The International Journal of Digital Accounting Research
Vol. 23, 2023, pp. 19-45
ISSN: 2340-5058

Hope or hype? Blockchain and accounting

Michael Alles. Rutgers Business School, USA, alles@business.rutgers.edu

Glen L. Gray. California State University, USA, glen.gray@csun.edu

Abstract. Gartner's hype cycle of technology famously progresses from the "peak of inflated expectations" to the "plateau of productivity" via the "trough of disillusionment". Accounting researchers and practitioners—like researchers and practitioners in many other fields—have jumped onto the blockchain bandwagon for fear of missing out on what has been hailed as a world changing technology. Unfortunately, there is a pervasive lack of understanding of what blockchain is, and misconceptions about what it can do. A fundamental problem is that blockchain was derived from bitcoin and there is a great deal of difficulty in defining what blockchain is, and how suitable the methodology for a trustless, public cybercurrency application is to a public blockchain between trusted partners. It is time, we believe, to look at blockchain in accounting with more objectivity. We undertake a detailed exploration of blockchain and identify several key factors that will defines the uses of this technology, namely, the distinction between public and private blockchains and the importance of processing costs as a validating mechanism.

Keywords: Blockchain, bitcoin, auditing, opportunity cost.

DOI: 10.4192/1577-8517-v23_2

Submitted August 2022
Accepted January 2023

1. INTRODUCTION

To accounting information systems (AIS) researchers blockchain is the latest in a long line of emerging technologies to develop "inflated expectations" over—in the terminology of the Gartner Hype cycle—following on from audit analytics, big data, XBRL, drones, expert systems, cloud computing, and so forth. All these topics also generated a large AIS research literature largely extolling the benefits to accounting practice of these technologies. To some extent, this enthusiasm for emerging technology is a healthy outcome since AIS researchers are meant to be the thought leaders of the accounting profession and leaping ahead is the role of pathfinders. However, precisely because it is such a radical innovation, it is important to complement enthusiasm for blockchain technology with a realistic appreciation for both its potential strengths and its current shortcomings.

We have been following bitcoin (and other subsequent major cryptocurrencies) and the latest incarnations of blockchain for over a decade and we are struck how still today there are misstatements, misunderstandings, and misrepresentations as to what blockchain is. That is the reason why we wrote this paper. This is not a primer on blockchain technology since there are already many other excellent sources of that information (Stratopoulos, 2020). Rather, we focus on the way in which the capabilities of the technology both shape and constrain how it can be applied to accounting. In particular, the essential role of cost in determining blockchain security, and the difference between private and public blockchains. Our hope is that this paper will help accounting researchers to develop a vision for the application of blockchain to accounting that is consistent with practice and more likely to make the transition from normative concept to practical implementation.

That objective is even more pressing given that the last few months of 2022 saw yet another crisis for the highly volatile cryptocurrency sector with the virtually overnight collapse of the FTX exchange.[1] Over the course of that year cryptocurrencies lost trillions in market value, which led many to question their future and even legitimacy.[2] Even the leading cryptocurrency, Bitcoin, fell from $47,738.59 on January 1, 2022 to below $17,000 towards the end of the year, a fall of two-thirds of its value that would be considered astonishing for any other asset class.

[1] https://www.nytimes.com/2022/11/11/business/ftx-bankruptcy.html
[2] https://fortune.com/2022/11/11/sam-bankman-fried-ftx-collapse-lehman/

And yet, there are many who continue to serve as cheerleaders for the underlying technology of cybercurrencies, which is blockchain: *"Saying you are not bullish on crypto because of FTX is like saying you are not bullish on stocks because of Bernie Madoff,"* said Ric Edelman, a former financial advisor and founder of the Digital Assets Council of Financial Professionals. *"FTX has nothing to do with blockchain or digital assets, any more than Madoff had anything to do with the stock market…" Edelman emphasized that the underlying benefits of blockchain and digital assets are unaffected by FTX and SBF, as blockchain technology allows businesses to operate faster, safer and cheaper, with greater transparency and inclusion. "Which is why 90% of all banks worldwide are developing the technology, with more than 70,000 software engineers engaged," he said. "More than $35 billion has been invested in this technology in the past two years alone; PwC says it will add nearly $2 trillion to the global economy by 2030, and McKinsey says 70% of global GDP will be digital by 2030. BIS says every government will deploy CBDCs by then — China and The Bahamas already have — and there is broad bipartisan support in almost every country."*[3]

Note the reference in this quote to PwC. The Big 4 professional service firms are in the forefront of pushing blockchain as a technology to solve business problems, which is the other reason for our paper. In an article titled "Inside KPMG, Deloitte, EY and PwC's Plans for Blockchain and Crypto", Stevens (2020) surveys the activities of the Big 4 in the blockchain space. All the Big 4 firms are enthusiastically selling their consulting services to help clients implement various blockchain solutions, such as supply train tracking and managing tax on crypto investments. For example, EY uses its OpsChain platform to enable the Canadian Blood Service to track blood donations, while its Blockchain Analyzer tool *"lets auditors batch trace transactions, look up transaction history, [and] apply tax rules to blockchain business transactions".* KPMG has also developed a blockchain-based supply chain application for its pharmaceutical clients, while PWC helps clients with smart contracts (*"Smart contracts are immutable, after all, and an immutable error is hard to change after launch. PwC helps out with this sort of stuff."*). Deloitte advises clients on accounting and auditing crypto assets, and it also spends a great deal of time educating clients about the potential benefits of

[3] https://finance.yahoo.com/news/why-mark-cuban-others-still-210007022.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACqf17vNdJQVzn3Yd2p_SjJLyJTnYhOub1HyYmrBIUKE2ABmXLeNlctlef5_8iVkRCEPFcJmqLCs6CGTUK_maP-2zbAfwYSpPW243-ctrSVfLKeARm4kb7X5jSsTLHM70AdUiY_OzcGQVaqOT0xSGyMluBBuf-fSq7Xdapx90T4u

blockchain, having developed a tool called "Blockchain in a Box" for this purpose. Stevens (2020) quotes Deloitte's UK blockchain leader, Tyler Welmans: *""We do find that there is still generally not a particularly strong level of understanding in comparison to some other technology trends," he said. However, Welmans argued, there's a deeper understanding of the technology among specialists. Deloitte also acknowledges that educating clients is partly about "teaching them to focus on how they can benefit from using blockchain, rather than getting tied down trying to understand every technical or cryptographic detail around how exactly a blockchain works." "After all," he added, "that's what the specialists are for.""*

Focusing on the benefits of blockchain while leaving it to specialists to figure out how blockchain works is also a good summary of the burgeoning literature by accounting researchers on how blockchain should be used to transform accounting and auditing practice. Desplebin et al. (2021) recently reviewed the already large literature on this topic. Beginning with 229 academic articles and 30 professional articles obtained from a keyword search, the authors eliminated papers that were more about explaining blockchain-based technology (for example, bitcoin) and not on how that technology would impact accounting practice. They ended up reviewing a still substantial set of 39 papers, mostly academic publications, along with a few white papers, such as from the ICAEW (2018). Similarly, Bellucci et al. (2022) undertake a bibliometric analysis of hundreds of papers across a variety of business disciplines and publication outlets and find 127 papers on blockchain and accounting and/or auditing.

