Blockchain Research Report

Stefan Forsström
Istitution of Information Systems and Technology
Mid Sweden University, Sundsvall, Sweden
Email: stefan.forsstrom@miun.se

Abstract

This research report outlines the current research into blockchain technologies as of December 2018. Starting with an overview of the blockchain technology to introduce the theory. To then follow with deep looks into the different aspects of blockchain technologies, investigating the research articles and current state of work in these area, including the forefront of the research frontier. As well as existing blockchain products, an outlook on the future, conclusions that can be drawn from this study. With the intent to both create understand of the technologies, as well as inspire further research work and identifying potential knowledge gaps.

I. Introduction

WITH the intent of creating an understanding in the broad and diverse area that is blockchain, this report outlines the current research into blockchain technologies and existing literature as of December 2018. This work is intended to be used as a basis for further research work, as well as a way of identifying knowledge gaps in the research area and show the potential to fill these. With the purpose of finding potential areas to have future collaborative research projects in. The scope and focus is set on blockchain technologies specifically, but related technologies such as cryptocurrecies will indirectly be a part of this work as well. The methods that has been used for creating this work have been based on both literature studies, studies on the most cited works, trend observations, reading of news articles, analyzing technological trends, and observing interests of the large IT enterprises.

The remainder of this report is organized as follows: Section II presents an overview of the technology itself, to reiterate and introduce some of the technical terms for creating a better understanding for the remaining of this article. Including information on its origin and history. Section III presents the literature review and is split into subsections which focus on different categories of articles. Section IV presents a specific study on related works related the problems, challenges, and impact of GDPR to blockchain systems. Finally, Section V presents our conclusions regarding this work and presents an outlook on future research and potential future problems.

II. Blockchain technology overview

This section will provide an overview of the blockchain technology as a way to introduce the theory and research area. A blockchain is an immutable ledger since once data have been added to the chain it cannot be changed. This process is based on cryptographic hashes that overlap the blocks and since it has this overlap, the data is chained together. Hence, the name blockchain, i.e. a chain of blocks. These blocks can also contain additional information which then becomes immutable as well. Which is the primary property that blockchain technology is used for. Figure 1 shows an illustrative example on how this chain works.

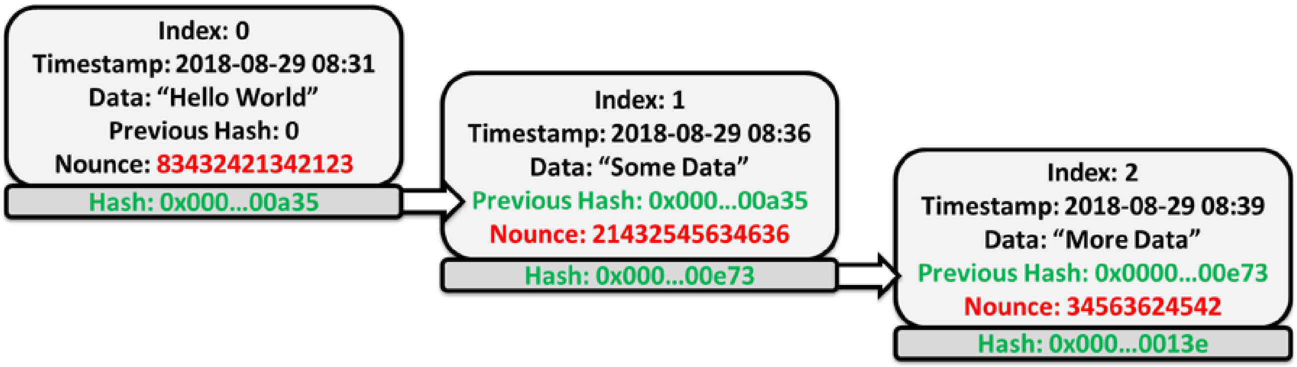

Fig. 1. Overview of a simple blockchain with three blocks chained together.

In this figure, one can see three blocks chained together. The genesis block with index 0, and two chained blocks, index 1 and 2. Each block contains a timestamp, some data, the hash of the previous block, a nounce, and the hash of the block itself.

