Blockchain technology in the auditing environment

Pedro W. Abreu
Intituto Universitário de Lisboa (ISCTE-IUL)
pedro.w.abreu@gmail.com

Manuela Aparicio
Intituto Universitário de Lisboa (ISCTE-IUL), ISTAR-IUL
NOVA, Information Management School (NOVA IMS), Universidade Nova de Lisboa
manuela.aparicio@acm.org

Carlos J. Costa
ISEG (Lisbon School of Economics and Management), Universidade de Lisboa
cjcosta@iseg.ulisboa.pt

Abstract — **Blockchain technology is already being talked about as one of the megatrends for the next years. Researchers and organisations are starting to understand the potential benefits of this technology and are exploring how it can disrupt the world we live in with a diverse range of applications. But the truth is the ability to move blockchain from concept to adoption and production has been minimal yet. When it comes to auditing, blockchain solutions could have important benefits by reducing the workload of the auditors, helping in minimising fraud and optimising the existing processes but is also vital to have in mind other emerging technologies. Factom, Libra, and Verady are some examples of companies developing blockchain solutions that can be applied in the auditing environment, but much of the necessary development is still yet to be done.**

Keywords - Blockchain; cryptocurrency; auditing.

I. INTRODUCTION

The CEO of IBM, Ginni Rometty, said: "*What the internet did for communications, blockchain will do for trusted transactions*." It is expected that by 2024, the amount of global blockchain market to be worth $20 billion [1] and currently, 90% of major North American and European banks are now exploring blockchain technology in the field of payments [2], giving us a glimpse of how big this trend is becoming. But in fact, there is still a considerable lack of technical know-how in the blockchain development area. By mid-2016 there was an estimation that there were only "5,000 developers dedicated to writing software for the cryptocurrency, Bitcoin, or blockchain in general" [3].

According to the 2017 Upwork Skills Index ranks, blockchain developers were ranked second in the fastest-growing skills in the U.S. freelance job market, just after robotics [4].

This paper aims to explore what is the blockchain technology and some of its variations, how can the this be applied to auditing and present some existing solutions. For that, a literature review was used by including information from different articles, books, and websites related to the topic. This is not a technical paper; it does not explore the programming and mathematical basis that sustains the blockchain technology.

It starts by defining the blockchain concept, how it began and how it is evolving, then it will focus on how this technology can be used in the auditing environment, its impacts and benefits as well as some example of companies that are developing solutions for auditing and other purposes.

II. BLOCKCHAIN CONCEPT

The blockchain concept can be defined as "*shared, distributed ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible — a house, a car, cash, land — or intangible like intellectual property, such as patents, copyrights, or branding*." [24]. This ledger information operates with encrypted data to implement identification, authentication, and authorisation of access to information. Integrity and trust on data, which is in the information systems, is the main objective of blockchain technology. Blockchain is a technological tool to comply with data integrity, in terms of its completeness, correctness, and free of contradiction, in distributed software systems. Distributed software systems are a number of independent computers that cooperate with each other in numerous informational transactions, without having a centralised computer to control or monitor those transactions. In a centralised system only one computer can control all the information occurred in a specific context or network. In our everyday life economy, we know that transactions should not be in only one computer to prevent fraud risk, but rather in multiple computers. For this reason, companies use decentralised information systems. Within this decentralised system, ownership of information must be authenticated, the ownership proof has three elements: (1) the identification of the owner, (2) the identification of the object being owned, and (3) mapping the owner with the correspondent object. This object and the mapping to its owner is maintained in a ledger, corresponding to a proof of ownership. Next figure represents the ownership concepts used to certify and proof property.

Information owner access is maintained through the usage of asymmetric cryptography during the data transaction. In this process data is protected from being accessed by unauthorised individuals. The asymmetric cryptography is composed by two complementary keys (private key & public key). The private key protects data by cypher text, a function which transforms any kind of data into a number of fixed length (hash), this process is named encryption. The public key turns cyphered text back into useful data, this part of the process is named decryption. In each of these processes, and for every one of them, blockchain

produces a hash, so that data is linked with the produced hashes that link each piece of data with another piece of data, a chain. Blockchain use asymmetric cryptography to identify accounts (user accounts correspond to the public cryptographic key), and to authorize transactions. All these transactions are kept.

