial market, with a blockchain-based platform (ASX 2020). Australia is at the forefront of implementing blockchain technologies within key sectors of their economy, with the Australian government providing grants and incentives to study potential use cases of blockchain technology for the public sector (Ølnes 2017) and industry (Coyne 2016; Coyne and McMickle 2017).

Lastly, Australia is recognised as a global leader in blockchain technology, 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 necessary to collect and analyse data from a range of individuals working across a range of organisations. As Table 2 illustrates, a total of twenty interviews were conducted with eighteen blockchain experts from various industries in Australia[4]. 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. 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[5] as the interviewees were based in another Australian city.

[Insert Table 2 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

[4] Our respondents collectively consulted across a wide range of sectors per the Global Industry Classification Standard categories, including IT, energy, materials, industrials, consumer discretionary and staples, health care, financial services, communication services and utilities. We note less focus on the real estate sector. Two interviewees were interviewed a second time in order to triangulate their views with other respondents.
[5] Zoom is a video conference call software. See https://zoom.us/ for more information.

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 a greater understanding of important concepts (Liamputtong 2013). At 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. Additional, generally worded clarification questions then flowed on occasion, from interviewee lines of thought as recommended in Kvale (2008). The full list of semi-structured interview questions are provided in Appendix A.

Each interviewee offered verbal and written consent to record their interview. The researchers used a mobile device in each interview to record audio, whilst also taking hand-written notes of key thoughts and insights offered by interviewees. Following the 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[6]. These transcripts were finally 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 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 our findings.

[6] 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.

Findings

We discuss our findings as they relate to public, private and consortium blockchains. Within each sub-section, we offer four areas of focus – an initial explanation of the definitional aspect of the blockchain system (*what are the attributes of it?*), the manner of its operation (*how does it work?*), the accountability of participants (*who is accountable?*) and an explanation of how errors are absorbed (*what if something goes wrong*), a further signal of accountability.

Public Blockchains

What are its' attributes?

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.

> 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."

How does it work?

A public blockchains' 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[7] 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 accountability, trust and transparency

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."

[7] The name of the license has been changed for anonymity purposes.

> 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…"

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."

Explaining that public blockchain technology is open source and published under no liability licenses[8], 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 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 there are instances where coin exchanges held an individual's private key, responses revealed that ultimate responsibility still lay with the individual.

[8] For example, on the Ethereum website, there is a limitation of no liability. https://ethereum.org/en/terms-of-use/

> 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.”

In summary, most respondents with public blockchain expertise explained that public blockchains facilitate open-ness and a high level of transparency. Notwithstanding their high degree of user anonymity, individuals were identified by a strong majority of respondents as being wholly responsible for their personal security and identity in the event breaches occurred, and that accountability cannot be abdicated to the public blockchain. To this extent, accountability was individualised and substantively abdicated from the system itself. Trust between participants neither high nor low. It was simply considered less important, as the extent of transparency across public blockchain platforms was high.

Private Blockchains

What are its’ attributes?

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, generally 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… 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… you've just got a little bit more control theoretically over what your participants can and can't do."

How does it work?

Control within a private blockchain is essentially centralised by a single entity. 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."

As the notary decides which nodes participate in the network and transactions to accept, the notary becomes the entity in private blockchains which holds users accountable.

Using a central authority to assure accountability, private blockchains thereby lack anonymity. Unlike public blockchains, the notary is aware of the underlying identity of every node participant. This lack of anonymity allows for issues to be assessed more directly.:

> Interviewee 6: "Typically in permissioned (private) 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."

Explaining accountability, trust and transparency

The presence of an all-controlling central authority notary entity alters the dynamic between accountability, trust and transparency. First, while much accountability lies with the notary, respondents argued that developers (Interviewee 6) and regulators (Interviewee 5) of the chain might bear responsibility in the event of a breach/failure.

> 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."

