Bitcoin and Blockchain Security
A Study in Misconceptions

Svein Ølnes
Western Norway Research Institute, Sogndal, Norway
sol@vestforsk.no

Abstract. Since its inception in 2008/2009 Bitcoin and its underlying blockchain technology has been thoroughly studied and the number of scientific articles has grown substantially. Irrespective of the research field, most of the articles have an introduction to blockchain technology where the key parts of it are described. However, many authors make misconceptions about the security model of Proof of Work-based blockchains when describing it. The most prevailing misconception is the confusion of the concepts tamper evidence and tamper resistance. There are also other misconceptions regarding blockchain security. This article presents the result of an extensive literature review of blockchain publications indexed by Web of Science where we study how the security of blockchains is described. We find that almost a third of the studied papers are misleading when describing the security of the technology.

Keywords: Blockchain security, Proof of Work, Tamper evidence, Tamper resistance

1 Introduction

Bitcoin [1] was the first successful attempt to create a secure way of reaching consensus in an open and distributed system with no central authority. A vital part of the solution was the combination of Proof of Work (PoW) as a consensus method and economic incentives via the built-in digital currency [2].

Bitcoin's security features are many, and on different levels. Although Bitcoin and its blockchain technology is quite concrete, at least compared to other disruptive technologies of today, it is also difficult to grasp and can lead to misconceptions and myths [3].

This paper concentrates on the security aspects of public, permissionless blockchains that use the PoW consensus method and we use Bitcoin as the primary example of such a blockchain. PoW-based blockchains are still the most common type of permissionless blockchains. Although Bitcoin is used to describe the blockchain technology the issues discussed here are also valid for other PoW-based blockchains.

Information security is a comprehensive field with a breadth of topics. The international standard, ISO/IEC 27002 [4], defines information security as the preservation of the confidentiality, integrity and availability of information, the so-called CIA triangle. Whitman and Mattord [5] define information security as "the protection of information and its critical elements, including the systems

and hardware that use, store, and transmit that information". However, as Von Solms and Van Niekerk [6] point out information security has evolved from a strictly technical focus to also comprise non-technical aspects, and also that the original three aspects have been expanded with new aspects.

Blockchain security is a good example of the importance of a broader understanding of information security. The main security challenges in blockchain technology are, of course, related to cryptography and consensus methods, where the latter is comprised of both technical security and game-theoretical social actions and considerations. This paper does not cover hardware issues that are also part of the total blockchain security. We will discuss blockchain security on the blockchain level (how blocks can be manipulated) and relate this to the key aspects of information security.

For the first two categories, confidentiality and integrity, the concepts tamper evidence and tamper resistance are especially important when discussing blockchain technology. It is important to understand the difference between these concepts to understand blockchain security properly. Tamper evidence is the feature of disclosing attempts to manipulate data, in our case transaction data, preferably in an easy and obvious way. Analogies of physical tamper evident design mechanisms are many, e.g. seals that have to be broken, wires that have to be cut, or coatings that have to be removed [7]. The tamper evidence must be clearly visible and cannot be reversed by the malicious actors without it being easily noticed (ibid.).

Tamper resistance, on the other hand, is the ability of a product or system to prevent malicious attacks to succeed. Techniques to prevent successful attacks can range from physical protection mechanisms, hardware design, and software design (ibid.). In our case software design in combination with game theory is the key technique to avoid malicious attacks to be effective.

The research question guiding the work was: How does impactful papers on blockchain technology describe the security? The underlying assumption is that a substantial part of scientific papers has an incorrect description. A second research question was also formulated during the work: "Does the research field influence the correctness of the technology description?".

Although blockchain technology is quite concrete there seems to be some misconception regarding the security model of blockchains based on the PoW method. To the best of our knowledge, this is the first survey of how blockchain technology is described in academic literature and what misconceptions exist therein.

2 Bitcoin and Blockchain Security

A public, permissionless blockchain system such as Bitcoin consists of several layers, as shown in the figure below [8]. This paper limits the security

discussion to the consensus layer, especially focusing on the consensus method and its block generation.