The papers surveyed by Desplebin et al. (2021) are uniformly confident that blockchain represents a historical inflection point for accounting. Indeed, given the extent to which all the papers reviewed foresee blockchain as fundamentally changing accounting practice, the conclusion by Desplebin et al. (2021) that *"the points raised here do not imply that the accounting or auditing professions could disappear"* sounds more of a threat than a relief. By contrast, Bellucci et al. (2022) conclude that *"Although there are some proposals for the use of blockchain in accounting, thus far, none have been commonly accepted."* With regard to the objectives of this paper, it is also worth noting the conclusion by Bellucci et al. (2022) that *"Many research products have already contributed to highlighting the essential features and critical elements of blockchain in the context of accounting.* Therefore, we agree with Pimentel and Boulianne (2020, p. 342) that we do not

need more research *"on what a blockchain is or high-level ruminations over how it could be used or abused."* On the basis of our own analysis we shall come to our own conclusion about whether the essential features and critical elements of blockchain no longer warrant much thought by accounting researchers.

In contrast to this academic literature, Stevens (2020) survey of the Big 4 has far less to say about how these firms will apply blockchain to themselves. To be sure, many of the Big 4 are developing tools to assist their auditors value and calculate taxes on cybercurrency holdings, but the only mention by Stevens (2020) of an application of blockchain to the internal processes of these firms is almost comical: *"Deloitte has even dabbled with integrating blockchain into itself, allowing employees in Luxembourg to pay for canteen lunches with Bitcoin."* Not explained are the cost/benefit calculation of paying for a sandwich with bitcoin versus reaching into your pocket for some Euros. More telling than this public relations gambit is the fact that Deloitte has ruled out accepting payment in bitcoin from their own clients.[4]

We don't think that this difference between what academic research is focused on and what practitioners are doing is an accident. Their difference in objectives arises naturally from the divergent incentives of academics and practitioners, namely, getting new publications in accounting journals for the former and getting new customers for the latter. Hence, AIS researchers tend to describe a new technology as a magic bullet that will inevitably transform accounting practice, while practitioners seek to obtain the larger revenues that come from offering the technology as a new product to managers, rather than going after only the much smaller market of process improvement in accounting practice.

There is little doubt that blockchain is a powerful technology that businesses from a wide range of industries sees as transformative. But as Stevens (2020) points out, it is still in the demonstration and experimental stage. He quotes Sam Wyner, one of KPMG's blockchain leaders as saying *"When it comes to enterprise blockchain, clients are coming to us with problems where they think blockchain might be the right way to solve it… We help clients, whether it's looking at business cases, evaluating them, determining if blockchain is the right solution."* By contrast, the AIS literature surveyed by Desplebin et al. (2021) is almost entirely positive, as opposed to normative: in other words, the authors are not "determining if

[4] https://decrypt.co/9358/deloitte-employees-can-use-bitcoin-at-the-canteen

blockchain is the right solution", they assume that it is, and then proceed to lay out the details of their favored solution. The problem with this approach, of focusing only on the benefits of blockchain and ignoring it technical details, is that it all too easy to gloss over the shortcomings that even the most innovative technologies possess. Indeed, perhaps the greater the innovation a technology represents, the greater the caution with which it must be initially approached until sufficient experience enables it to be seen from a proper perspective.[5]

For example, consider the environmental cost of bitcoin, ethereum and other blockchain applications that rely on proof of work as a validation mechanism. Bitcoin uses so much energy that it in increasingly drawing the ire of both environmentalists and governments. Police in Malaysia crushed 1069 bitcoin mining computers using a steamroller because they were operated using stolen electricity.[6] Until recently, an estimated 75% of bitcoin mining took place in China and the energy consumption that necessitated threatened that country's global climate change commitments.[7] As a result, the Chinese government is in the process of discouraging mining in that country and bitcoin miners are moving to other places with cheap electricity, including to Texas.[8]

The accounting literature on blockchain rarely mentions these drawbacks, let alone discuss how they might affect their predictions that blockchain is the future of accounting practice. One response is that the accounting literature is focused on blockchain and not bitcoin, but blockchain often depends on the same energy-intensive validation mechanisms as bitcoin. An alternative approach is to dismiss the energy problems inherent in proof of work with the assertion that it will be soon replaced with more efficient validation mechanisms, such as proof of stake. But as we show in this paper, there is a good reason why these alternatives have yet to fully supplant proof of work. For example, the transition from proof of work to proof of stake in ethereum was delayed for many years before finally becoming implemented in 2022.

Another reason that the accounting literature on blockchain diverges from practice is that there is no consensus yet on what comprises that technology. While this gives

[5] An exception to this positive perspective on blockchain is Coyne and McMickle (2017) which argues that distributed ledgers are not suited for financial reporting due to technical concerns with the Byzantine Generals problem that underlies blockchain.
[6] https://www.bbc.com/news/av/business-57897444
[7] https://www.bbc.com/news/business-56671488
[8] https://www.cnbc.com/2021/06/15/chinas-bitcoin-miner-exodus-.html

researchers the flexibility to create blockchain solutions as they see fit, it also means that there is no guarantee that their vision is consistent with what exists in practice. Blockchain lacks a clear definition because it began not as a proof of concept, as is usually the case with a new technology, but as the outcome of reverse engineering a technology application, the cybercurrency bitcoin.

Hence, people came to know of blockchain only after the media drew their attention to bitcoin. Not surprisingly, then, many subsequently associate blockchain with bitcoin and use the terms interchangeably. It is not unusual to see blockchain articles, including articles published by the AICPA and ISACA, that have titles like how blockchain will impact accountants or how accountants should include blockchain in their practice, but the article is solely about cryptocurrency, in general, with heavy emphasis on bitcoin—and any definitions of blockchain in those articles is based on the specific infrastructure of bitcoin. They are two completely different concepts. Moreover, even within each concept of cryptocurrency and blockchain, there are countless variations that makes it very challenging to generalize either term.

This definitional ambiguity makes it exceptionally difficult to separate what characterizes a blockchain from what is necessary for bitcoin to operate, but it is essential to do so when the application is something as far removed from a cybercurrency as supply chain management of blood supplies or the sale of non-fungible tokens in a piece of digital art. Perhaps the best way of thinking of blockchain is that it, like art, is in the eye of the beholder, and everybody has their own interpretation.