Regulators can also 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, experts offered new insights into private blockchains. Like in public blockchains, where an individual form of accountability was identified, the experts of private blockchains identified individuals to be occasionally responsible if failure occurred:

> 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, the need for accountability from accounting practices such as audits were argued as necessary until blockchain technology became more commonplace and trusted. This was not only the blockchain technology, but systems driving their operation such as in private blockchains.

> 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, … 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, who similarly differentiated private from public blockchains:

> 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)."

In summary, the majority of our respondent experts indicated that accountability in private blockchains were not limited to users alone, but especially directed to the notary (central authority), as well as developers and regulators in the instance of major failure. This was driven by its centralised structure and trust in one specific entity to drive its operation. The level of transparency in private blockchains was thus identified by respondents as being lower owing to its closed nature, and the lower presence of trust in this closed system drove a greater role for accounting intervention (auditing) to verify and lend accountability to the operation of private blockchains.

Consortium Blockchains

What are its' attributes?

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."

How does it work?

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 accountability, trust and transparency

In a consortium blockchain, users are responsible to one another (who they transact with). Therefore 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."

To this extent, there is some similarity between consortium and public blockchains. However, respondents indicated that an appointed governing body, referred to as the network overseer, assists users in determining who is accountable. This has some relation to private blockchains, though lacking the total control a central authority possesses in private blockchains.

> 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 accountability rests on some level in the work of auditors in instances of failure, respondents identified founding consortium members as responsible in the design and operation of consortium blockchains. This was primarily due to the distributed control that members had in defining/limiting data that is accessible to each party on the blockchain from the network's inception, alongside with dispensing voting rights.

To gauge whether these entities are responsible in any other instances in consortium blockchains, respondents 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."

In summary, a majority of our respondents indicated a set of accountability factors that reveal consortium blockchains to possess elements of public and private blockchains, and this has consequences for a transparency and trust that reflects a compromise between both. Most of our respondents explained that transacting (consortium members/users) and governing entities (consortium members/developers) should be held accountable to some extent in consortium blockchains. While transparency can be high, it is arguably not as complete or as autonomously furnished by the system in the way experienced in a public blockchain. Finally, most respondents conceded that trust was required between users and not without relevance such as that observed in public blockchains.

The next section provides a discussion of the above findings, explaining how respondent feedback regarding the three blockchain systems plausibly advances our understanding of the workings between accountability, trust and transparency.

Discussion

Using the findings gathered, we broadly discuss how accountability elements and forms manifest in blockchain systems and introduce our first two contributions. We then proceed to explain the role of transparency and trust as two mechanisms shaping accountability in blockchain systems, subsequently introducing our third contribution.

Accountability in Blockchain Systems

In private blockchains, the central authority holds 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. This relates to a hierarchical form of accountability described by Roberts (1991), prevalent in most traditional settings.

In addition to employing hierarchical accountability, private blockchains facilitate the individual accountability form (Bovens 2005). Individual participants are given the responsibility to input and approve the data within the blockchain and 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, 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 is simply one's own conscience driving blockchain behaviours in a morally acceptable way (Bovens 2005).

Consortium blockchains, like private blockchains, rely on the principal-agent relationship (Lindberg 2009; Mulgan 2000) to assure accountability. However, unlike private blockchains, the "principal" employed in consortium blockchains are a collection of entities – typically a group of companies rather than a single entity (Asolo 2018a; DragonChain 2019; Khatwani 2018; Yafimava 2019; Zheng et al. 2018). This means that accountability within consortium blockchains differ from network to network. Principals within a consortium blockchain demand network participants to account for their actions and could impose sanctions (Lindberg 2009; Mulgan 2000) to different degrees. 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 and is more concerned with the needs of all users, adopting a wider stakeholder view (Allen and Berg 2020) 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. Overall, we claim the following accountability literature contribution relating to public blockchains.

> *Key Contribution 1:*
>
> 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, the first key contribution of this study is explaining how elements traditionally considered vital to accountability are not required to construct accountability in public blockchains. We offer a conceptual explanation for how accountability might operate in a

novel manner relative to traditional notions of accountability, but in ways that are conceptually different from the explanations of Roberts (2009) and Messner (2009).