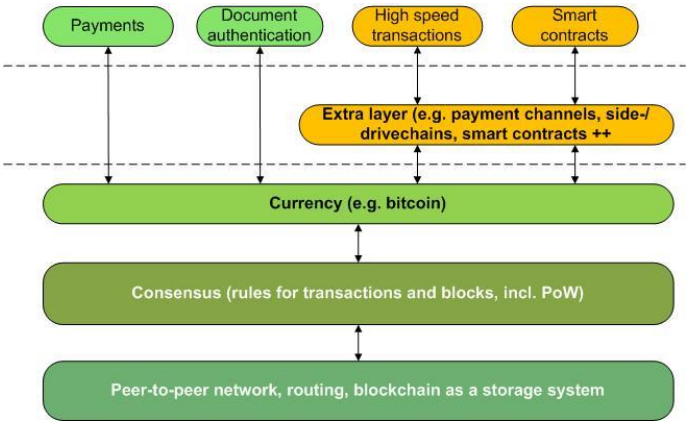

Fig. 1: The layered architecture of public, permissionless blockchains [8].

The PoW method in Bitcoin consists of calculating the hash of the fields in the block header plus information in the coinbase transaction [2]. The hash value should meet a predefined target; that is, it should be less than a given value (ibid.).

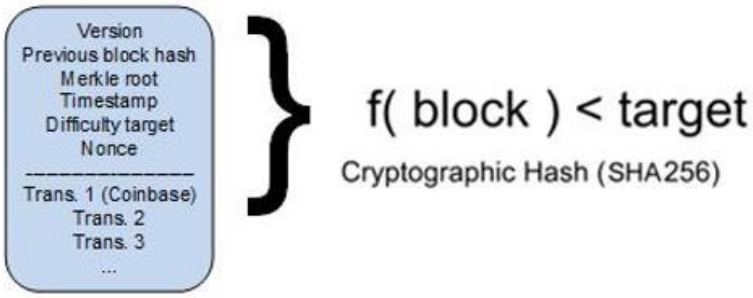

Fig. 2: The PoW process to find a hash value less than the current target (slightly revised from [9])

Since the block hash also contains the hash of the previous block ("Previous block hash" in the figure), any changes to the previous block will generate a new hash and therefore be easily spotted. This is what makes blockchains tamper evident. It is easy to observe attempts to change a previous transaction. However, this does not prevent manipulation of transactions and attempts of double-spending.

Tamper resistance, on the other hand, is the ability of a system to withstand attack from adversaries [7]. In Bitcoin, and other blockchains based on the PoW consensus method, it is the work needed to be able to append a new block to the blockchain that prevents adversaries to manipulate transactions and therefore prevents double-spending and the ability to change the blockchain history. In Bitcoin work translates to use of electric energy to carry out computations. Tamper resistance is what eventually guarantees a blockchain's immutability.

A threat to the PoW method is the 51 % attack. If a malicious actor can muster more than half of the computing power in a PoW-based blockchain system, he/she can manipulate the blockchain by secretly mining new blocks with double-spending and then present the "shadow" blockchain at a certain time. The security of Bitcoin and other PoW systems is based on the premise that it will be more profitable to follow the rules than to try to break them and this is the game-theoretical part of the security model [2]. Note that the hash linking cannot prevent this type of attack.

Nodes accept or reject a new block. There is no "voting", as often is indicated. It all comes down to the consensus ruled the node's software is running [10]. If one node rejects a new block it means that this node is running a different version of the blockchain software and thus operates on a different blockchain. That can happen after a hard fork, which is a change to the software that is not backwards compatible and requires all the nodes to update [10]. There is a tendency to forget that software is what runs the blockchain, including the consensus rules.

Going back to the original key aspects of information security; confidentiality, integrity, and availability, confidentiality comprises both privacy and the security of private keys. Permissionless blockchains have great transparency and as such can be said to be weaker on this aspect of information security. It is important for this type of blockchain to be as open and transparent as possible because a lot of the necessary verification hinges on this. The pseudonymous nature of most permissionless blockchains will grant some privacy and thus give some prevention from transactions being traced to specific persons. However, this is still regarded as one of the main vulnerabilities of Bitcoin and other permissionless blockchains [11].

Integrity in blockchain technology most of all relates to the immutability property of blockchains. The description above shows that the immutability of blockchains has both a technical and social side and that game theory is important to understand the actions, both real and anticipated, from the stakeholders in the system.

Availability means that the blockchain must be up and running constantly to serve the users. The peer-to-peer architecture and the prevention of (D)DOS attacks help this. However, the number of full nodes is critical to obtain constant availability, as is the degree of decentralization of the blockchain [12]. A full node is a client that stores the entire history of bitcoin transactions (every

transaction by every user, ever), manages the user's wallets and can initiate transactions directly on the bitcoin network [2].