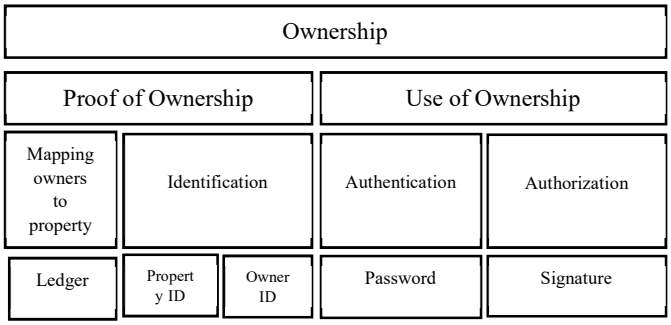

Figure 1: Concepts of ownership [27]

Blockchain means different things to different background people [24] [27]. For some authors blockchain is defined as a data structure, for others is an algorithm, for others can be defined as a suite of technology, and even for others blockchain can be a group of systems that communicate peer-to-peer within a common application area [27]. Drescher [27] defines blockchain as a distributed ledgers system, which uses an algorithm for computers to communicate with each other with cryptographic and security technologies to achieve and maintain data integrity.

In October 2008, Satoshi Nakamoto published a paper where he introduced the concept of a decentralised trustless peer-to-peer digital currency called Bitcoin, the first cryptocurrency, that was not issued and backed by a central authority, but by automated consensus among networked users [5]. The backbone of Bitcoin is the blockchain technology, a distributed ledger which contains the details for every record processed since the very first one. The validity and authenticity of each transaction are protected by digital signatures resorting to cryptography, thus the denomination cryptocurrency.

The way the bitcoin blockchain works is represented in a simplified manner in the Fig. 2.

In the bitcoin blockchain, the proof-of-work methodology is used to guarantee the validity of the ledger's transactions. It demands cryptographic puzzles, with increasing difficulty, to be solved by using electricity and computational power to mine a new block of transactions recorded on the blockchain. When the puzzle is successfully solved, a new block on the chain is mined, a predefined number of coins is distributed to the miner, as well as the fees associated with the transactions in the block. This block integrates the transactions that have been made and broadcasts them through the network to be approved.

While with fiat money, currency backed by governments, it is possible to easily see and distinguish money, with cryptocurrencies is not so easily perceptible.

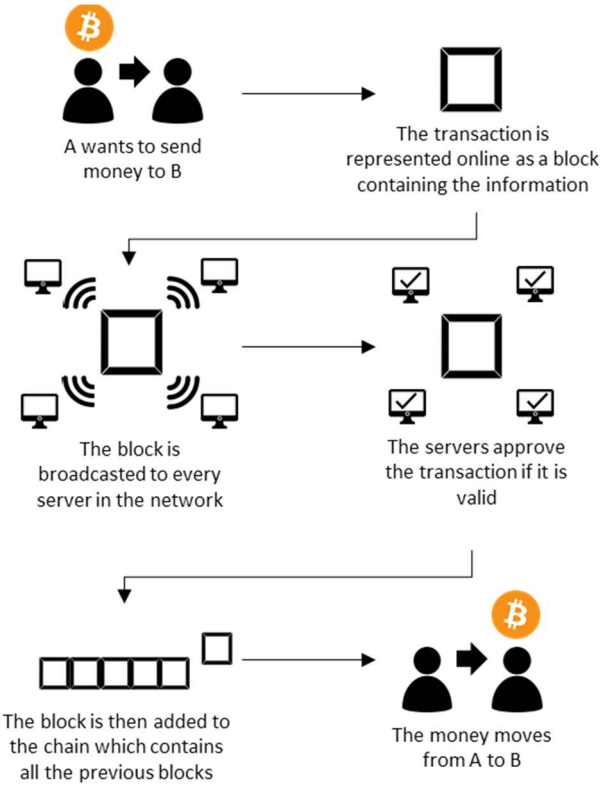

Figure 2: How does a transaction in the blockchain work?

To understand better, it is necessary to comprehend how the cryptography on the bitcoin blockchain works. Digital signatures are produced by using hash functions and encrypted resorting to a private key. This key is used to authenticate and authorise transactions in the bitcoin network, confirming the ownership of the bitcoins in each address, which identifies senders and receivers of transactions. The public key is used in the creation of bitcoin addresses by a digital application known as wallet [6]. From a user perspective, in a transaction, the sender must know the address of the receiver and inputs merely the desired amount to transfer.