Where the index and timestamp is only for the ordering. The data is the data that will be stored in the blockchain and will become immutable once the blocks are chained together. The previous hash is the link to the previous block. In the genesis block the previous hash is 0, otherwise it is set to the hash of the previous block. The nounce is not mandatory of all types of blockchains, but it is used to adjust the difficulty of the hashing. Basically, the final hash should have a predefined number of leading zeroes to be accepted. Finally, the hash field is the hash of the entire block, including the index, data, previous hash, nounce, etc. And it is this hash and the previous hash that makes it into a chain. If any single piece of data is changed in any block, it can easily be detected and the chain becomes broken. For example if a malicious user tries to change the data in a stored block. For example a change in block 0 from ”Some Data” to ”Some Data!”, the resulting hash will become something completely else and therefore not correspond to previous hash of the block 2. Hence, the change will easily be detected by all other users and the edited block will be discarded. Thus, ensuring the immutability of the blockchain.

For a good introduction to how blockchains work and how to implement them, we suggest the textbooks: Blockchain Basics by Daniel Drescher[1] and Beginning Blockchain by Singhal et al [2].

A. *Blockchain Origin and Genesis*

This background story and history of blockchain and bitcoin is based on the history told references [3], [4], and [5].

The domain name bitcoin.org was registered in August 2008 and in October 2008 a white paper authored by an author named Satoshi Nakamoto was posted to a cryptography mailing list. The title of the white paper was Bitcoin: A Peer-to-Peer Electronic Cash System [6] and was a detailed description of using a peer-to-peer network to create an immutable ledger. Published in the form of a white paper, which means that it is a non scientifically peer-reviewed article. It was simply made available on the Internet for people to read. In January 2009, the implemented bitcoin network came into existence with Satoshi Nakamoto mining the genesis block of bitcoin (block number 0), which also had a reward of 50 bitcoins. One of the first supporters, adopters, contributor to the bitcoin blockchain and receiver of the first bitcoin transaction was a developer named Hal Finney. Finney who received 10 bitcoins from Nakamoto in the world’s first bitcoin transaction on 12 January 2009. Other notable early supporters and developers were Wei Dai, Nick Szabo, and Gavin Andresen.

The author Satoshi Nakamoto is however presumed to be a pseudonym for what is yet an unidentified person or persons. It is known that Nakamoto was responsible for creating the majority of the official bitcoin software and was active in making modifications and posting technical information on the official bitcoin forums. However, the true identify is still unknown. Probably made because the bitcoin creators were afraid of convictions and trials, especially in USA. Since the U.S. Mint had informed in 2006 that the circulation of medallions such as the Liberty Dollar as legal tender, is considered a federal crime and they had also seized a large amount of liberty dollars in 2007 as well as made formal criminal charges against its inventor Bernard von NotHaus in 2009. Meaning that the bitcoin inventors could easily face similar threats.

A number of people have been been suspected to be Satoshi Nakamoto, including the previously mentioned developers Wei Dai, Nick Szabo, and Hal Finney. But all have denied these accusations. Nakamoto’s involvement with the bitcoin code development does not appear after 2010, and in April 2011 Nakamoto communicated with one of the other bitcoin contributors saying that he had moved on to other things. But the bitcoin blockchain clearly states in the ledger that he amassed over 980 000 bitcoins for his mining efforts in the early days of bitcoin. Meaning that he theoretically is one of the 250 most wealthiest persons in the world if he were to monetize these assets [7]. This is, however, very unlikely. Since if these bitcoins ever were to be monetized, his real identity would become known and the actual bitcoin price would drop significantly because of the unstable market forces this would create. Hence, the real identity of Satoshi Nakamoto still remains unknown and that is probably for the best for ensuring the credibility and stability of the bitcoin market. Most of Satoshi Nakamotos emails, forum posts, etc. have been saved for historical and archival purposes [8]

Prior to the release of bitcoin there were a number of related digital cash technologies published. For example the issuer based ecash protocols by David Chaum and Stefan Brands [9], [10]. Hashcash, a proof-of-work scheme for spam control by Adam Back [11]. Wei Dai’s b-money [12] and Nick Szabo’s bit gold [13]. As well as, Hal Finney’s reusable proof of work using hashcash as its proof of work algorithm. One can also argue that the AbsoluteProof system can also be seen as a very early blockchain, since it is based on basic mechanics by Haber and Stornetta. In which AbsoluteProof have published a hash of their AbsoluteProof database every week since 1995 in the new york times magazine, ensuring the immutability of their database [14].