To sum up the security aspects of PoW-based blockchains the consensus method, in Bitcoin called Nakamoto consensus, is what prevents double-spending and makes the blockchain tamper resistant [13]. Hash-linking, on the other hand, makes the blockchain tamper evident in addition to providing a mechanism to traverse the blockchain.

3 Method

To answer the research question "How does impactful papers on blockchain technology describe the security?" we have conducted a systematic literature review to identify how current research treats this challenge. The review followed the guidelines provided by Kitchenham and Charters [14] on how to carry out systematic literature reviews in software engineering. The research is explorative in nature.

We chose the database collection of Web of Science (WoS) Core Collection and searched for the terms 'blockchain' and 'technology' in the title of the papers. WoS was chosen because it is a citation index that provides a very good coverage of the relevant science disciplines.

The search resulted in 2,270 papers as of mid-June 2020. The results of a search like this is a moving target and will vary with time. However, the results correspond well with Dabbagh et al.'s bibliometric study of blockchain literature based on WoS [15]. They found altogether 1,120 publications in the period 2013-2018 using the search phrase 'blockchain'.

We arranged the result set based on the number of citations the paper had. This was done because a higher citation frequency usually means higher relevance and more impact. The more impact a paper has, the more important it is that it has a correct description of the essential part of the blockchain technology, otherwise the risk of carrying mistakes over to new publications increases.

To be included in the final review the papers had to: (1) be peer reviewed, (2) have the term 'blockchain technology' or just 'blockchain' in the title, (3) be accessible in full-text, and (4) be written in English. A few papers in the result set (less than five) did not meet these criteria. The complete list of results is given in the appendix.

We picked the 100 first papers in the list of results and studied the description of blockchain technology security in each of them. Based on the description the papers were labelled one of the following three categories: (1) Correct description, (2) Ambiguous or unclear description, or no description at all, and (3) Wrong or misleading description. Examples from papers in the different categories are given in section 4.

We have limited the discussion of blockchain security to PoW-based permissionless blockchains. However, the description of the technology in all the analyzed papers was based on the PoW consensus method, either explicitly or implicitly.

We also categorized the papers according to research field, in the following domains: (1) Technology, (2) Energy and environment, (3) Economy and Finance, (4) Business Management (including Supply Chain Management), (5) Governance and e-government, and (6) Health care. The research fields were constructed through a bottom-up process where the content of the paper indicated the research field.

4 Analysis of Blockchain Papers

As mentioned in the previous section we analyzed 100 blockchain-related research papers from the Web of Science index, sorted after the number of citations, see appendix.

In evaluating the papers, the section of blockchain technology description was read and the papers categorized in one of the three categories 'Correct', 'Partly correct', and 'Incorrect'. Papers were judged "Correct" if they had a description of the technology that was in line with the description given in section 2. The category 'Partly correct/No description' was attributed to papers that did not explicitly have a wrong description of the technology, but nevertheless had ambiguous statements and would leave the reader with a somewhat improper understanding of the technology. Also, publications that did not describe the security of blockchain technology were placed here. The final category, "Incorrect", was used for papers that had a clear misunderstanding or false description of the technology. Above all, confusing tamper evidence and tamper resistance was the most common error.

Table 1. Result of analysis of 100 papers on the description of blockchain technology.

Category	Correct	Partly correct/No description	Incorrect
Number of papers	36	34	30

Note that the table above only reflects whether papers on the whole have a correct or description of the technology or not. Thus the total number corresponds to the number of papers evaluated.

Other errors and misunderstandings in the papers evaluated were (a) Incorrect description of private and public keys, and their roles, (b) Confusing

statements such as “majority of nodes need to approve the new block”, (c) Does not recognize the importance of PoW as the major security mechanism for integrity and degree of immutability, and (d) Vague or no description of blockchain technology and/or security at all. The table below shows the distribution of the different misconceptions.

Table 2. Prevailing misconceptions in the reviewed papers.