The remainder of this paper is organized as follows. Section 2 examines the disputed definition of blockchain. Particular attention is paid how those components differ between public and private blockchains. In section 3 we discuss the role of processing costs as a validating mechanism. Most famously, bitcoin uses proof of work that is a very secure way of ensuring data integrity. Proof of work (from Dwork & Naor, 1992) is one of the significant adoptions in bitcoin, but the adoption has become increasingly controversial because it is extraordinarily energy intensive. That has resulted in the increasing interest in proof of stake as an alternative. But as we show, the key point is that any validation system must have a significant cost associated with it if blockchain to be credibly secure in a trustless environment. Section 4 provides a broader discussion of the plusses and minuses

associated with blockchain as applied to accounting. Section 5 offers concluding comments.

2. DEFINING BLOCKCHAIN

After scrutinizing diverse blockchain applications, we conclude that there is no such thing as the blockchain standard portfolio of technologies and configurations and, as such, any generalities about blockchain can be misleading (Alles & Gray, 2020b). Decades before the publication of Nakamoto (2008) and the subsequent development of bitcoin cryptocurrency, a chain of blocks or block chain (as two words) was a data structure where, as the name implies, data are stored serially in blocks with each block linked to its previous block. Haber and Stornetta (1991) described using hashing (cryptographics) to create a tamperproof blockchain. Bayer et al. (1992) added Merkle trees to the blockchain design to improve efficiency. Without ever using the term "blockchain" specifically, Nakamoto (2008) brought these and other existing technologies together to create bitcoin cryptocurrency and, the interest in the blockchain concept rapidly expanded in parallel to the growth of interest in bitcoin.

Blockchain was created by reverse engineering the underlying logic of bitcoin to obtain a general-purpose technology as opposed to one specifically meant to operate a cybercurrency. This is the reverse of the usual development process in which an agreed upon basic technology standard is developed first and only then used to create different applications (for example, XML gave rise to XBRL and GPS satellites to Google Maps and Waze). When abstracting from bitcoin to blockchain there are differences of opinion as to whether what is being dropped from bitcoin is only what is needed to operate the cybercurrency application, or whether it is essential for any blockchain application. Is it blockchain data structure *plus* all the attributes associated with bitcoin, which is based on Nakamoto (2008), the true basis for the definition of blockchain? Jeffries (2018) and Bo (2018) discuss the issues associated with blockchain definitions and point out that the reason is not a linguistic one, but rather, the confusion in practice as to what a blockchain is. Jeffries (2018) writes: *"There are countless blockchain explainers in text, audio, and video around the web. Almost all of them are wrong because they start from a false premise. There is no universal definition of a blockchain, and there is widespread disagreement over which qualities are essential in order to call something a blockchain."*

The International Standards Organization defines blockchain as a *"distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links".*[9] To say the least, this is a very minimalistic definition, leaving out more than it includes. For example, the definition says nothing about whether the blockchain is public or private, or how precisely blocks are "confirmed". In defense of the ISO, the standard is still an ongoing project. The Oxford English Dictionary defines blockchain in a similar way, but the differences are illuminating: *"A system in which a record of transactions made in bitcoin or another cryptocurrency is maintained across several computers that are linked in a peer-to-peer network."*[10] The key with the OED definition is the reference to bitcoin, which is acknowledging the inescapable dependence of blockchain on the original bitcoin application created by Nakamoto (2008).

Narayanan and Clark (2017) provide a broader academic perspective on the development of bitcoin. From their perspective as computer science and information technology researchers, they consider Nakamoto (2008) as the culmination of decades of work in cryptography, computer science, data bases and other related technologies. As they say, *"this is not to diminish Nakamoto's achievement but to point out that he stood on the shoulders of giants."* Perhaps the most important insight that Narayanan and Clark (2017, emphasis added) provide in their article is about going from bitcoin to blockchain: *"So far, this article has not addressed the blockchain, which, if you believe the hype, is bitcoin's main invention. It might come as a surprise to you that Nakamoto doesn't mention that term at all. In fact, the term blockchain has no standard technical definition but is* ***a loose umbrella term used by various parties to refer to systems that bear varying levels of resemblance to bitcoin and its ledger****."*

While Narayanan and Clark (2017) undoubtedly intended in this last sentence to imply that most blockchain applications do not meet what they consider to be the necessary requirements for the technology underlying bitcoin, we think that *"the various levels of resemblance to bitcoin and its ledger"* is as good a definition of public blockchain as it is feasible to have at this current time.

The bitcoin blockchain is an example of a **public blockchain**. Public blockchains are also referred to as permissionless or trustless blockchains because anybody can

[9] https://www.iso.org/obp/ui/#iso:std:iso:22739:ed-1:v1:en
[10] https://www.lexico.com/en/definition/blockchain

join the application without prior approval and the users are anonymous and do not know (or necessarily trust) each other. By contrast, the prominent Walmart mango tracking blockchain application (Kamath, 2018) is an example of a **private blockchain** that does not include all the technology components of bitcoin and some of the remaining components are configured significantly differently. Private blockchains are also referred to as **permissioned** and trusted applications because the users are known to (and trusted by) each other and must be approved to join the application.

Figure 1 illustrates the main differences between a public blockchain (as exemplified by bitcoin, the oldest and one of the more complex public blockchains) and a private blockchain (as exemplified by IBM's broad generic private blockchain design fundamentals described in Gupta (2018)).

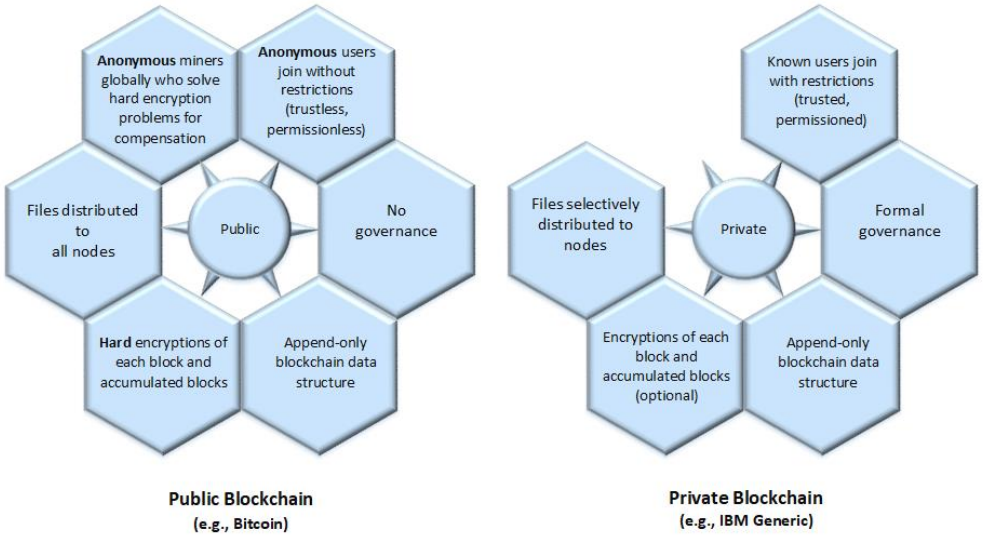

Figure 1. Typical components of public and private blockchains

Prominent examples of private blockchains include Ripple and Hyperledger, and they have very different operation philosophies to public blockchains like bitcoin or ethereum. This operating assumption of private blockchains shows why many authors don't consider private blockchains to be a true blockchain application at all, since they are designed for such a different setting (Bo, 2018; Narayanan & Clark 2017). By contrast, though, many accounting papers lump all types of blockchains together and don't consider the tradeoffs inherent between them.