Additionally, while 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. All participants have the same privileges (Fanning & Centers 2016; Kokina et al. 2017; Nakamoto 2008) and no actor is required to trust any other in the network.

In addition to the types of accountability previously discussed above as relating to public and private blockchain systems, 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). Furthermore, 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 can also hold individual contributors accountable (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). Overall, we note that the corporate and socialising forms of accountability generated by consortium blockchains play a more prominent role in providing accountability in consortium blockchains than other forms.

Key Contribution 2:

Prior studies have broadly offered dichotomous classifications of accountability as hierarchical/socialising (Roberts 1991) or corporate/individual (Bovens 2005). We find these to be somewhat incomplete in relation to the three blockchain systems. We advance Cai et al. (2018) and Hughes et al. (2019) in explaining how accountability relates to public, private and consortium blockchains, and further highlight the need for blended and varying descriptions of accountability in newer system arrangements, such as those posed by blockchain systems. Multi-faceted forms of accountability operate simultaneously, and we observe that the relative importance of individual accountability changes across the three different types of blockchain systems.

Trust, Transparency and Accountability in Blockchain Systems

Trust and transparency facilitate accountability within blockchain systems (Schmitz & Leoni 2019). Our findings reveal that in private blockchains, trust as a mechanism of accountability leads to lower monitoring and surveillance costs (Bromiley & Cummings 1992; Calnan & Rowe 2008). Utilising a central authority to ensure that only trusted parties can participate in transactions, private blockchains reveal the need for, and use of, trust as a mechanism to achieve accountability.

Private blockchains also use transparency within the network to assist the central authority in holding users responsible. However, whilst being an effective tool for encouraging actors to become more engaged and practice aligned behaviours (Ammeter et al. 2004; Calnan & Rowe 2008), transparency within private blockchains can be inhibited by the central authority overriding and deleting transactions on the blockchain, essentially generating their own version of reality. Corroborating the work of Roberts (2009), we find that transparency does not necessarily lead to greater accountability, particularly in instances where control is concentrated into one central entity.

Within consortium blockchains the trust used to facilitate accountability differs from network to network, with options ranging from groups of companies to auditors (Asolo 2018b; Khatwani 2018; Yafimava 2019; Zheng et al. 2018). Regardless of the governing body given the responsibility to hold network participants accountable for their actions, this body will be able to govern the permissioned network trusting that network participants have the capacity to meet expectations (Ammeter et al. 2004; Rotter 1967). 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 especially when their competitors are involved in the blockchain (Calnan & Rowe 2008; De Cremer et al. 2001; O'Neill 2004, p.269). Consortium blockchains therefore signal that trust is a preferable but insufficient mechanism for ensuring accountability.

To address this, consortium blockchains use transparency within the network to increase accountability. Although, 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, a mix of both trust and transparency collectively raises accountability to a workable level, allowing for consortium blockchains to function in practice.

Public blockchains, like private and consortium blockchains employ trust and transparency as mechanisms of accountability. However, within this type of blockchain these two constructs are used in ways which differs from the other two types of blockchain systems. In traditional systems, trust as a mechanism of accountability emerges from principals utilising pre-established notions of an actor to determine their ability to meet expectations (Ammeter et al. 2004; Rotter 1967). However, public blockchains enable a system where trust is placed in the code (Jeacle & Carter 2011). Building on Jeacle and Carter (2011), we note that trust is instead 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 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. Facilitated by the pseudo-anonymous identities and immutable transactions (Hobson 2013; Thibodeau 2019; Dai et al. 2017; Fanning & Centers 2016; Kokina et al. 2017) generated in public blockchains, actors are compelled to take responsibility for the transactions they undertake, independent of their identity being verified.

