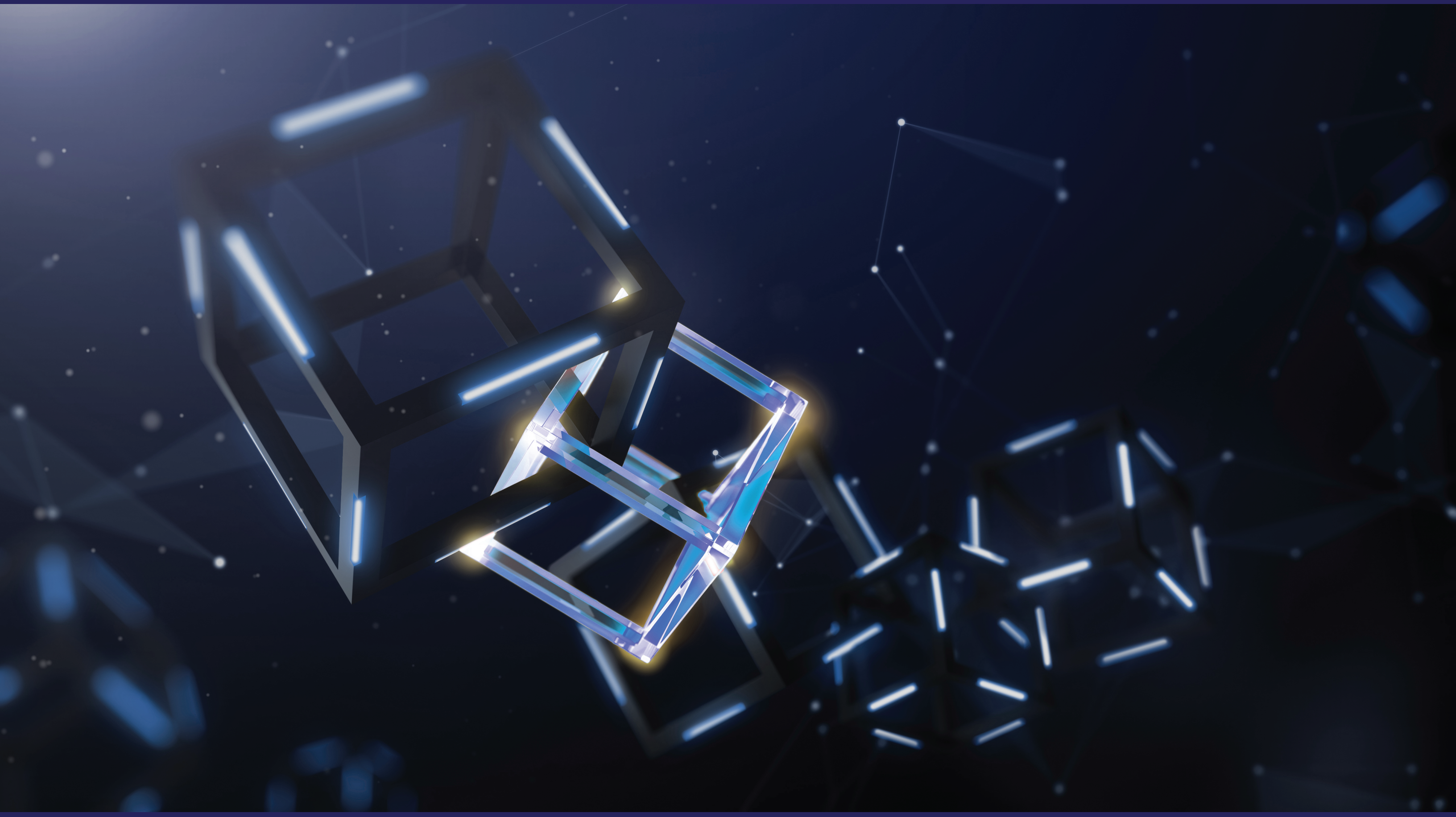
Blockchain

The Next Disruptive Technology

By Ryan McCracken



cgn

Good thinking. Globally.