Perhaps the most important difference between the two is that users on a private blockchain are in it for their own self-interest and have been given permission to join. They can be thought of as the equivalent of vendors who have obtained permission to be listed on a customer's authorized vendor list. A subset of these users might take part in the private blockchain's validation system (for example, chosen randomly in the case of Hyperledger), with validation as task they do willingly as the price for having access to the system.

By contrast, public blockchains typically need to reward those who undertake the onerous task of validating new blocks, as well as storing the entire distributed ledger which continuously increases in size. That is why almost all public blockchains, even those whose main purpose is operational tasks like hosting smart contracts (ethereum, for instance), have their own cyber currencies to serve as the medium of reward. Of course, in the case of pure cyber currencies like bitcoin, the currency is not just a means towards the end of validation, but the end in itself. Regardless, once a cyber currency exists, it will be traded and the main driver of transactions in it will be speculation in the hope of gain, independent of whatever "real" function the public blockchain has (hence, the sorry saga of FTT, the token currency issued by FTX). Accounting papers on blockchain applied to accounting rarely mention what validation mechanism they have in mind, let alone what the implications are of being dependent upon a cyber currency that may be subject to highly volatile trading.

Another crucial factor differentiating blockchain applications is the characteristics of what is represented on the blocks of the blockchain application. It is critical whether the blockchain application is being used as a medium for digital-only transactions (e.g., bitcoin) versus physical transactions (e.g., representing the movement of tuna fish through the supply chain). Table 1 illustrates the mix of these two dichotomies.

		Blockchain Applications	
		Public	**Private**
Assets being Tracked	**Digital**	*Cell 1*	*Cell 3*
	Physical	*Cell 2*	*Cell 4*

Table 1. Blockchain applications vs. assets tracked matrix

The columns represent the public vs. public dichotomy and the rows represent the digital vs. physical dichotomy. Each cell in the Table 1 matrix has radically distinct characteristics that will substantially affect developing a specific application, designing the appropriate controls, and planning the subsequent audit. With very few exceptions, all cryptocurrency applications are in Cell 1 (public blockchain/digital assets) and physical-world applications (e.g., tracking agricultural products) are in Cell 2 (public blockchain/physical assets) if they use something like ethereum, though those run by corporations like Walmart are in Cell 4 (private blockchain/physical assets). Because banking participants legally cannot be anonymous, most banking-related applications are in Cell 3 (private blockchain/digital assets). Alles and Gray (2020a) provides a deeper discussion of the differences (and related audit issues) between using blockchain for physical versus digital assets, while this paper focuses on public versus private blockchains.

The accounting literature tends to focus on blockchain as a ledger and not take into consideration at all whether the transactions being recorded are physical or digital. As Alles and Gray (2020a) point out, until there is a solution to what they call "the first-mile problem" unavoidable with physical transactions—ensuring that the digital record stored on the blockchain is exactly isomorphic to the physical product that the data refers to—accountants will still have to perform reconciliations. In other words, they point out the logical error in the unqualified optimism of ICAEW (2018): *"For accountants, using blockchain provides clarity over ownership of assets and existence of obligations, and could dramatically improve efficiency."*

3. THE ROLE OF PROCESSING COSTS IN THE BLOCKCHAIN VALIDATION MECHANISM

Since bitcoin has no governing body and the users are anonymous and unknown to each other, bitcoin had to be designed to ensure immutability of the bitcoin file and to guard against double spending the same bitcoin on two different transactions. First, we will explore immutability. Public blockchains such as bitcoin is permissionless and trustless and has no intermediaries. In such an environment, protecting the integrity of the data is critical. Nakamoto (2008) addressed the problem by using proof of work as a consensus mechanism.

Participants who wish to take part in the consensus mechanism are known as miners and they primary work is referred to as the proof of work, which is a *"piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements."*[11]

Narayanan and Clark (2017) explain Nakamoto's (2008) innovation in bringing together a variety of technologies to ensure the integrity of bitcoin: *"In bitcoin, a secure ledger is necessary to prevent double spending and thus ensure that the currency has value. A valuable currency is necessary to reward miners. In turn, strength of mining power is necessary to secure the ledger. Without it, an adversary could amass more than 50 percent of the global mining power and thereby be able to generate blocks faster than the rest of the network, double-spend transactions, and effectively rewrite history, overrunning the system. Thus, bitcoin is bootstrapped, with a circular dependence among these three components."* The way this circular dependence works in bitcoin is that hashes of the latest transactional data are only added to the distributed ledger if there is consensus among participants (in the case of bitcoin, consensus means a simple majority, often inaccurately described as a 51% rule).

Miners must come up with a 32-character hash that begins with a certain number of zeros using the SHA-256 cryptographic hash function. Given that there are SHA-256 cryptographic hash function algorithms available, this is a not a difficult problem to solve, but since it can only be done by trial and error, it takes time to do so. Moreover, the bitcoin software automatically adjusts the difficulty of the problem miners must solve so that it always takes about ten minutes of computing time despite the increasing power of the computers running the hashing calculators and the number of miners.

Since the reward is paid only when the majority of miners agree, it is essential that no one party can represent that majority by themselves, since they would then be in control of the distributed ledger and undermine the integrity of the entire system. That is why the proof of work is deliberately difficult and, assuming that there are many miners, it becomes very costly for a single party to create a majority of the total mining power (remember, in order to be a bona fide miner, you have to actually do the work). The weakness of this scheme is that as the value of the bitcoin increases, it may be worthwhile for coalitions of miners to attempt to form a

[11] https://en.bitcoin.it/wiki/Proof_of_work

majority instead, as Eyal and Sirer (2018) point out. However, exploring that issue is beyond the scope of this paper.[12]

The real value of this seemingly pointless exercise of the proof of work is that the majority of miners have to agree that one of them came up with the required solution first—in order to claim the reward—and they will only do so if they agree that they are in fact verifying the same data. In other words, as far as the design of bitcoin is concerned, proof of work and the consensus mechanism are simply a means towards the end of ensuring the integrity of the data entered in the distributed ledger. But and this is a big but, for individual miners, mining is an end in itself, since it gives them the chance to earn bitcoins as a reward. Nakamoto's (2008) great achievement was in seeing how this private incentive could be used to generate the public good of a secure distributed data set.