Key Contribution 3

> From the above discussions, we advance accountability theory by demonstrating the inverse relationship between trust and the presence of transaction transparency via consensus building mechanisms, advancing Coyne and McMickle (2017). In public blockchains, transparency is high because of the immutability of the code governing transactions, and trust is not or much less required. Private and consortium blockchains, however, operate in reverse. With lower transaction transparency within the network, greater reliance is placed in trusting the blockchain's accepted network participants and the behaviours of its single network administrator.

In closing, we again highlight Table 1 as offering a visual explanatory summary of the link between our motivation, research questions and three contributions.

Conclusion

We examine 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 revealing that public blockchains do not require many of the traditionally vital components of accountability, and that the dichotomous explanation of accountability (Bovens 2005; Roberts 1991) must be enhanced with more blended types of accountability that simultaneously manifest to ensure the working of such new technology settings (public, private, consortium blockchains). Furthermore, 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 capture new ways in which trust, transparency and consensus can be used to facilitate accountability in practice. Crucially, we explain how the different types of blockchain systems tackle the broad range of responsibilities they are expected to uphold across a wide range of stakeholders, beyond the traditional principal-agent relation dominantly discussed in earlier accountability studies.

There are several implications of this research for broader society. 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. Management of corporates will benefit from the managerial implications posed by our study, raising questions regarding the strategic value of different blockchain systems in aiding their transaction management with external parties.

Respondent feedback from our study also offer accounting managers further insights to consider the strategic disclosure of their corporate practices using financial and non-financial reporting, and consider trust and transparency and tools through which the rationale for decision making in their organisations might be better communicated. The release of ad hoc reporting systems, or more formal reporting documents are two examples of how these might be effected by accounting managers.

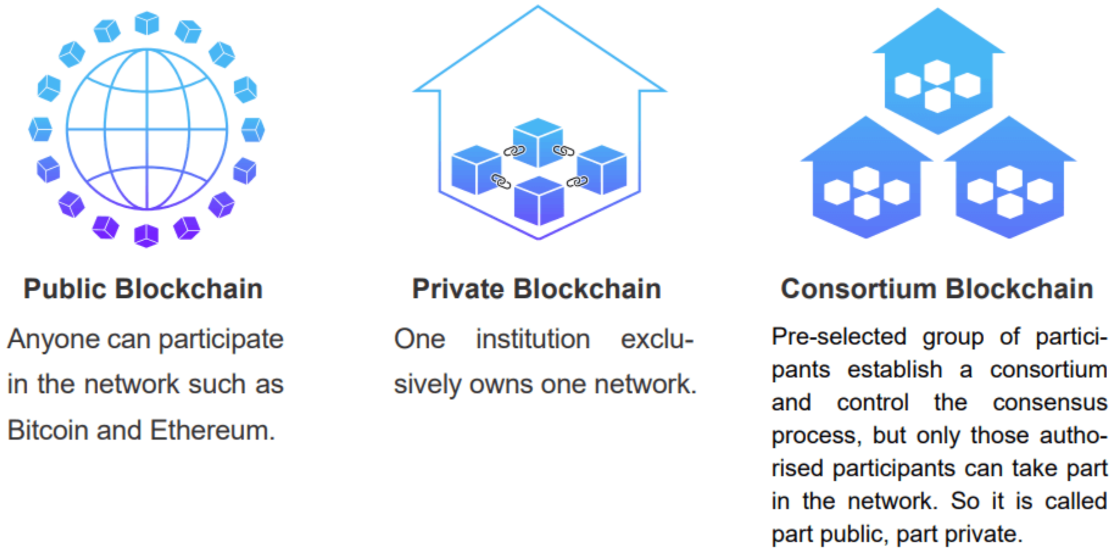
Auditors should also revisit their auditing of financial transactions and internal controls of companies that run private blockchains, especially for consortium and private blockchains. More specifically, in more fluid blockchain systems such as consortium blockchains, the management of corporate agency risk requires a careful consideration of how transparency and trust must be operationalised to facilitate positive outcomes. Finally, our 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 offer new avenues for research. Firstly, 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.