415 SW. Washington St.
Peoria, IL 61602
www.cgnglobal.com

Table of Contents

Introduction

Innovation is essential for companies to maintain their competitive edge. Most often, it leads to incremental change in business models, markets, and technology.[1] Today, the digital revolution is causing substantial increases in efficiency and productivity, while also transforming the business environment. The pace of change is only increasing with each advancement or new technology. Every business leader is hyperattentive to new and developing technologies because the next one could fundamentally transform the business environment, and put them out of business or provide a first-mover advantage to an existing competitor. Furthermore, being the first adopter could lead to peril as well; lost time, money, and opportunities.

It is true, new technologies like the Artificial Intelligence, Internet of Things (IoT) and Blockchain are likely to be the next disruptive technologies that transform the world as we know it.[2] However, each needs to overcome several daunting hurdles for their benefits to be fully realized. The primary concern with the adoption of these new technologies is security.[3] A more interconnected and automated world increases a malicious actor's impact on the integrity of data, networks, and systems. However, technology will eventually be able to overcome this obstacle. The question is which technology will be able to resolve security concerns. Blockchain's potential for resolving security vulnerabilities is the reason it is viewed as a transformational technology.

When most people think of blockchain, they think of digital currencies. Bitcoin gained notoriety because it was the first digital currency to solve the double spending problem that had prohibited the adoption of digital currencies.[4] Though the concept of digital currencies can be attractive, other reasons make it impracticable. Ultimately, there is no doubt that some form of a digital currency will exist in the future, but it probably will be like bitcoin is today. The anonymity of Bitcoin's users and its disconnection from monetary policy, which some tout as strengths of bitcoin, are also weaknesses that make it problematic. Anonymity makes bitcoin a preferred platform for criminals and money launderers who want to conceal the sources of their funds, and its lack of centralized control prohibits the implementation of monetary policy by governments to stimulate economic growth. Both make bitcoin a likely target for future government regulations.

Nevertheless, further development of blockchain is warranted; because its advancement could prove more applicable and valuable for other uses. The key aspect of blockchain is its ability to provide trust between participants who may not know each other, allowing them to transact in a more secure and transparent way.[5] In particular, a promising area of blockchain's development is with the use of smart contracts.[6] Essentially, smart contracts are programmed conditions stored within a blockchain network and automatically executed upon satisfaction of specific preconditions or terms.[7]

Many businesses could benefit from this type of network to reduce costs, increase speed, improve accuracy, and increase transparency. The areas that could benefit from blockchain include, energy - production and consumption, currency transactions and tracking, healthcare, voting systems, supply chain management, media - copyright protection and authorization, pharmaceuticals, real estate - land ownership registration and ownership transfer, auditing, document security, regulatory compliance, stock trading, insurance, identity management, tax collection, auditing, supply chains, and OEM-supplier relationships.[8]

Imagine the terms of an insurance contract stored on a blockchain network. Upon the occurrence of an event, payment is made to the insured. For an original equipment manufacturer and a supplier, many times either party would not want to use the legal system if either is aggrieved by the other. Increased automation and transparency could strengthen this relationship and prevent its deterioration due to leadership changes or fluctuations in business cycles. Orders, product quantities, and payments could be tracked in a blockchain network and a smart contract could provide redress to either party when the other is not living up to their obligations. This accountability would foster trust and allow both parties to make better decisions on the future of their business. In terms of product integrity, information about products and their sources could be stored within blockchain to provide