Type of misconception	No. of papers
Confusing tamper evidence and tamper resistance by hash linking securing immutability	15
Does not recognize the importance of the consensus method for security and immutability	9
Weak, diffuse, or misleading description	4
Confusing and/or wrong description of the roles of public and private keys	2

A couple of quotes serve to illustrate the typical confusing of tamper evidence and tamper resistance:

> “*Because every block is securely linked to the block preceding it using the hash, malicious changes are prevented from being made to the blockchain ledger. The immutability is a key property of blockchain.*” [16]

> “*Once these blocks are connected within a chain, they become immutable: they cannot be changed or deleted by a single actor.*” [17]

There are, of course, many papers with a precise description of the security in PoW blockchains, e.g.:

“*To form a block, the miner must solve this puzzle, consuming both operational resources and capital for each block—this wasting of resources is part of the checks in the design that ensure security and financial integrity in the decentralized consensus system, and the solution is called proof of work (PoW)... The security of Bitcoin's system is based on this longest-chain rule.*” [18]

Furthermore, the sample of 100 papers were categorized by research field in the categories shown in the table below.

Table 3. Results of blockchain technology description sorted by topic.

Topic	Correct	Partly correct	Incor-rect	Sum
Technology (T)	12	13	3	28
Energy and Environment (EE)	3	2	4	9
Economy and Finance (EF)	8	1	5	14
Business Management (SCM ++) (BI)	6	7	13	23
Governance and e-Gov. (G)	4	4	1	9
Health care/e-Health (H)	3	7	4	14
Sum	36	34	30	100

The table above shows the results of the analysis categorized by topic of the papers. We formulate a H0 hypothesis that says the degree of correct or incorrect papers will be the same for all research fields. A Chi-squared test gives the result 19.463577, with 10 degrees of freedom and a p value of 0.0347546. The H0 hypothesis therefore has to be rejected. The research field does influence how the blockchain technology is described. Not surprisingly the technological research field show a substantial lower number of incorrect papers than anticipated in H0. On the other end of the scale the research field Business management, with mostly SCM-related papers, show the greatest deviation from the expected number of incorrect papers. While the results seem to align with what we would expect initially, we should bear in mind that the sample here is not perfectly stochastic since Web of Science contains journals that are pre-screened before inclusion. On the other hand, the pre-screening should be a guarantee for higher quality and thus more influential papers.

5 Discussion

This paper started out with the research question “How does impactful papers on blockchain technology describe the security?” with an underlying assumption that there were misconceptions in the descriptions. The analysis of results shown in the previous section has made it clear that the initial assumption was legitime as almost a third of the evaluated papers describe the blockchain technology in an incorrect and even erroneous way. The prevailing misconception is that the hash linking of blocks in a blockchain guarantees immutability.

We also categorized the papers into research fields to examine whether the specific field could explain some of the main results. We had to reject the H0

hypothesis that all research fields had the same relative distribution of correctness. The technology field stood out with much fewer incorrect papers and the business operations, with mostly supply chain management-based papers, had a greater number of incorrect papers. This is in line with what would be expected since the topic being investigated is highly technical. The reason for business-oriented papers, mostly SCM, being over-represented in the category of incorrect description is more difficult to explain. There is no obvious reason for papers in this research field to be weaker in technology description and understanding than e.g. economy or governance.

The findings in this research give reason to worry about possibly failed investments and system developments based on blockchain technology. Even though permissioned blockchain systems have not been discussed in this work, failing to understand how consensus methods prevent successful attacks and manipulations also applies to these. It can be costly to underestimate the security threats both for permissionless and permissioned blockchains.

Our investigation has shown that of the three key aspects of information security; confidentiality, integrity, and availability, understanding how integrity is secured in blockchain technology poses the greatest challenge. The misconceptions in blockchain technology found in this work are almost solely connected to what secures the integrity, and especially the crucial distinction between tamper evidence and tamper resistance.

6 Conclusions and Further Research

The results shown in this paper should be a reminder that we need knowledgeable and qualified reviewers that understand the technology well. Blockchain technology is still fairly new and is still struggling to find its way into curriculums in the universities [19]. There is a need for educating researchers in all research fields and disciplines about the core properties and security of blockchain technology, especially at the consensus layer.

Although there are different types of blockchains, permission-wise or consensus-wise, there are some key elements that underpins almost all of them. The distinction between tamper evidence and tamper resistance and the effects on the immutability of the blockchain is one of these. It is crucial to understand this difference and its consequences to fully understand the security and vulnerability of blockchains. A study of the Bitcoin blockchain is a good way to understand the blockchain technology.

Both reviewers of blockchain-related papers and editors of journals where these eventually are published should be aware of the misconceptions that are identified in this paper. They should assure that the reviewers are confident and

knowledgeable with blockchain technology such that common misconceptions can be avoided.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Consulted*, vol. 1, no. 2012, p. 28, 2008.