Secondly, 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 that 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: A Visualisation of the Different Types of Blockchains



Source: ICOinRating.com 2018

Table 1: Linearity of Research Question, Motivations, Findings and their Related Contributions

	Research Question: *How do blockchain systems construct accountability?*	
	Practitioner Motivation	Theoretical Motivation
	Practitioner calls for a better understanding regarding the role of accountability in blockchain systems (McBurney 2018) in corporate society.	Incorporate the full spectrum of blockchain systems beyond public blockchains into the accounting literature and understand their implications for accountability.
	Key Findings	Related Contributions
1	Public blockchains eliminate the need for the separation of a principal and agent, they do not require a "relationship of responsibilities" (Mulgan, 2000, p.87).	Using 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).
2	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.	Advance Cai et al. (2018) and Hughes et al. (2019) in explaining how accountability relates to public, private and consortium blockchains, highlighting that dichotomous classifications of accountability as either hierarchical or socialising, per Roberts (1991) or corporate or individual, per Bovens (2005), are somewhat incomplete.
3	Public blockchains place trust in the code and consensus algorithm (Jeacle and Carter 2011) and offers high transparency as everyone sees all transactions on the network. Private blockchains place trust in a central authority, that has control over transaction visibility (lower transparency) and cannot be separated from the social and political drivers that construct them (Roberts 2009; McKernan 2007; Power 2004; Robson 1992). Consortium blockchains reveal trust and transparency elements that are an amalgam of public and private, and manifest differently from network to network.	Advance accountability theory by demonstrating the inverse relationship between the need for trust and the presence of transparency through consensus building mechanisms, advancing Coyne and McMickle (2017). In public blockchains, transparency is high because of the immutability of the code governing transactions. This in turn deems the need for trust amongst network participants low and the anonymity of participants is accepted. Private and consortium blockchains, however, operate on the reverse of this. With lower transaction transparency within the network, greater reliance is placed in trusting the blockchain's accepted network participants.

Table 2: Interviewee Details

Interviewee ID	Occupation and Organisation	Time in Industry	Specialty Type of Blockchain	Interview (hr: min:sec)
Interviewee 1	Solutions architect in medium-sized blockchain software firm.	20 yrs IT	Public and Consortium	0:54:52
Interviewee 2	Developer in contractor role.	30 yrs IT	Public	1:10:58
Interviewee 3	Developer in small research and development lab.	5 yrs IT	Public	1:11:45
Interviewee 4	Solutions architect and executive in small blockchain software firm.	15 yrs Eng., 3 yrs IT	Public	1:00:48
Interviewee 5	Lawyer in medium-sized law firm.	4 yrs Law	Public and Private	0:45:25
Interviewee 6	Blockchain auditor & production manager blockchain, Big4 Acc'g firm.	4 yrs IT	Private and Consortium	0:58:35
Interviewee 7	Product manager in medium-sized blockchain software firm.	5 yrs IT	Public and Consortium	0:55:18 0:53:26
Interviewee 8	Lawyer, business advisor and executive of small freelance law firm.	8 yrs Law	Public and Consortium	0:48:11
Interviewee 9	Developer, exec. &co-founder of small blockchain security firm.	15 yrs IT	Public	1:06:24 1:18:33
Interviewee 10	Developer in contractor role.	6 yrs IT	Public	0:35:41
Interviewee 11	Developer and co-founder- small blockchain development firm.	4 yrs IT	Public and Private	1:16:18
Interviewee 12	Solutions architect- small blockchain development firm.	3 yrs IT	Public and Private	0:46:57
Interviewee 13	Developer- medium-sized blockchain software firm.	12 yrs Eng., 7 yrs IT	Public	1:57:06
Interviewee 14	Solutions architect – blockchain, Big4 Acc'g firm.	9 yrs Eng., 5 yrs IT	Private	1:20:30
Interviewee 15	Developer in small blockchain software firm.	38 yrs IT	Public	1:02:54
Interviewee 16	Developer - small blockchain development company.	21 years Eng, 8 yrs IT	Public and Private	1:19:07
Interviewee 17	Developer -small blockchain software company.	28 yrs IT	Public	1:15:14
Interviewee 18	Head of blockchain tech. - digital travel company.	23 yrs Eng., 13 yrs IT	Public, Private and Consortium	0:42:24