Bitcoin was intentionally developed to be fully trustworthy to people that had no other basis to trust each other. Many of its characteristics, such as the proof of work, Merkle Chains and cryptography are necessitated by the need to ensure that transactions can take place between participants who know nothing about each other, not even their identities, and have zero trust between them. While Nakamoto (2008) has succeeded brilliantly with his solution to this problem, it comes with considerable drawbacks.

Most particularly, trust is replaced by high processing costs, in the form of the proof of work, which impedes opportunistic behavior by any party. In the case of bitcoin, the processing cost is measured in terms of the electricity costs of running the proof of work algorithms (less widely discussed is the carbon footprint and heat pollution the computers running the algorithms generate, not to mention the e-waste created as the need for ever faster processing results in large quantities of obsolete computers being dumped). The number of hashing calculations being performed by bitcoin miners is growing exponentially, and de Vries (2018) estimates that the electricity required to do so amounts to some half-percent of world electricity usage in 2018. There is now a game of sorts of calculating which nation's electricity consumption is equal to that used to mine bitcoin, with candidate countries growing

[12] Another problem is that since the number of bitcoins that can be issued is limited to prevent inflation, at some point the reward for mining may become so small (and eventually it will become zero) that there may no longer be an incentive to keep mining. The problem is that as the number of miners decrease, it becomes cheaper for any one miner or consortium of miners to attain majority control. Again, the implications of these aspects of bitcoin are beyond the scope of this paper.

larger and larger in population, from El Salvador to Austria and Argentina.[13]

Ethereum is now using proof of stake in place of proof of work arguing that it provides similar levels of security as a validation mechanism at much lower energy cost. Proof of stake means that users with larger holdings of the ethereum based cybercurrency (or more precisely, a cybertoken), ether (ETH), have a larger role to play in the consensus mechanism. In a proof of stake setting there is no longer any need to solve an algorithm to be eligible for a reward, so transactions will be processed much faster, perhaps as much as 15,000 per second, comparable to Visa.[14] Newer proof of stake based cybercurrencies, such as Cardano, promise even faster transaction speeds, up to a million per second in the case of Cardano.[15]

How does proof of stake work? Ethereum explains: *"Proof-of-stake is the underlying mechanism that activates validators upon receipt of enough stake. For Ethereum, users will need to stake 32 ETH to become a validator. Validators are chosen at random to create blocks and are responsible for checking and confirming blocks they don't create. A user's stake is also used as a way to incentivize good validator behavior. For example, a user can lose a portion of their stake for things like going offline (failing to validate) or their entire stake for deliberate collusion. Unlike proof-of-work, validators don't need to use significant amounts of computational power because they're selected at random and aren't competing. They don't need to mine blocks; they just need to create blocks when chosen and validate proposed blocks when they're not. This validation is known as attesting. You can think of attesting as saying "this block looks good to me." Validators get rewards for proposing new blocks and for attesting to ones they've seen. If you attest to malicious blocks, you lose your stake."*[16]

The underlying logic of proof of stake is that since their own money is at risk, attestors have a reason to maintain the legitimacy of the ethereum system. Proof of stake eliminates the electricity consumption of proof of work, but on the other hand, because the probability of being chosen as a validator depends on how much of a stake one holds, it results in the rich becoming richer. Moreover, attestors are rewarded in proof of stake with freshly created ETH, acting effectively as interest on their stake. This has two implications. First, that inflation is higher under proof

[13] https://digiconomist.net/bitcoin-energy-consumption/
[14] https://www.finextra.com/blogposting/19890/ethereum-vs-bitcoin---similarities-and-differences
[15] https://www.nasdaq.com/articles/why-cardano-could-be-an-ethereum-killer-2021-07-02
[16] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

of stake than proof of work. And second, that anyone who holds ETH but does not take stake it will find their holding diluted by the newly created ETH. Hence, all ETH holders will also be forced to stake, with all the costs and risks that this entails. Moreover, the fact that stakeholders effectively earn interest on their stakes means, in turn, that it is feasible for governments to impose a capital gains tax under proof of work, which creates all manner of problems of its own.[17]

The value of 32 ETH as of December 21, 2022, is $38,704.32,[18] which means that the initial cost of being an ethereum attestor is far higher than that of a proof of work miner (approximately, just under $10,000). In practice, under both systems, all but the richest individuals will have to join a consortium to increase their probability of earning rewards and with economies of scale, consolidation will see the number of players decrease in number and increase in size. Arguably, such a process will be faster and more complete with easy to move money than computer servers.

Unlike proof of work with its relatively straightforward mining process, the efficacy of proof stake depends critically on design choices, such as the algorithm for selecting attestors, the circumstances under which stakes are voided for inappropriate behavior, and so forth. It is a complex game-theoretic application that balances speed of attestation versus the level of security of the process. If bitcoin's proof of work is the benchmark for a highly secure, but correspondingly slow blockchain process, it remains an unresolved question what tradeoffs are inherent in proof of stake applications such as Ethereum 2.0 or Cardano.

In short, proof of stake is not the panacea that it has been portrayed for the downsides of proof of work. With both validation mechanisms, the devil is in the details. On the other hand, it cannot be overemphasized how important it is that proof of stake or some other more efficient validation mechanism succeeds in replacing proof of work. Without getting away from the environmentally damaging energy consumption that mining necessitates it is hard to see how the blockchain enabled world envisioned by so many, not least accounting researchers, can ever be made feasible.

The main point is that the rationale for blockchain in its strictest bitcoin version is to allow transactions to take place between parties who have virtually no trust in

[17] https://www.youtube.com/watch?v=wc-X3XHtmhE
[18] https://walletinvestor.com/converter/ethereum/usd/32

each other. That is why it builds in high processing costs to prevent cheating. Nevertheless, if there is even a modicum of trust between parties, then high transaction cost or processing cost becomes a hurdle whose value should be questioned. Ironically, given the necessity for all parties in the transaction layer to agree to use the communication protocol, the very act of operating the blockchain will begin to stimulate trust.

That is not to say that the blockchain may not add value, for there remains the great benefit of the common and distributed storage layer. As projects such as that used to track shipping containers show, in a very fragmented system with always changing parties there may be value in having a single easily accessible way to store and share information. In this case, with many different countries involved, having a storage layer not controlled by any one nation may also be an attraction, if nothing else, for reasons of political sensitivities. However, as always, a single centrally controlled database would achieve the same ends much more cheaply, which means that the case must be made for why the application must be "blockchained". Perhaps, at this time, the true explanation is that the novelty of the technology brings parties to the table in a way that they could not be drawn before.