B. *Blockchain Timeline and Trend*

In this report we have also studied the term blockchain, its origin, usage, and appearance in media. Especially in the context of Sweden and the usage of the term *blockkedja* in Swedish media. From what we can find, the first usages of the term bitcoin in Swedish media was in may 2011 by Nanok Bie. Publishing a series of articles in SVT nyheter on how this new cryptocurrency works and its threat to the existing finance systems[15], [16]. Today, Nanok Bie still writes and is involved in articles related to Bitcoin since he is the editor-in-chief for the news section of the official bitcoin.com website. The first usages of the term blockchain and blockkedja in Swedish media is made as a series of articles in may 2013 by journalist Anders Lotsson at International Data Group (IDG) [17]. These articles were written for the Computer Sweden newspaper, but they were also published in other IDG newspapers and on different IDG websites. Since this, there has been numerous other publications made on the topic in Swedish media. Figure 2 shows the number of Swedish news articles using the term Bitcoin and Figure 3 shows the terms blockchain or blockkedja. Split into each year, from 2008 to today. One interesting thing to note is that even though the original Bitcoin paper was published in 2008, it took until 2013 for Swedish media exposure to highlight Bitcoin and blockchain technologies.

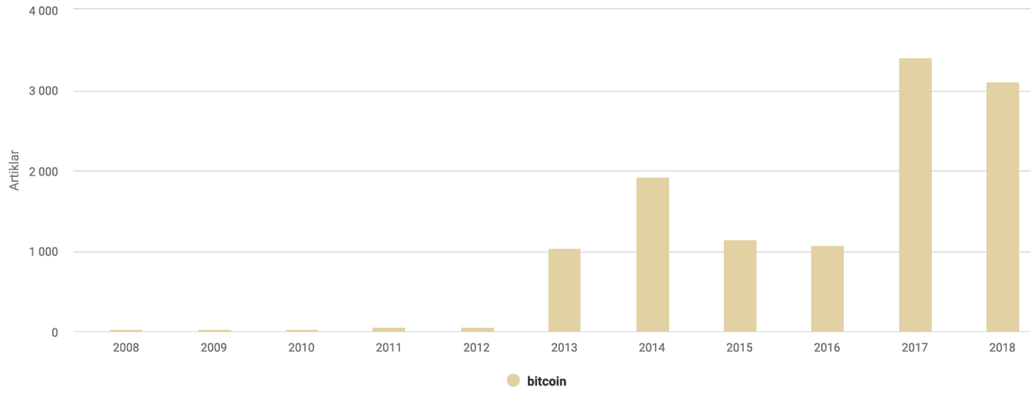

Fig. 2. The number of Swedish media articles on the topic bitcoin divided per year

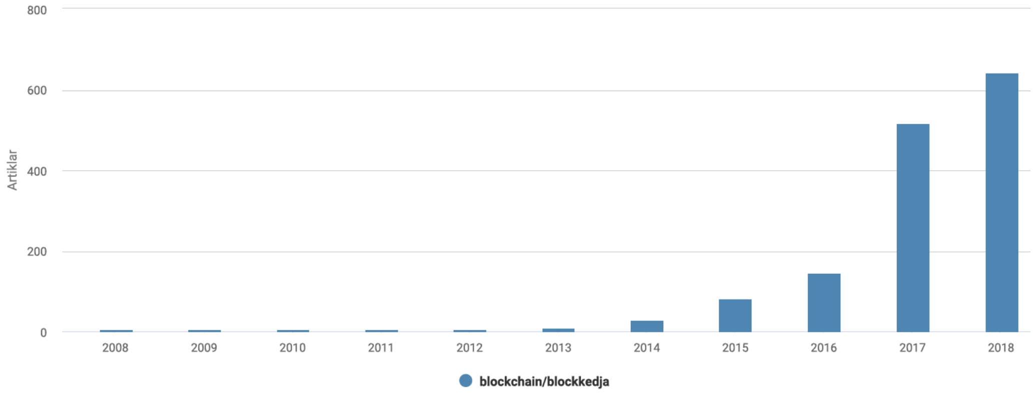

Fig. 3. The number of Swedish media articles on the topic blockchain or blockkedja divided per year

We can also do a similar observation in the search interest using Google Trends. Figure 4 shows the relative interest of Swedish Google searches articles using the term Bitcoin and Figure 5 shows the relative interest in the term blockchain. Figure 6 shows both of them together, showing that the interest in Bitcoin is significantly higher than blockchain.