[1] See Economics of Blockchain, Davidson, Filippi, Potts (May 2016) at 8.
[2] See Blockchain: The Key to IoT's Full Potential, Saunders (November 2017)
[3] Id.
[4] See Economics of blockchain at 6.
[5] Economics of Blockchain at 3, See Semantic Blockchain to Improve Scalability in the Internet of Thing, Ruta, Scioscia, Ieva, Capurso, Sciascio (2017) at 47-48.
[6] Designing a Smart-Contract Application Layer for Transacting Decentralized Autonomous Organizations, Norta (2017) at 3, The green blockchain: Managing decentralized energy production and consumption, Imbault, Swiatek, de Beaufort, Plana (2017) at 2.
[7] Id.
[8] See Blockchain technology in the chemical industry: machine-to-machine electricity market, Blockchain machine to machine electricity market, Sikorski, Haughton, Kraft (2017) at 8. Understanding the Blockchain Using Enterprise Ontology, Kruijiff, Weigand (2017) at 4. See Blockchains Everywhere: A Use Case in the Pharma Supply-Chain. Bocek, Rodrigues, Strasser, Stiller, See THE BLOCKCHAIN PHENOMENON - The Disruptive Potential of Distributed Consensus Architectures, Juri Mattila (2016), 18. The green blockchain, at 2.
[9] See THE BLOCKCHAIN PHENOMENON at 15.
[10] See Economics of Blockchain at 5, Understanding the Blockchain using Enterprise Ontology at 3.

consumers more transparency regarding their product purchases.[9] Consumers would benefit from more information about their products and gain trust in each product's integrity. In sum, these are examples of how blockchain could enable more trust and certainty in an increasingly uncertain world.

Blockchain could also lead to transformational change – decentralization of the way information we exchange information.[10] The decentralization of our information system has the potential to disrupt or render existing business models obsolete and give rise to completely new business models. Much like the internet changed the way we share information with each other, blockchain could also alter the way we exchange information.

Today, information systems are centralized.[11] Information is stored and transferred from one single source to another. However, as our digital and physical world become more integrated, the costs of this 'single source' system will increase exponentially. As we continue to become more integrated with technology, more data will be produced, stored, transferred, and processed. Cutting edge technology like Artificial intelligence, automation, Augmented Reality, and IoT will compound this capacity issue of our information ecosystem's.

Further, this centralized system will pose a substantial security threat, and even a threat to national security. Technological advancements will continue to challenge the information ecosystem's capacity to handle the exponentially increasing volume of data that technologies generate. Ultimately, either capacity constraints, costs, or both will render our current information ecosystem obsolete.[12] To overcome this bottleneck, new ways of communicating, transferring, and storing information must be developed. The technology we commonly refer to as "blockchain" could be the innovation we need to help transform our information ecosystem into one that is more secure, productive, and efficient.

How can blockchain do this? The answer lies in the unique characteristics of blockchain and the applications for which it would be useful. Blockchain has several fundamental attributes that make it unique.

More Than Just a Digital Ledger

Ledgers have been used for centuries to keep consistent, accurate, and reliable records of the ownership and flow of funds, accounts, assets, and liabilities. A requirement to ensure accurate and reliable records is that a central authority must control the ledger.[13] However, Blockchain technology removes the need for a central authority and allows for a decentralized system in which the ledger is securely distributed within a network of computers (nodes). Each node maintains the exact same copy of the digital ledger at-all-times, and any change to one version is contemporaneously made to all versions.[14] This ensures no alternate version of a records exists. To achieve the task of uniformity across the nodes, blockchain uses two techniques; encryption through use of hash functions and transaction validation through a consensus mechanism.[15]

Encrypted Transactions - Hashes

The transactional records stored in blockchain are made immutable (unchangeable) through a two-step process – (1) creating a cryptographic (encrypted) record of a transaction called a "hash", and (2) 'chaining' the transaction records together upon storage.[16] First, a mathematical function converts the information into what's known as a **hash** – a cryptographic (coded) value of defined length that represents the original information.[17] After a hash, values are created for a transaction and an adjacent transaction, both hash values are put through the function again to obtain a new hash value representing both transactions, also called a "hash of hashes".[18] This process is systematically repeated for each set of transactions until only one hash value exists for the entire set of transactions.[19] This last hash value or "hash of all hashes" is called the Merkle Root for the set.[20] Since the transactions are interconnected through the 'hashing' process, if a hash is changed, then all the other subsequent hashes would be altered.[21] This interconnection of hashes also make it easier to check if a specific transaction has been included in a block without having to download the entire blockchain ledger.[22] Once a Merkle Root Hash ('hash of all hashes' for a set of transactions) is obtained, the Merkle