III. PROOF-OF-WORK VS. PROOF-OF-STAKE

Other methodologies can also be used instead of proof-of-work. Proof-of-stake is one example of them. In this methodology, instead of having to use electricity and computational power to validate transactions, the new block creator is chosen in a deterministic way based on the stake, usually cryptocurrencies, he is willing to allocate to the blockchain [7]. One of the biggest criticisms to proof-of-work blockchains, such as bitcoin, is the massive energy consumption it takes to validate transactions. Currently, it is estimated the bitcoin blockchain consumes approximately 53 TWh per year, more than the annual consumption of some countries [8]. Proof-of-stake can be seen as a solution to this problem and the basis of present and future blockchains as well as being more secure and reducing the risk of centralisation.

Regarding the security of the blockchains, in proof-of-work methodology, it is necessary to have at least 51% of all the computational power on the blockchain to manipulate the information that exists there. This is virtually impossible and incredibly costly. In the bitcoin blockchain, it never happened. In proof-of-stake, it is necessary to have at least 51% of all the currency, meaning that, in both scenarios, the cost to hack the blockchain itself is incredibly high and much higher than the benefits of it. The issues here are the fraud instances that cannot be entirely eradicated such as phishing attacks, transactions to wrong addresses, loss of private key or exchanges account hacking for example. The successful adoption of blockchain is highly dependent on the security of the underlying environment.

The summary of three most relevant dimensions for comparing two methods can be seen in Table I.

TABLE I. COMPARISON BETWEEN PROOF-OF-WORK AND PROOF OF STAKE

	Proof-of-work	**Proof-of-stake**
Power consumption	Huge amounts of electricity required to secure the blockchain due to the processing needed.	Much lower amounts of electricity required to secure the blockchain.
Security	Required to have more than 50% of the processing power to hack.	Required to have more than 50% of the stake (coins) to hack. Can be more expensive to hack due penalties defined in the protocol such as loss of the stake.
Risk of centralisation	There is a risk of having mining pools, group of miners working together, controlling vast amounts of mining power. Currently, three different mining pools control more than 50% of the mining power [9].	Lower risk due to economies of scale being less of an issue. Not dependent on mining equipment.

IV. BLOCKCHAIN CONCEPT EVOLUTION

The blockchain concept is usually associated with bitcoin, but this technology has many other applications beyond payments when there is the need for an accurate record. Whereas blockchain 1.0 is for the decentralisation of money and payments, blockchain 2.0 is for the decentralisation of markets more generally and contemplates the transfer of many other kinds of assets, beyond currency, using the blockchain. Blockchain 2.0 protocols either use the Bitcoin blockchain or create their separate blockchains [10]. The most known example of a blockchain 2.0 is Ethereum, established in 2014. It is a project which attempts to build technology on which all transaction-based state machine concepts may be developed [11], this allows developers to create their decentralised applications and define their own set of rules to validate the transactions, this is also known as smart contracts. This concept was first introduced by Nick Szabo in the article "Smart contracts: building blocks for digital free markets" [12] in 1996, but only nowadays, with the widespread adoption of cryptocurrencies, it is possible to observe concrete use cases. It is already being adopted in areas such as authorship and ownership, commodities, data management, gaming, energy, government, IoT, market forecasting, media, real estate, social networks, supply chain, among many others. It is only logical to think a ledger that is secure and resistant to modification, where it is possible to store all kind of pre-defined information, can be used in the auditing environment.

Blockchains can also be considered public or private. Public blockchains are the ones anyone can access and use, like the bitcoin blockchain. Private blockchains are used within an organisation or consortium where only people with permission can access and use it, meaning they are more like databases with cryptography to secure it, this means they are not entirely decentralised and can be easily changed by the known interested parties. The transactions can be much cheaper due to the need to be validated by few trusted nodes with high processing power, existing faults on the nodes can be quickly addressed, and the level of privacy can be greater comparing to public blockchains. There are areas where it makes more sense to have private blockchains such as in supply chain due to the need of efficiency, transparency to authorised parties and level of consistency to minimise errors throughout the supply chain system [13].

The following figure summarises the key concepts of blockchain for business [24].