That seems to be the case with the Openfiling initiative which is creating a centralized depository for financial statements currently being filed with the regulators of the individual member nations of the European Union. They intend to use blockchain as a way, they claim, of ensuring via hashing that the reports have not been changed since they were originally filed. This seems to be a solution in search of a problem since no one has questioned the integrity of statements obtained from the SEC's Edgar system, for example, despite the lack of a hashed digital signature. On questioning by the authors of this paper of a senior member of this initiative as to why a regular database would not suffice, as opposed to a distributed ledger, the member finally admitted that the reason was political. By distributing the ledger to all national members, they were less likely to feel that there were simply handing over "their" nation's financial information to a more powerful institution in Brussels or Frankfurt.

4. BLOCKCHAIN PLUSSES AND MINUSES

"Given the investment in crypto research there are player gagging for a return on investment. My question is, what is the problem or opportunity you are solving with crypto currencies, because I have not seen an argument that stacks up yet."[19]

One of the most highly acclaimed blockchain applications was its use to track shipping containers in an initiative headed by the shipping giant Maersk and IBM.[20] But that award winning project, TradeLens Digital Ledger, is to shut down in the first quarter of 2023.[21] As Avivah Litan, a vice president analyst at Gartner Research explained, *"I think the ROI just wasn't there. They were spending more than they were getting back in terms of financial value. Also, IBM is no longer willing to take losses on their enterprise blockchain projects and have been gradually exiting their blockchain business."*[22]

If one only read the accounting literature on blockchain you would not be aware that there is any downside whatsoever to the technology. The perspective of those papers is almost uniformly that of a cheerleader, which is perhaps only to be expected of papers that are normative in intention. But it is important to see that like all technologies, blockchain has both plusses and minuses. In this section we discuss both, with many of the examples drawn from bitcoin, the blockchain application par exemplar.

The three most widely publicized aspects of blockchain in general, and bitcoin (and all other cybercurrencies, such as ethereum,) specifically are immutability, disintermediation, and distributed ledger technology (DLT). In our opinion, immutability and disintermediation are probably overhyped, and DLT is underhyped. DLT may also be described as *shared ledgers* in that all the participants are sharing "a single version of truth". Shared ledger is not a new concept, but it is a very powerful one.

For example, conceptually the buyers and sellers in a supply chain blockchain are sharing the exact same data files. A seller's accounts receivable file is a buyer's accounts payable file. At the 2019, 44th World Continuous Auditing and Reporting

[19] User comment to article https://www.theguardian.com/commentisfree/2021/jul/05/cryptocurrencies-financial-system-digital-future

[20] https://www.maersk.com/digital-solutions/tradelens

[21] https://www.tradelens.com/press-releases/tradelens-wins-supply-chain-transformation-of-the-year-award-at-supply-chain-asia-forum; https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens

[22] https://www.computerworld.com/article/3682128/maersks-tradelens-demise-likely-a-death-knell-for-blockchain-consortiums.html

Symposium (WCARS) in Seville, Spain, a representative of the Danish Business Authority made a presentation regarding a proposed platform for financial reporting and VAT settlement where buyers, sellers, and the Danish Business Authority shared one blockchain application. A buyer and seller would share a common invoice reflecting their agreed terms and the resulting invoices could be used to calculate VAT liabilities for sellers for their tax filings.

Immutability is not absolute; with enough computer resources and/or collusion among key people, data can be hacked. The ultimate degree of immutability is significantly affected by numerous blockchain design decisions. Disintermediation (eliminating third parties such as banks and credit card companies) can introduce a completely new set of trust issues because disintermediation usually means replacing one set of third parties with another set of third parties (in particular, online exchanges in bitcoin transactions).

In terms of the blockchain disintermediation advantage of having no central authority, that can be both a positive and a negative. Steve Wozniak, cofounder of Apple Computer, was defrauded when he transferred seven bitcoins to someone who gave him a stolen credit card number. There was no recourse because there was no intermediary (e.g., bitcoin or credit card company) he could contact to help retrieve his seven bitcoins. One could argue that this is just one anecdote and that the use of a stolen credit card or the bankruptcy of an exchange company are outside of the direct purview of blockchain or bitcoin; but that is a shallow argument if you cannot get your stolen bitcoins back. Consider the following comment on a blockchain article (Figure 2).[23]

To the argument that this is simply a beginner's mistake that would not take place today, consider the case of Mircea Popescu, who was swept away by a rogue wave on a beach in Cost Rica in early July 2021. He was a pioneer and highly sophisticated investor in cryptocurrencies and possessed the single largest [known] holdings of bitcoin with a value estimated at anywhere between $1-2 billion.

[23] https://coinsutra.com/bitcoin-double-spending/

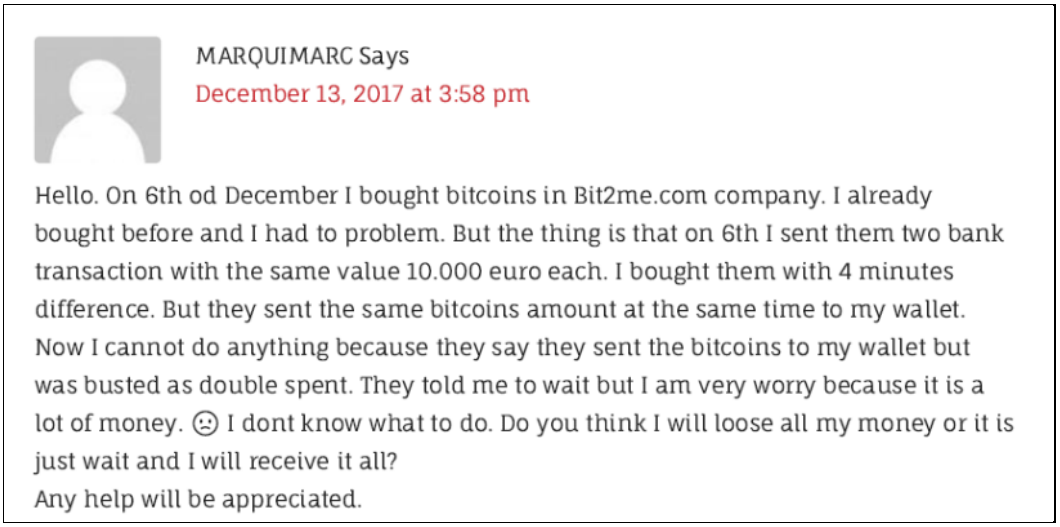

Figure 2. Bitcoin double spending post

His unfortunate and unexpected death revealed a singular problem with entirely digital assets: *"What is unclear is how Popescu stored his crypto? Is it in a cold wallet, unconnected by computers, that only he holds the private key to, or is his cache of bitcoin held with a third-party? Some speculate that he had a private key and that no one has access to it, which would mean that his fortune, whatever its size, is lost on the blockchain forever. "Access to Mircea Popescu's reported $2 billion in Bitcoin would only be accessible through his private keys, whether he stored them digitally or in cold storage like a physical Bitcoin wallet," Voyager Digital CEO Steve Ehrlich told MarketWatch via email. "It's unclear if anyone besides Popescu has access to those wallets," he said. "If there isn't anyone who has the private keys to his Bitcoin storage, those coins could essentially be 'lost' forever in the sense that they will just sit in his wallets without the ability to be liquidated.""*[24] There have been numerous news stories of lost bitcoin keys[25], but it should be noted that the same problem can arise with other cybercurrencies, such as Ethereum.[26]