[11]Understanding the Blockchain Using Enterprise Ontology at 4.
[12]See Blockchain based trust & authentication for decentralized sensor networks. Moinet, Darties, Baril (June 2017) at 2.
[13]THE BLOCKCHAIN PHENOMENON at 7.
[14]Id 7-8.
[15]Id at 1,6-7.
[16]Blockchain based trust & authentication for decentralized sensor networks at 2.
[17]Blockchain technology in the chemical industry, 3-4.
[18]Understanding the Blockchain Using Enterprise Ontology, 4. See also Blockchain based trust & authentication for decentralized sensor networks at 2.
[19]Id.
[20]Blockchain based trust & authentication for decentralized sensor networks at 2.
[21]Blockchain Machine to Machine Electricity Market at 4, see also Blockchain based trust & authentication for decentralized sensor networks at 2.
[22]Understanding the Blockchain using Enterprise Ontology at 3.
[23]Blockchain technology in the chemical industry at 23.
[24]Id.
[25]Id. See Blockchain based trust & authentication for decentralized sensor networks at 2.

Root Hash is included within the blocks of the next set transactions. This process interconnects or 'chains' all of sets of transactions together.[23]

This structure, called a Merkle tree, is the process of compiling data within a blockchain network.[24] A diagram of a Merkle Tree looks much like a pyramid or decision tree.[25] Each value is inserted into the mathematical function until only one figure remains for the entire set.[26] The purpose of this method for organizing data is to easily locate, summarize, copy, and verify data.[27] A Merkle tree's organization and interconnection of data allows it to be easily checked for tampering, use less resources to locate data, and allows for easy verification of transactions.[28]

This is one of Blockchain's defining characteristics - its method of converting, compressing, and organizing information.[29] The integrity of the data is evidenced by the hashes themselves – a change in any hash value causes a change in every subsequent hash value in the chain.[30]

Validation of Transactions - Consensus Mechanisms

Conceivably, you could imagine it may be possible to alter all the chains or hashes to manipulate records. However, blockchain resolves this issue by including a consensus mechanism to verify the validity of a transaction.[31] The chaining of hashes and the consensus mechanism make the blockchain records 'immutable' – unchangeable.[32]

A blockchain's consensus mechanism can be tailored, depending on the blockchain's desired function.[33] For example, a blockchain network can be a public like Bitcoin, where each user (node) has the same rights and visibility of transactions and miners perform extremely complex mathematical equations to authenticate and validate transactions, which is called a Proof-of-Work consensus model.[34] On the other end of the spectrum, blockchain networks can be a private network where the rights of users (nodes) can be restricted, and the consensus mechanism may be less complex, like a majority vote from the nodes.[35] The more complicated the consensus protocol the more difficult it would be to alter a record. For the consensus mechanism to allow a transaction, a majority of the nodes must also have the same version of the ledger. Therefore, any improper hashes or records are either rejected or overwritten by the proper version of the ledger held by a majority of the nodes.

Essentially, the only way to alter any transactional information is to override the data held by all the nodes at the same time.[36] The only way to achieve this is to overpower the system by utilizing more computing power than the combined computing power possessed by a majority of the nodes.[37] For networks with a substantial number of nodes, long transaction histories, or both, it could become impossible because a person could not obtain the requisite computing power to overcome the system or the vast amount of power required would be prohibitive.[38] Therefore, the cryptographic has values and the difficulty in rivaling the networks computing power make blockchain a more secure method of storing a distributed ledger across a network. Since Blockchain is adaptable, it can achieve the desired function for many different applications.[39]

Blockchain's Value Add: Smart Contracts

Blockchain's immutable storage of information and consensus validation is particularly useful for software applications.[40] Codes can be written, stored, and distributed across a blockchain network, and executed when specified conditions are met.[41] These are called smart contracts, because they contain specific commitments automatically executed upon the occurrence of specified conditions.[42] The way a blockchain network stores these commitments makes them easily retrievable, secured within the network, and verifiable by nodes.[43]