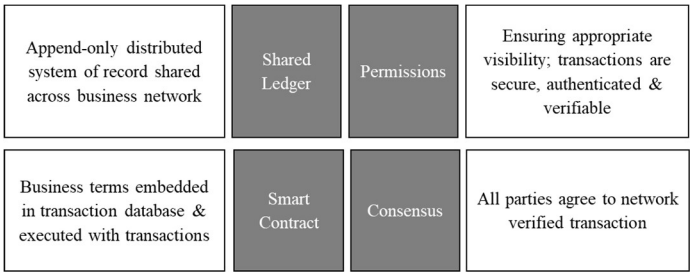

Figure 3: Blockchain key concepts for business [24]

Shared ledger is a blockchain business solution that prevents duplicate transactions in every node of the network. There is only one source of truth which is shared among the participants, through replication (meaning that each participant has a duplicate copy of the shared ledger). Replication eliminates the need to occur in extra costs of duplication and creation of as many ledgers as many as the participants' numbers because they get a copy. Blockchain can be permissioned or permissionless, permissions assure the access to certain participants, who have the authorisation to view some transactions, while auditors may have permission to access more transactions to assure the process. Consensus can be used when all the network parties are known and trusted. Therefore transactions can be approved by a consensual agreement (proof of stake), whereas proof of stake is more adequate to the private blockchain, proof of work is more adequate to the public blockchain. In a smart contract, transactions can be made automatically in part, or have self-enforced clauses to reduce costs. Usually, those self-enforced clauses are provided by the application of the law.

V. BLOCKCHAIN IN AUDITING

The blockchain is a technology which is distributed to store data, and it has the following properties: immutability, append-only, ordered, time-stamped, open and transparent, secure, and eventually consistent [27]. According to blockchain properties, this technology can be applied in several situations, when needing to guarantee the proof of existence, nonexistence, time order, identity, authorship, and ownership. Auditing is a systematic, independent and documented process to obtain evidence by evaluating it objectively to monitors whether the audit criteria are fulfilled [14]. Blockchain can be used when there is the need of compliance of businesses activities with the regulations because it ensures an audit track.

The blockchain can be used as a basis for verification of reported transactions. An example might be where, instead of asking clients for bank statements or sending confirmation requests to third parties, auditors can easily verify the transactions on publicly available blockchain ledgers. The automation of this verification process will drive cost efficiencies in the audit environment [15]. What distinguishes using the blockchain from other forms of data timestamping and authentication, is that documents and other sets of data in the blockchain are decentralised proof. Assuring that data can't be erased or modified by anyone, not by your own company nor competitors, third parties or governments [16], which can help on one of the biggest issues when conducting audits, frauds and the detection of it.

According to a study in 2011 [17], hidden documents/information, altered documents, fake documents and collusion with third parties total 81% of evidence schemes, through which management creates or hides evidence to conceal the fraud. Premature revenue recognition, fictitious revenues, overvalued assets and understated expenses, omitted or understated expenses/liabilities total 78% of account schemes, through which management perpetrates fraud by manipulating account balances or disclosures. Having a blockchain system where accountants must input the companies' financial statements, in a secure and resistant to modification ledger, that could be used in real time would have a considerable positive impact in the reduction of that kind of frauds.

There are also external forces to consider when studying the implementation of blockchain in auditing. One example is the changes in regulation such as General Data Protection Regulation (GDPR) that aims to protect all EU citizens from privacy and data breaches. This will force companies to change how they keep sensitive personal data in their systems and may affect the records of financial transactions, debit and credit memos, invoices and receipts for example. Throughout the final version of the regulation released in the 6th of April 2016 [18], it is suggested multiple times to use cryptography to encrypt sensible data. Using a private blockchain, where only parties with authorisation can access, to keep these records safe may be an option.

VI. COMPUTER ASSISTED AUDIT TOOLS AND TECHNIQUES, CAATTS

CAATTs stands for; computer-assisted audit tools and techniques, used in auditing context. Blockchain technology can be included in those technologies [19] [25] [26 although it addresses not only auditing, blockchain as auditing tools can perform a valuable input in auditors' work [28] [29] [30] [33]. Therefore, blockchain must be well adapted with the existing solutions for a successful implementation but, in fact, some tools and techniques were still not accepted by auditors such as artificial intelligence which is, on pair with blockchain, a megatrend for the next few years. This proves a challenge in the transformation [32] of the existing business practices, and with self-verifiable audit trail models [31].

Some of the emerging technologies include data mining techniques and fraud detection, big data and analytics, cloud auditing and bring your own device (BYOD) and audit tools [19]. All these technological innovations mean the audit profession will need people who have accounting skills but who are also extremely IT literate due to a future enabled by technological platforms. In some years is expected that fully automated audit reports, where information is uploaded in the blockchain and artificial intelligence extracts and analyses it in real time, might be an example of this technological evolution.