[2] A. M. Antonopoulos, *Mastering Bitcoin - Unlocking Digital Cryptocurrencies*, 1st ed. San Francisco: O'Reilly Media Inc., 2014.

[3] C. R. Harvey, "Bitcoin myths and facts," *Available SSRN 2479670*, 2014.

[4] A. Standard, "ISO/IEC 27002," in *Informationtechnology-security techniques-code of practice for information security controls,(AS ISO/IEC 27002: 2015)*, 2015.

[5] M. E. Whitman and H. J. Mattord, *Principles of information security*. Cengage Learning, 2011.

[6] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, 2013.

[7] S. Ravi, A. Raghunathan, and S. Chakradhar, "Tamper resistance mechanisms for secure embedded systems," in *17th International Conference on VLSI Design. Proceedings.*, 2004, pp. 605–611.

[8] S. Ølnes and A. Jansen, "Blockchain technology as infrastructure in public sector: an analytical framework," in *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, 2018, pp. 1–10.

[9] CuriousInventor, *How Bitcoin Works Under the Hood*, (Jul. 14, 2013). Accessed: Aug. 25, 2020. [Online Video]. Available: https://www.youtube.com/watch?v=Lx9zgZCMqXE

[10] A. M. Antonopoulos, *Mastering Bitcoin: Programming the open blockchain*. O'Reilly Media, Inc., 2017.

[11] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 4, pp. 3416–3452, 2018.

[12] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016.

[13] J. Nijsse and A. Litchfield, "A Taxonomy of Blockchain Consensus Methods," *Cryptography*, vol. 4, no. 4, p. 32, 2020.

[14] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007.

[15] M. Dabbagh, M. Sookhak, and N. S. Safa, "The evolution of blockchain: A bibliometric study," *Ieee Access*, vol. 7, pp. 19212–19221, 2019.

[16] S. Angraal, H. M. Krumholz, and W. L. Schulz, "Blockchain technology: applications in health care," *Circ. Cardiovasc. Qual. Outcomes*, vol. 10, no. 9, p. e003800, 2017.

[17] Y. Wang, M. Singgih, J. Wang, and M. Rit, “Making sense of blockchain technology: How will it transform supply chains?,” *Int. J. Prod. Econ.*, vol. 211, pp. 221–236, 2019.
[18] I. Eyal, “Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities,” *Computer*, vol. 50, no. 9, pp. 38–49, 2017.
[19] S. Ølnes and S. J. Knutsen, “Blockchain Technology in Education–TheChallenge of Interdisciplinary Teaching,” in *Digital samhandling*, pp. 373–389.

Appendix

Title	Correct	Partly correct	Incorrect	Field
Where Is Current Research on Blockchain Technology?-A Systematic Review			x	T
Blockchain technology in the chemical industry: Machine-to-machine electricity market	x			EE
Blockchain distributed ledger technologies for biomedical and health care applications	x			H
Blockchain technology and its relationships to sustainable supply chain management		x		BI
The IoT electric business model: Using blockchain technology for the internet of things		x		T
Blockchain technology in the energy sector: A systematic review of challenges and opportunities	x			EE
Blockchain in government: Benefits and implications of distributed ledger technology for information sharing	x			G
Blockchain-based sharing services: What blockchain technology can contribute to smart cities			x	BI
When Intrusion Detection Meets Blockchain Technology: A Review	x			T
Blockchain Technologies: The Foreseeable Impact on Society and Industry			x	BI
The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy	x			BI
Trusting records: is Blockchain technology the answer?	x			G
Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology	x			H
Blockchain Technology Applications in Health Care			x	H
Blockchain Technology in Business and Information Systems Research			x	BI
Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?		x		G
Blockchain Technology in Finance			x	EF
The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy	x			EF
Making sense of blockchain technology: How will it transform supply chains?			x	BI
Blockchain Technology Use Cases in Healthcare		x		H