The best way to demonstrate this is to use an example. Assume there is a town equipped with a blockchain network for purpose of keeping track of energy production and consumption.[44] Many homes within the town are equipped with solar panels, and these panels are connected to its energy grid.[45] The amount of energy produced by each home from the solar panels and the amount of energy used by each home is recorded within a blockchain network, each home acting as a node within the network.[46] Any solar power produced by a home, and not used, can be sold to another home within the network that is in need of energy. Smart contracts on the blockchain would allow

[26] Id.
[27] Semantic Blockchain to Improve Scalability in the Internet of Things, 51.
[28] Id., See also Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain at 2.
[29] Id.
[30] Blockchain based trust & authentication for decentralized sensor networks at 2.
[31] Economics of Blockchain at 3.
[32] The green blockchain at 2, See Towards Self-Sovereign Identity using Blockchain Technology, Baars, at 31.
[33] See Understanding Blockchain Consensus Models, Baliga (April 2017), 4.
[34] Id at 7
[35] See Id at 3, See also Understanding the Blockchain Using Enterprise Ontology at 5.
[36] Blockchain machine to machine market at 7.
[37] Blockchain technology in the chemical industry: machine-to-machine electricity market at 7.
[38] See Understanding Blockchain Consensus Models at 4.
[39] Id.
[40] Town Crier: An Authenticated Data Feed for Smart Contracts. Zhang, Cecchetti, Croman,

individual homes to transact with each other for the optimal use of resources by each node. Further, this type of network would automatically optimize its use of resources through micro-transactions, for which payment and delivery of energy would be automatic.[47]

This same type of system can be utilized to enable IoT devices to communicate with each other, transact, then validate the transaction by other devices within the system.[48] This type of network would allow devices from any manufacturer to transact with one another seamlessly.[49] Further, payment for services could be based upon actual use and enable efficient allocation of a device's resources.[50]

Imagine communities that own several autonomous lawnmowers that cut each home's lawn whenever it reaches a certain height. The system would automatically optimize the use of the mowers to ensure everyone's lawn was mowed and ensure the least amount of time and gasoline is used. Payment for this service could occur automatically upon the mower performing services, and an owner of a mower could ensure minimal idle time for its use. Now, there are safety concerns with lawn mowers, but this example demonstrates the concept.There is a vast amount of capital that is spent on items that sit idle, like automobiles and lawn mowers. This system would increase efficiency by allowing consumers to pay only for their actual use. Homeowners would be able avoid buying a lawnmower, only to have it sit idle most of the time. The result would be the efficient allocation of resources and reduction in transaction times; allowing any potential excess resources to be utilized.[51]

Blockchain & IoT (Internet of Things) - Overcoming Privacy & Security Issues

IoT is a network of integrated or interconnected devices with electronics, sensors, and software.[52] If IoT devices can be integrated with blockchain, it would transform the human-initiated experience from a human use-based interaction to a device-initiated interaction. Devices could initiate their own agreements based upon parameters set by smart contracts, enabling seamless devices function.[53] Enhanced communication and interaction of devices will also enable a complete network of devices to more efficiently allocate resources.[54]

Currently, IoT is primarily used for data collection, remote monitoring, and device automation. By 2020, it is expected there will be over 20 billion IoT devices in operation worldwide.[55] The vast number of IoT devices expected to be in operation would present significant challenges in terms of server capacity, data transfer, security, and reliability.[56] The integration of these devices and networks present a monumental challenge, in order to capture the benefits of IoT at scale.[57]

The security issues presented by IoT devices are especially problematic. They are extremely susceptible to malicious cyber-attacks due to their limited computing capacity.[58] IoT devices can be easily bombarded with hacks or requests for data to achieve the desired malicious effect.[59] Further, there are no common security standards for the manufacturers of IoT devices.[60] The lack of consistency in security capabilities make data security and privacy, node authentication, and management of a network's trust impossible.

However, blockchain may be able to bolster IoT devices by making them more secure. Essentially, IoT devices could communicate through smart contracts stored on a blockchain to ensure their security and operation.[61] Though Blockchain might be able to resolve these issues regarding IoT's scalability, significant developments in infrastructure and networks are required for Blockchain to achieve the scale necessary to have any transformative effect.