VII. SOME EXISTING AND FUTURE BLOCKCHAIN SOLUTIONS

Nowadays there are already companies trying to disrupt the auditing environment resorting to the blockchain technology to develop their own solutions.

Factom is one of the most well-known examples and uses a method to secure the blockchain like the proof-of-stake. This company has two different products available: Factom Harmony that converts document management solutions into a blockchain based document platform that eliminates lost documents reduces audit time and prevents costly disputes; and dLoc, a document authentication solution that lets secure physical documents on the blockchain. Factom's cryptocurrency is named as "Factoid," which is a token used to purchase entry credits, and used to constitute entries into the Factom blockchain, for the services offered by the platform. They are used to maintain the server's infrastructure and reward server operators for running the system. Factoids can also be traded against other cryptocurrencies as well [20].

The policy and reward mechanism in Factom is similar to proof-of-stake. Factom differs from most proof-of-stake systems in that only a subset of users' stake is recognised. Only value which has been committed to the system has a voting share [21]. Other companies that will launch their solutions this year are Libra and Verady.

Libra wrote their goal was "*to help auditors expand their ability to offer assurance services to any blockchain platform and change the timing of their service from post-transaction to real-time. To create software that, extracts, normalises, monitors, notifies, analyses, and reports on data against pre-set rules, notifications, and control frameworks that are specific to specific auditors' approaches and methodologies*" [22]. Verady, asserts that "*a gap exists in terms of blockchains not holding the information in a form that accountants, auditors and other financial professionals can access, understand or use*." VeraNet is the Verady's blockchain asset assurance network, which objective is to address assurance. The basis of this assurance is

to guarantee these assets information veracity. The VeraNet provides the bond blockchain-based crypto-assets and the traditional financial ecosystem. This link is designed to manage the complexities of blockchain technology to deliver concrete, standardised reports, and to ensure that data is reliable by conventional financial institutions [23].

VIII. Conclusions

It is undoubtful that the blockchain technology can have a profoundly positive impact on the auditing environment and bring much-needed optimisation to the existing processes.

With the increase of the knowledge around it and the awareness of its importance, companies are starting to develop solutions for many different areas where trustworthy and secure data is crucial and are beginning to see proof-of-stake blockchains as a viable alternative to the proof-of-work blockchains. Auditing is one of these areas, and it is already possible to use solutions developed by Factom and in the future by Libra and Verady.

It is also important to consider how to match blockchain technology with other emerging technologies such as computer Assisted Audit Tools and Techniques (CAATT). Like big data and analytics that are enabling auditors to assess increasing volumes of data as well as continuous monitoring and artificial intelligence audit software, and also non-technological forces, the growing complexity of the regulatory landscape for example.

Having the endorsement of official entities such as the Certified Public Accountants Associations would be an essential boost towards the adoption of the blockchain technology, it could be part of the review engagement for example.

The truth is there is still a long way to go until widespread adoption in this area is made. Investment is currently outpacing the offer and know-how. Accountants and auditors are not yet familiarised with this technology and how can they use it. It is necessary that companies dedicate innovation teams to make the transition from the standard auditing to the optimised auditing using blockchain technology. In such a fast-paced technological environment it is crucial to keep an eye on disrupting technologies such as blockchain to be successful.

References

[1] Cision, "Worldwide Blockchain Technology Market is Anticipated to Exhibit a CAGR of 58.7% Between 2016 and," Cision PR Newswire, 2018. [Online]. Available: https://www.prnewswire.com/news-releases/worldwide-blockchain-technology-market-is-anticipated-to-exhibit-a-cagr-of-587-between-2016-and-2024-elimination-of-third-parties-improves-demand-and-security-of-online-transactions--tmr-611067345.html. [Accessed: 28-Feb-2018].

[2] R. Meszaros, D. Adachi, H. Dharamsi, B. Yetiskin, and P. Thomas, "Blockchain Technology: How banks are building a real-time global payment network," *Accenture Mobility*, 26-Oct-2016.

[3] W. Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. John Wiley & Sons Inc, 2016.

[4] "The Hottest Freelance Skills on Upwork: Q3 2017," *Upwork Blog*, 02-Nov-2017. [Online]. Available: https://www.upwork.com/blog/2017/11/freelance-skills-upwork-q3-2017/. [Accessed: 04-Mar-2018].