Banking on Blockchain: Costs Savings Thanks to the Blockchain Technology	x			EF
Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies			x	EE
How Can Blockchain Technology Disrupt the Existing Business Models?			x	BI
Blockchain Technology in Healthcare: A Systematic Review			x	H
Blockchain technology for enhancing supply chain resilience		x		BI
The outlook of blockchain technology for construction engineering management		x		BI
Fraud detections for online businesses: a perspective from blockchain technology		x		EF
Blockchain Technology in the Oil and Gas Industry: A Review of Applications, Opportunities, Challenges, and Risks	x			BI
The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin	x			EF
A systematic literature review of blockchain-based applications: Current status, classification and open issues	x			BI
When Mobile Blockchain Meets Edge Computing	x			T
A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain		x		T
Blockchains for Business Process Management - Challenges and Opportunities		x		BI
Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems		x		H
A blockchain future for internet of things security: a position paper		x		T
FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data		x		H
Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability			x	H
Blockchain and value systems in the sharing economy: The illustrative case of Backfeed	x			EF
Blockchain for AI: Review and Open Research Challenges			x	T
Energy Demand Side Management within micro-grid networks enhanced by blockchain		x		EE
Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA			x	BI
Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application			x	EE
A Decentralized Privacy-Preserving Healthcare Blockchain for IoT	x			H

A Survey about Consensus Algorithms Used in Blockchain	x			T
Future challenges on the use of blockchain for food traceability analysis	x			BI
Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks		x		T
A survey on the security of blockchain systems	x			T
A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems		x		T
E-residency and blockchain		x		G
Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda			x	G
Blockchain and Cryptocurrencies: Mode Techniques, and Applications	x			EF
Blockchain technology for improving clinical research quality			x	H
Blockchain Technologies for the Internet of Things: Research Issues and Challenges	x			T
Blockchain tokens and the potential democratization of entrepreneurship and innovation			x	EF
An Empirical Study on Modeling and Prediction of Bitcoin Prices With Bayesian Neural Networks Based on Blockchain Information			x	EF
Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities	x			EF
Understanding the Blockchain technology adoption in supply chains-Indian context		x		BI
Toward open manufacturing A cross-enterprises knowledge and services exchange framework based on blockchain and edge computing			x	BI
The mean-variance approach for global supply chain risk analysis with air logistics in the blockchain technology era		x		BI
Research on agricultural supply chain system with double chain architecture based on blockchain technology			x	BI
Understanding blockchain technology for future supply chains: a systematic literature review and research agenda			x	BI
Applications of Blockchains in the Internet of Things: A Comprehensive Survey		x		T
A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks		x		T

MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain		x		H
Copyright in the blockchain era: Promises and challenges		x		G
Digital enablement of blockchain: Evidence from HNA group			x	BI
LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem			x	EE
Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends	x			G
Blockchain's adoption in IoT: The challenges, and a way forward	x			T
Blockchain based hybrid network architecture for the smart city		x		T
Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases			x	BI
The impact of the blockchain on the supply chain: a theory-based research framework and a call for action			x	BI
Tamper-Resistant Mobile Health Using Blockchain Technology		x		H
Analysis and outlook of applications of blockchain technology to equity crowdfunding in China			x	EF
Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform			x	T
Blockchain technology: A panacea or pariah for resources conservation and recycling?		x		EE
Blockchain: The Evolutionary Next Step for ICT E-Agriculture		x		BI
Computation Offloading and Content Caching n Wireless Blockchain Networks With Mobile Edge Computing	x			T
Blockchain characteristics and consensus in modern business processes	x			BI
Governance on the Drug Supply Chain via Gcoin Blockchain		x		H
To Blockchain or Not to Blockchain: That Is the Question	x			EF
A Privacy-Preserving Trust Model Based on Blockchain for VANETs		x		T
A survey on privacy protection in blockchain system	x			G
Blockchain Practices, Potentials, and Perspectives in Greening Supply Chains			x	BI
Blockchains and the economic institutions of capitalism	x			EF
Blockchain and the related issues: a review of current research topics		x		T
Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector		x		H
Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law		x		G
A Blockchain Research Framework What We (don't) Know, Where We Go from Here, and How We Will Get There	x			BI

A blockchain-based smart grid: towards sustainable local energy markets	x			EE
A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT		x		T
A Survey on Security and Privacy Issues of Bitcoin	x			T
Blockchain and IoT Integration: A Systematic Survey	x			T
Blockchain application and outlook in the banking industry			x	EF
Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids			x	EE
Blockchain challenges and opportunities: a survey	x			T
Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT	x			T
BlockChain: A Distributed Solution to Automotive Security and Privacy		x		T
Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems	x			T
Blockchain's roles in strengthening cybersecurity and protecting privacy		x		T