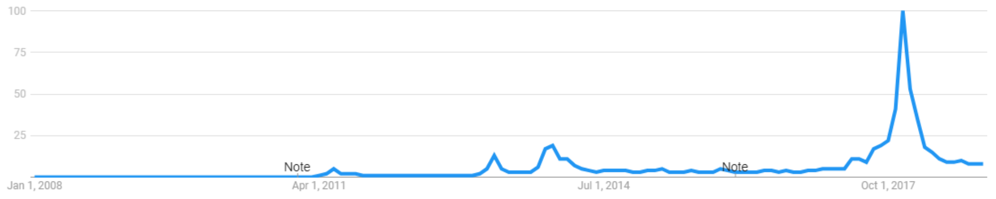

Fig. 4. The relative Swedish interest in the Google search term bitcoin

We can also look at more the number of published scientific articles in each of these areas. Which actually shows that there are more research articles in the area of blockchain than the area of Bitcoin. Figure 7 shows the amount of Inspec indexed published scientific articles in the area of Bitcoin and Figure 8 shows the number of published scientific article in the area of blockchain. One reason for difference can be that since blockchain is the underlying technology for Bitcoin, that it is of more

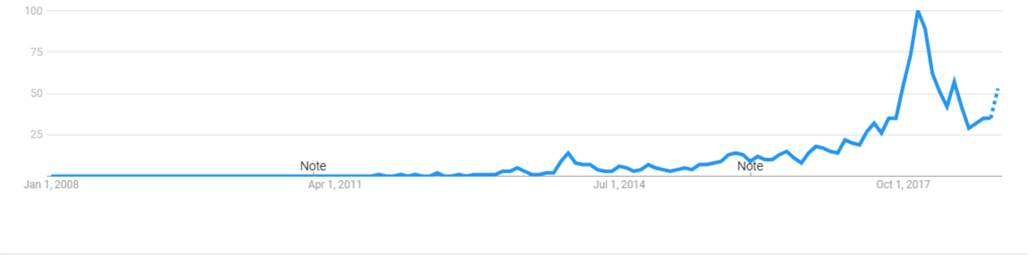

Fig. 5. The relative Swedish interest in the Google search term blockchain

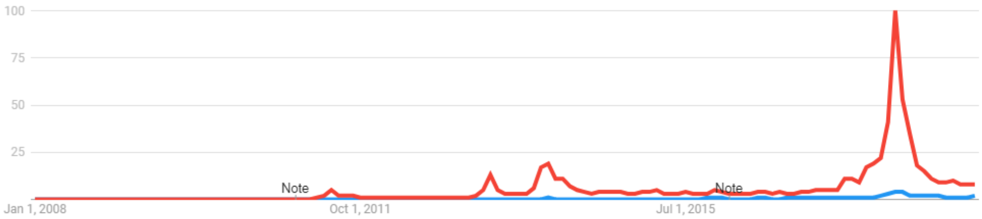

Fig. 6. The relative Swedish interest in the Google search terms bitcoin and blockchain for comparison

interest to computer science researchers. The cryptocurrency itself seems to not have the same knowledge gap and research potential, as the more general underlying technology.