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Oct-2008.

[6] P. Martins, *Introdução à Blockchain: Bitcoin, criptomoedas, smart contracts, conceitos, tecnologias, implicações*, 1st ed. Lisboa: FCA, 2018.

[7] D. Larimer, "Transactions as Proof-of-Stake," Nov-2013.

[8] Digiconomist, "Bitcoin Energy Consumption Index," Digiconomist, 2018. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption. [Accessed: 03-Mar-2018].

[9] "Hashrate Distribution," *Blockchain.info*. [Online]. Available: https://blockchain.info/pools. [Accessed: 04-Mar-2018].

[10] M. Swan, *Blockchain: Blueprint for a new economy*. Sebastopol, California: O'Reilly, 2015.

[11] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger (revision)," Apr-2017.

[12] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets," *Extropy*, 1996.

[13] J. Donaldson, "Public vs Private Blockchain In A Wide World Of Unique Applications," Aug-2017.

[14] "Guidelines for auditing management systems (ISO 19011:2011)," *BSI Standards Publication*, 2011.

[15] S. Psaila, "Blockchain: A game changer for audit processes."

[16] C. Findlay, "Decentralised and inviolate: the blockchain and its uses for digital archives," *Recordkeeping Roundtable*, Jan-2015.

[17] L. Gao and R. Srivastava, "The Anatomy of Management Fraud Schemes: Analyses and Implications," *Indian Accounting Review*, Jun-2011.

[18] Council of the European Union, "General Data Protection Regulation 5419/1/16 REV 1." Apr-2016.

[19] I. Pedrosa and C. Costa, "Financial auditing and surveys: How are financial auditors using information technology?: An approach using expert interviews," 2012. in Proceedings of the Workshop on Information Systems and Design of Communication, New York, NY, USA, 2012, pp. 37–43

[20] J. Buntinx, "What Is Factom?," *The Merkle*, Feb-2018. .

[21] P. Snow, B. Deery, J. Lu, D. Johnston, and P. Kirby, "Factom: Business Processes Secured by Immutable Audit Trails on the Blockchain," Nov-2014.

[22] J. Drane, "Wait, blockchains need audited?!?," Dec-2016. [Online]. Available: https://www.linkedin.com/pulse/wait-blockchains-need-audited-jeremy-drane/. [Accessed: 28-Feb-2018].

[23] STUDIOS, "Verady's Vision for Asset Audits and Verification," *Bitcoin Magazine*. [Online]. Available: https://bitcoinmagazine.com/articles/veradys-vision-asset-audits-and-verification/. [Accessed: 28-Feb-2018].

[24] M. Gupta, *Blockchain For Dummies*, John Wiley & Sons, Inc, 2017

[25] I. Pedrosa and C. J. Costa, "New Trends on CAATTs: What Are the Chartered Accountants' New Challenges?," in Proceedings of the International Conference on Information Systems and Design of Communication, New York, NY, USA, 2014, pp. 138–142.

[26] I. Pedrosa and C. J. Costa, "Statutory Auditor's Profile and Computer Assisted Audit Tools and Techniques' Acceptance: Indicators on Firms and Peers' Influence," in Proceedings of the International Conference on Information Systems and Design of Communication, New York, NY, USA, 2014, pp. 20–26.

[27] D. Drescher, Blockchain basics. Springer, 2017.

[28] K. Fanning and D. P. Centers, “Blockchain and Its Coming Impact on Financial Services,” Journal of Corporate Accounting & Finance, vol. 27, no. 5, pp. 53–57, Jul. 2016.
[29] D. Broby and G. Paul, “The financial auditing of distributed ledgers, blockchain and cryptocurrencies,” Journal of Financial Transformation, vol. 46, 2017.
[30] G. Wolfond, “A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada’s Public and Private Sectors,” Technology Innovation Management Review, vol. 7, no. 10, 2017.
[31] S. Gupta, A Non-Consensus Based Decentralized Financial Transaction Processing Model with Support for Efficient Auditing. Arizona State University, 2016.
[32] C. Firestone, “Continual Disruption,” Aspen Institute, Washington, DC, USA, 2015.
[33] I. Pedrosa, R. M. Laureano, and C. Costa, “Motivações dos auditores para o uso das Tecnologias de Informação na sua profissão: aplicação aos Revisores Oficiais de Contas,” Revista Ibérica de Sistemas e Tecnologias de Informação, pp. 101–118, 2015.