In response to Popescu's death, another bitcoin investor, Anthony Pompliano, co-founder and partner at Morgan Creek Digital Assets, sent out a now deleted tweet

[24] https://www.marketwatch.com/story/bitcoin-pros-speculate-over-possible-loss-of-2-billion-crypto-fortune-after-death-of-one-large-owner-11625255745
[25] https://cryptonews.com/exclusives/man-looking-for-lost-btc-7-500-in-a-rubbish-dump-plans-hi-te-10998.htm.
[26] https://www.the-sun.com/news/3338091/family-6million-ethereum-crypto-fortune-lost/

that perhaps best captures the laissez faire philosophy that underlies bitcoin (Figure 3).[27]

Figure 3. Bitcoin post 2

What we stress in this article is that blockchain is not a technology in isolation. Rather, it must be placed within the full context of the environment in which it operates to design, control, and audit the application. That point is made very clearly in a concern that has recently been raised by British regulators about how cybercurrencies could be used to hide and steal corporate assets: *"The government could face "limitless" losses as a result of businesses that accept payments in untaxed and untraceable cryptocurrencies going bust, an insolvency expert has warned. A growing number of companies, including the ethical cosmetics firm Lush and office-sharing firm WeWork, have begun taking payments for goods and services in cryptocurrencies such as bitcoin, alongside debt, credit or cash. But while the shift has been welcomed by crypto-enthusiasts, experts said it could be an easy way for directors to hide cash from authorities, particularly when companies go bust. Julie Palmer, a managing director at insolvency firm Begbies Traynor, said the growing popularity of cryptocurrency payments would make it harder for administrators—who are in charge of winding down a business after it fails—to*

[27] https://www.marketwatch.com/story/bitcoin-pros-speculate-over-possible-loss-of-2-billion-crypto-fortune-after-death-of-one-large-owner-11625255745

*track where money has come from, and whether owners, staff or directors are stripping funds out of the business illegally. It means criminals could walk away with income that would usually be clawed back and distributed to creditors, including the tax collectors at HM Revenue and Customs and local authorities. Palmer said that without new regulations and taxation plans, the government could face huge losses. "The potential is limitless, depending on how popular this becomes," she warned. It is the latest threat emerging from the rising popul*arity *of cryptocurrencies, which have been linked to money laundering and black market dealings."*

Perhaps accounting researchers can justify ignoring the problem of lost keys as something that only affects cybercurrencies and so is not an "accounting problem". But the fear that they can be used to get around bankruptcy protection for shareholders is very much an accounting issue and it stands in stark contrast to the viewpoint expressed by the ICAEW (2018) that "*using blockchain provides clarity over ownership of assets and existence of obligations".*

5. CONCLUSION

When it comes specifically to blockchain and the accounting domain, there is a frequent disparity between what many accounting practitioners and researchers are saying about the benefits of blockchain, and the issues and concerns associated with the current realities of blockchain applications. Accounting practitioners and academics are predicting that blockchain will reduce operating costs, reduce fraud, improve audits, and reduce accounting activities. Appelbaum and Nehmer (2018) confidently state that *"soon the audit profession will be forced to examine blockchain in an engagement, and even blockchain events in a cloud."* NYU professor David Yermack opines that the audit profession may be dead in 10 years due AI and blockchain because blockchain *"reduces the need for audit by 97 percent"* (Yermack, 2018).

By contrast, Kathleen M. Hamm, PCAOB Board Member, stated: *"Blockchain does not magically make information contained within it inherently trustworthy. Events recorded in the chain are not necessarily accurate and complete. Recording a transaction on a blockchain does not alleviate the risk that the transaction is unauthorized, fraudulent, or illegal. Blockchain also does not address threats that parties to a transaction are related, or that side agreements exist that are not reflected in the chain. And nothing in the technology ensures proper classification*

of transactions in the financial statements."[28] In a similar vein, Carson et al. (2018) say, *"blockchain is [not] a truth machine...Blockchain cannot assess whether an external input is accurate or 'truthful'—this applies to all off chain assets and data digitally represented on the blockchain."* They go on to add: "*However, connecting and securing physical goods to a blockchain requires enabling technologies like IoT [Internet of Things] and biometrics. This connection can be a vulnerability in the security of a blockchain ledger because while the blockchain record might be immutable, the physical item or IoT sensor can still be tampered with. For example, certifying the chain of custody of commodities like grain or milk would require a tagging system like radio-frequency identification that would increase the assurance being provided but not deliver absolute provenance."*

As stated in the introduction, these discrepancies in blockchain literature is primarily due to the failure to distinguish between two fundamental aspects of blockchains. First, the incorrect transference of the characteristics and benefits of *public* blockchain applications to *private* blockchain applications. Second, not fully considering the risk ramifications associated with tracking digital assets (e.g., cryptocurrencies) versus tracking physical assets (e.g., agricultural products).

We end with an example from the accounting literature on blockchain applied to accounting from Dai and Vasarhelyi (2017). We do not question the innovation of their proposal to use blockchain to implement a form of triple-entry accounting, but we use this example only to show that as with much of this literature, the devil is in the details that are often overlooked.

Dai and Vasarhelyi (2017) describe their validation process: *"Although the verification process will be automated by blockchain technology, this process should be restricted to certain parties, such as accountants, management, auditors, etc. Therefore, the blockchain ledger in this scenario falls into the permissioned blockchain category. In addition, each party would have a specific role in the verification process, and their actions and concerns might be addressed differently. For example, if an auditor doubts a transaction, then it might be paused for confirmation by accountants, while the CFO could decide to cancel it entirely. These rules could also be executed by smart contracts. Valid transactions would be grouped into blocks and appended to the main chain, and then users who have authorizations can view and explore them. Due to the nature of blockchain,*

[28] https://pcaobus.org/News/Speech/Pages/what-auditors-need-to-know-blockchain-other-emerging-technologies.aspx

confirmed and uploaded transactions cannot be manipulated. To protect the privacy of a company's sensitive data, the transactions could be encrypted before being uploaded to the blockchain ledger, and only users who have the decryption key should be able to view the content of transactions."