Future Developments

Blockchain is developing rapidly and could be used in many different ways. For example, it could enable a person's digital identity management, allowing storage and control of personal information in one location.[62] Instead having every person's personal information stored by various entities, personal information would be stored in one location like a personal computer. Then, entities requesting information would get a yes or no answer to questions like, "Is this person over 21", or receive more detailed information if given permission. This would increase personal privacy and security, decrease identity fraud, and reduce transaction times. Bank transactions

Juels, Shi, (2016), at 270.
[41] Id at 272.
[42] Id.
[43] See Out-of-Band Authentication Scheme for Internet of Things Using Blockchain Technology at 4 & 5. See also Semantic Blockchain to Improve Scalability in the Internet of Things.
[44] Blockchains for Decentralized Optimization of Energy Resources in Microgrid Networks, Munsing, Mather, and Moura (March 2017) at 1.

[45] See Id.
[46] Id.
[47] See The green blockchain: Managing decentralized energy production and consumption.
[48] See THE BLOCKCHAIN PHENOMENON, 12.
[49] See Town Crier, at 270. See also Semantic Blockchain to Improve Scalability in the Internet of Things.
[50] Semantic Blockchain to Improve Scalability in the Internet of Things at 49.
[51] Id.

and mortgage due diligence could significantly benefit from a secure and reliable digital identity. Further, blockchain could even be used in this way to enable a universal medical record system shared by all hospitals.

Medical product supply chains could utilize blockchain for product information or conditions. For example, many medical and pharmaceutical products require specific environmental or storage conditions to maintain product integrity and quality.[63] A test case was performed where sensors were used to track temperature and humidity conditions throughout the supply chain, and these records were stored on a blockchain network. The use of blockchain in the way would increase the trust of a products' integrity and reliability of records for all parties involved.[64]

Lastly, one new development allows the transfer of information between different blockchain networks. This development is known as 'Pegged Sidechains', which are blockchain networks connected to a main blockchain network and allow the transfer of data from one blockchain to another.[65] If perfected, this could enable blockchain's scalability and universal use across different functions.

Conclusion

Blockchain can unlock a new era of technological advancement, where IoT devices communicate and transact with one another. Where blockchain is the source of validation, consistency, recordkeeping of the transaction, and smart contracts within blockchain govern execution and validation of IoT devices activity through their sensors. If this is type of seamless automated network is achieved, it will change business is conducted forever.

About CGN

At CGN Global, we help companies worldwide overcome core business challenges of growth, margin, and responsiveness. Going beyond simply solving their problems, we quickly and effectively deliver transformational results that are sustainable.

That's because we deliver results, not reports. We help our clients solve difficult problems and become winners in the marketplace. We do this with a powerful combination of good thinking, broad capabilities, and sheer drive to go beyond what's expected. It's what we do - and we've been doing it for more than 20 years.

[52] An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology. Wu, Du, Wang, Lin. (March 2018) at 1.
[53] See An Out-of-band Authentication Scheme at 1.
[54] See Id.
[55] Id.
[56] Id.
[57] Id.
[58] Id.
[59] Id.
[60] Id.
[61] Id at 5.
[62] See Towards Self-Sovereign Identity using Blockchain Technology, Baars.
[63] Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain at 774.
[64] Id at 773.
[65] Understanding the Blockchain Using Enterprise Ontology at 9, See Enabling Blockchain Innovations with Pegged Sidechains. Back, Corallo, Dashjr, Friedenbach, Maxwell, Miller, Poelstra, Timón, Wuill (2014)

Written by

Ryan McCracken
Consultant
ryan.mccracken@cgnglobal.com

References

1. Economics of Blockchain. Sinclair Davidson, Primavera De Filippi, Jason Potts. Public Choice Conference, May 2016, Fort Lauderdale, United States. https://hal.archives-ouvertes.fr/hal-01382002/document (accessed July 2018).

2. Blockchain: The Key to IoT's Full Potential. Jen Saunders, November 2017. https://www.business.com/articles/blockchain-key-to-internet-of-things/ (accessed July 2018).