Appendix A: Semi-structured Interview Questions

General Background *(gives context - age, professional background, years)*:

1. How long have you been working in the IT/legal industry?
   - What is your role within your current organisation?
   - How many years have you been working in this company?

Blockchain Expertise

2. What kinds of BC systems do you interact with in your work or personal time?
   - So by that I mean which types of blockchains, so perhaps public, private or consortium?

3. How do you interact with those types of BC?
   - Do you work with XX BC or do you interact with XX BC in your personal time?
   - What is the main BC project that you are currently working on?
   - What is your role in the project?
   - How does that BC work?

4. Considering that you are an expert in XX blockchains, how would you define a XX blockchain?

Accountability Insights

5. What role does accountability play in XX blockchains?
   - So, by accountability I mean who is responsible to whom in the development/operation of XX blockchains? Can someone demand another to account for their actions?
   - Can I have an example of what you mean?
   - Ok, so how do you know if the blockchain is performing as intended?
   - So, if something goes wrong, how might it go wrong? *(see the process*)
   - Has there been any instances in your experience where something has gone wrong?
   - Who was responsible in those instances?

6. In your expert opinion, who is accountable in the design and implementation/operation of XX blockchains?
   - Can you give me an example?
   - And who is accountable then in the operation of XX blockchains?
   - Can you give me an example?

7. Who do you think should be accountable in XX blockchains?
   - Can I have an example of what you mean?

8. How do you think this happens?
   - What are the key characteristics of XX blockchains makes people accountable?
   - Can I have an example of what you mean?

9. How does this differentiate with XX/other types of blockchains?
    - Can I have an example of what you mean?

Debriefing:

10. Do you have anything that you want to add?
    - Anything further you would like to discuss?
    - Can I have an example of what you mean?

Note: "XX" refers to the type of blockchain system relating to the interviewee concerned.

References

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

Allen, D. W. 2019. 'Governing the entrepreneurial discovery of blockchain applications.' *Journal of Entrepreneurship and Public Policy*.

Allen, D.W. and Berg, C., 2020. 'Blockchain Governance: What we can learn from the economics of corporate governance.' *The JBBA*, https://doi.org/10.31585/jbba-3-1-(8)2020.

Allen, D.W., Berg, C., Markey-Towler, B., Novak, M. and Potts, J., 2020. 'Blockchain and the evolution of institutional technologies: Implications for innovation policy.' *Research Policy*, 49(1), p.103865.

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.

Bonsón, E. And Bednárová (2019), "Blockchain and its implications for accounting and auditing", Meditari Accountancy Research, Vol. 27, No. 5, pp. 725-740.

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.

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.

Chen, Y. 2018, 'Blockchain tokens and the potential democratization of entrepreneurship and innovation,' *Business horizons*, vol. 61, no. 4, pp. 567–575.

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>.

Coyne, J.G. and McMickle, P.L. (2017), "Can blockchains serve an accounting purpose?", Journal of Emerging Technologies in Accounting, Vol. 14 No. 2, pp. 101-111

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.
ICOinRating.com 2018, *Ozex,* viewed 18th April 2021, <https://icoinrating.com/ozex/>.
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.
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.

Ølnes, S. (2017), "Blockchain in government: benefits and implications of distributed ledger technology for information sharing", Government Information Quarterly, Vol. 34, No. 3, pp. 355-364.

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.

Woodside, J. M., Augustine F. K. Jr, and Giberson, W. 2017 'Blockchain technology adoption status and strategies,' *Journal of International Technology and Information Management*, vol. 26, no. 2, pp. 65–93.

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.