Think carefully about how this system would work. Every business that has transactions with another will have entries on the blockchain. Of course, any business of any size will have interactions with hundreds, if not thousands of other firms. The accountants and auditors of all of these firms would need to have access to not only enter data onto the blockchain hosting the triple-entry ledger, but to correct and audit it too. Moreover, as Dai and Vasarhelyi (2017) write, innumerable users would need to possess private keys to decrypt the proprietary data on the blockchain to verify or assure them. This is about as far removed from the immutability of bitcoin as could be imagined.

The vulnerabilities of this proposal are not unique to it. At the 2020 World Continuous Auditing and Reporting conference, EY Assurance Services partner Michael Leonardson, in a talk entitled "Accounting for and Auditing Digital Assets", also made the point that internal auditors will need to have access to private keys to decrypt the business's own encrypted blockchains to check them. This will then require tertiary assurance ("who will guard the guards?") as is currently undertaken by IT internal auditors and external auditors to check what IT system superusers are doing with their ability to manipulate data on the corporate ERP system. In other words, even incorporating blockchain into accounting may not mark the end of auditing, simply a shift in its domain.

Accounting researchers and practitioners—like researchers and practitioners in many other fields—have jumped onto the blockchain bandwagon for fear of missing out (FOMO) on what has been hailed as a world-changing technology. Unfortunately, there is a lack of understanding of what blockchain is, and misconceptions about what it can do. A fundamental problem is that blockchain was derived from bitcoin and there is a great deal of confusion in defining what blockchain is and how suitable the methodology for a trustless, public cybercurrency application is to a private blockchain between trusted partners.

The focus of the paper is placing blockchain within the context of the business environment in which it is meant to operate. As we saw with previous technological innovations like cloud computing and XBRL, there is a tendency among accounting

researchers, to see a new technology as an end and not as a means towards an end. That shift in perspective makes a substantial difference to the perceived value added of blockchain technology. Now that the bloom has gone off blockchain and we are well into the trough of disillusionment, to use Gartner's terminology, AIS researchers should return to that old auditor's standby: professional skepticism. Their task as thought leaders is no longer to advocate for an emerging technology, but to research the best way to adapt it to the needs and constraints of accounting practice.

6. REFERENCES

Alles, M., & Gray, G. (2020a). "The First Mile Problem": Deriving an Endogenous Demand for Auditing in Blockchain-based Business Processes. *International Journal of Accounting Information Systems*, 38. https://doi.org/10.1016/j.accinf.2020.100465

Alles, M., & Gray, G. (2020b). What Accountants Need to know about Blockchain. 2020. In Information for Efficient Decision Making: Big Data, Blockchain and Relevance. Kashi Balachandran, editor. World Scientific Books, World Scientific Publishing Co. Pte. Ltd. https://doi.org/10.1111/1911-3838.12240

Appelbaum, D., & Nehmer, R. (2020). Auditing Cloud-Based Blockchain Accounting Systems. *Journal of Information Systems*, 34(2), 5–21. https://doi.org/10.2308/isys-52660

Bayer, D., Haber, S., & Stornetta, W.S. (1992). Improving the Efficiency and Reliability of Digital Time-Stamping. Proceedings of Sequences 1991. https://link.springer.com/chapter/10.1007/978-1-4613-9323-8_24

Bellucci, M., Cesa Bianchi, D., & Manetti, G. (2022). Blockchain in accounting practice and research: systematic literature review. *Meditari Accountancy Research*, *30*(7), 121–146. https://doi.org/10.1108/MEDAR-10-2021-1477

Bo, F. (2018). Blockchain: disambiguation problem. https://medium.com/swlh/blockchain-disambiguation-problem-ca72916bb51b Accessed 13 March 2023.

Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (2018). Blockchain beyond the hype: What is the strategic business value? https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value Accessed 13 March 2023.

Coyne, J., & McMickle, P. (2017). Can Blockchains Serve an Accounting Purpose? *Journal of Emerging Technologies in Accounting,* 14 (2), 101–111. https://doi.org/10.2308/jeta-51910

Dai, J., & Vasarhelyi, M. (2017). Toward Blockchain-Based Accounting and Assurance. *Journal of Information Systems,* 31(3), 5-21. https://doi.org/10.2308/isys-51804

Desplebin, O., Lux, G., & Petit, N. (2021). To Be or Not to Be: Blockchain and the Future of Accounting and Auditing. *Account Perspectives,* 743-769. https://doi.org/10.1111/1911-3838.12265

Dwork, C., & Naor, M. (1992). Pricing via processing or combatting junk mail. https://dl.acm.org/citation.cfm?id=705669 Accessed 13 March 2023.

Eyal, I., & Sirer, E. (2018). Majority Is Not Enough: Bitcoin Mining Is Vulnerable. *Communications of the ACM,* 61(7), 95-102. https://doi.org/10.48550/arXiv.1311.0243

Gupta, M. (2018). *Blockchain for Dummies,* 2nd IBM Limited Edition. John Wiley & Sons, Inc. Hoboken, NJ.

Haber, S., Stornetta, W. S. 1991. How to timestamp a digital document. *Journal of Cryptology*, 3(2), 99-111. https://link.springer.com/chapter/10.1007/3-540-38424-3_32

ICAEW. (2018). Blockchain and the future of accountancy. Institute of Chartered Accountants of England and Wales. https://www.icaew.com/technical/technology/blockchain/blockchainarticles/blockchain-and-the-accounting-perspective Accessed 4 March 2023.

Jeffries, A. (2018). 'Blockchain' is Meaningless: 'You keep using that word. I do not think it means what you think it means'. https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning Accessed 7 March 2023.

Kamath, R. (2018). Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM. *The Journal of the British Blockchain Association,* 1(1), 1-12. https://doi.org/10.31585/jbba-1-1-(10)2018.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

Narayanan, A., & Clark, J. (2017). Bitcoin's Academic Pedigree. *Communications of the ACM,* 60(12), 36-45. https://doi.org/10.1145/3134434.3136559

Pimentel, E., & Boulianne, E. (2020). Blockchain in accounting research and practice: current trends and future opportunities, *Accounting Perspectives,* 19(4), 325-361. https://doi.org/10.1111/1911-3838.12239

Stevens, R. (2020). Inside KPMG, Deloitte, EY and PwC's Plans for Blockchain and Crypto. https://decrypt.co/40865/inside-kmpg-deloitte-ey-and-pwcs-plans-for-blockchain-and-crypto Accessed 7 September 2023.

Stratopoulos, T. (2020). Teaching Blockchain to Accounting Students. *Journal of Emerging Technologies in Accounting*, 17(2), 63–74. https://doi.org/10.2308/JETA-2020-052

de Vries, A. (2018). Bitcoin's Growing Electricity Problem. *Joule,* 2(5), 801-805. https://doi.org/10.1016/j.joule.2018.04.016

Yermack, D. (2018). Audit dead in a decade? https://www.accountingtoday.com/news/audit-dead-in-a-decade Accessed 31 October 2022.