3. Semantic Blockchain to Improve Scalability in the Internet of Things. Michele Ruta, Floriano Scioscia, Saverio Ieva, Giovanna Capurso, Eugenio Di Sciascio. Open Journal of Internet of Things (OJIOT), Volume 3, Issue 1, 2017. https://d-nb.info/1137820225/34 (Accessed July 2018).

4. Designing a Smart-Contract Application Layer for Transacting Decentralized Autonomous Organizations. Alex Norta. Conference Paper 2017. https://www.researchgate.net/publication/308986556_Designing_a_Smart-Contract_Application_Layer_for_Transacting_Decentralized_Autonomous_Organizations (Accessed July 2018).

5. The green blockchain: Managing decentralized energy production and consumption. F. Imbault, M. Swiatek, R. de Beaufort, R. Plana. 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe). https://ieeexplore.ieee.org/document/7977613/ (Accessed July 2018).

6. Blockchain technology in the chemical industry: Machine-to-machine electricity market. Janusz J. Sikorski, Joy Haughton, Markus Kraft. Applied Energy (2017). http://www.arifsari.net/isma500course/project/10.pdf (Accessed July 2018).

7. Understanding the Blockchain Using Enterprise Ontology. Joost de Kruijiff, Hans Weigand. International Conference on Advanced Information Systems Engineering (2017). https://www.researchgate.net/publication/316636055_ Understanding_the_Blockchain_Using_Enterprise_Ontology (Accessed July 2018).

8. Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain. Thomas Bocek, Bruno B. Rodrigues, Tim Strasser, Burkhard Stiller. Communication Systems Group (CSG), Department of Informatics (IfI) University of Zurich. https://files.ifi.uzh.ch/CSG/staff/bocek/extern/publications/im2017_final.pdf (Accessed July 2018).

9. THE BLOCKCHAIN PHENOMENON - The Disruptive Potential of Distributed Consensus Architectures. Juri Mattila. BRIE Working Paper 2016-1, BERKELEY ROUNDTABLE ON THE INTERNATIONAL ECONOMY (BRIE) UNIVERSITY OF CALIFORNIA, BERKELEY (MAY 2016). http://www.brie.berkeley.edu/wp-content/uploads/2015/02/Juri-Mattila-.pdf (Accessed 2018).

10. Blockchain based trust & authentication for decentralized sensor networks. Axel Moinet, Benoit Darties, and Jean-Luc Baril. IEEE Security & Privacy, Special Issue on Blockchain (June 2017). https://arxiv.org/pdf/1706.01730.pdf (Accessed July 2018).

11. Towards Self-Sovereign Identity using Blockchain Technology. Djuri Baars. Robobank; University of Twente. https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf (Accessed July 2018)

12. Understanding Blockchain Consensus Models. Arati Baliga, PhD. Persistent Systems Ltd. (April 2017). https://pdfs.semanticscholar.org/da8a/37b10bc152 1a4d3de925d7ebc44bb606d740.pdf (Accessed 2018).

13. Town Crier: An Authenticated Data Feed for Smart Contracts. Fan Zhang, Ethan Cecchetti, Kyle Croman, Ari Juels, Elaine Shi. CCS'16, October 24-28, 2016, Vienna, Austria. https://eprint.iacr.org/2016/168.pdf (Accessed July 2018).

14. An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology. Longfei Wu, Xiaojiang Du, Wei Wang, and Bin Lin. 2018 International Conference on Computing, Networking and Communications (ICNC), March 2018. https://www.researchgate.net/publication/321491493_An_Out-of-band_Authentication_Scheme_for_Internet_of _Things_Using_Blockchain_Technology (Accessed July 2018).

15. Blockchains for Decentralized Optimization of Energy Resources in Microgrid Networks. Eric Munsing, Jonathan Mather, and Scott Moura. March 2017, University of California at Berkeley. https://ecal.berkeley.edu/-pubs/CCTA17_Blockchain.pdf (Accessed July 2018).

16. Enabling Blockchain Innovations with Pegged Sidechains. Adam Back, Matt. Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille. Blockstream, 2014. https://blockstream.com/sidechains.pdf (Accessed July 2018).