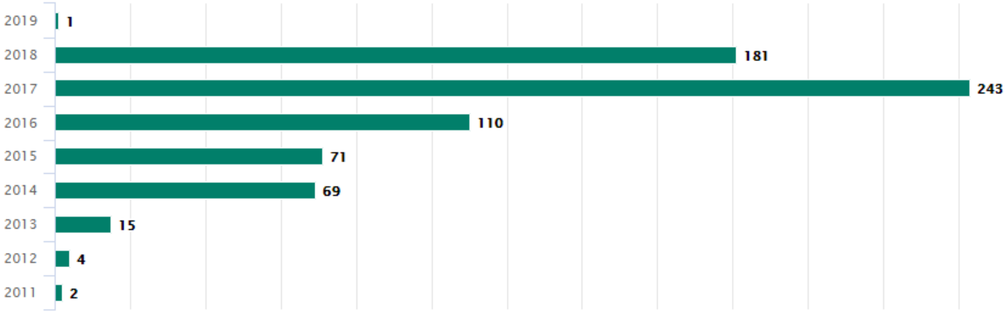

Fig. 7. The amount of Inspec indexed scientific articles on Bitcoin

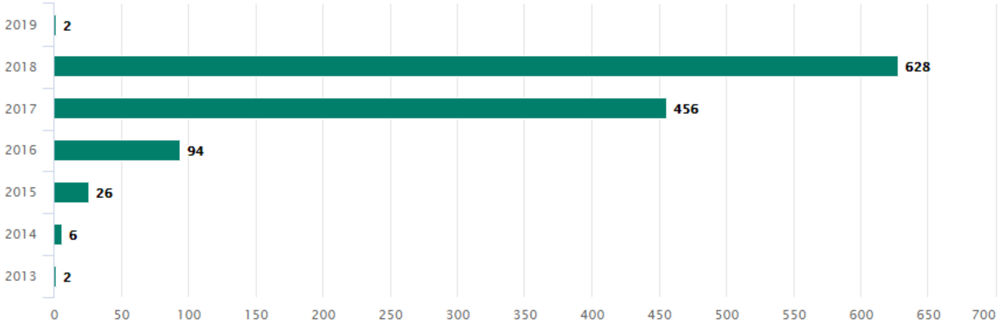

Fig. 8. The amount of Inspec indexed scientific articles on blockchain

III. Literature Review

This section will present the current literature and state of the art in the area of blockchain. This literature overview have been gathered using both academic search engines such Google Scholar and IEEExplore. The articles have been found on search and indexing terms such as: blockchain, blockchain applications, blockchain survey, blockchain consensus, bitcoin, bitcoin survey, etc. The articles found in these searches have been limited to only include the most cited articles, which for example included articles with more than 70 citations as of December 2018 according to Google Scholar. We have also studied which articles that cite these articles to include chains of citations. Finally, we have divided the articles into categories based on their content and specific blockchain area. These categories are:

- Textbooks, Surveys Articles, and General Reports
- Articles that Analyze Blockchain Technology
- Articles on Blockchain Improvements and Variant
- Articles on Different Blockchain Applications
- Articles Discussing the Future of Blockchains

However, we begin this literature review with the original bitcoin article by Satoshi Nakamoto:

Bitcoin: A peer-to-peer electronic cash system

S. Nakamoto, 2008, [6], cited by 4707

As previously stated, this article and the usage of blockchains as immutable ledgers can be seen as the origin of the blockchain technologies we see today. It is in this paper the bitcoin and blockchain revolution started. Even though the paper was published as a non peer reviewed white paper, it is one of the most cited works in the blockchain research area. The paper itself is short and does not include so many details. It primarily presents the overall idea and structure. Details on the solution, the specific technologies, and the exact properties on how the bitcoin system would be implemented is not included. Another interesting note, is that Satoshi Nakamoto never mentions the term *blockchain* specifically in his paper. But he does talk about chains of blocks, proof-of-work chains, and lengths of chains.

A. Textbooks, Surveys Articles, and General Reports

In this section we will study the different textbooks and survey articles related to blockchain. Because of their high point of view and overview perspective in writing, they tend to be good sources for the direction and understanding of a research area. One of the most well cited textbooks is by Melanie Swan, and below are the most well cited textbooks and surveys that we have found in this pre-study.

Blockchain: Blueprint for a new economy

M. Swan, 2015, [18], cited by 847

This book gives a good overview of the usage of blockchains and bitcoin as whole. As well as outlines three different versions of blockchain. Blockchain 1.0, 2.0, and 3.0. Where 1.0 can be seen as the currency, such as the original Bitcoin idea by Nakamoto. Where the blockchain is a method for a cryptocurrency, which also incorporates its own generation of the cryptocurrency as payments for the proof-of-work that has been done. Blockchain 2.0 is the next step into contracts. Meaning that it can be used for so much more than just currency in the finance world. It can for example be used in digital contracts, stocks, bonds, loans, smart contracts, smart properties, etc. Finally, the textbook explains blockchain 3.0, which extends the applications beyond the finance domain. Looking specifically into applications of government, health, science, literacy, culture and art. Where the discussions regarding government blockchains are most important for this pre-study. Including, but not limited to decentralized governance services, blockchain passports, blockchain weddings, and voting.

Mastering Bitcoin

A.M. Antonopoulos, 2014 and 2017, [19][20], cited by 611

This well cited textbook exists in two editions, where both editions are well cited. The first edition had the subtitle *Unlocking digital cryptocurrencies* and the second edition had the subtitle *Programming the open blockchain*, but they have similar contents in general. the second edition mainly includes recent updates that has come to the system which was made after the first edition was published. The book itself is centered around Bitcoin, how it works, and how it is implemented using blockchain technologies. Inclduing a deep dive into the Bitcoin refernce implementation that was originally written by Satoshi Nakamoto but has been heavily modified since then. The book also explains in detail how the distributed system works and how the blockchain is managed within it.

Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world

D. Tapscott, A. Tapscott, 2016, [21], cited by 439

This book is also well cited but has a quite different wiring perspective compared to the other books and articles. This book focuses on the revolution that blockchain technology brings, explaining the change, transformation, and digitization coming with blockchain technologies. The book primarily explains this from a business and economics perspective, using many historical quotes to put the blockchain revolution into historical context. But also highlight the importance of individuals, technology, and economic forces. Finally, the book ends with a look into different promises and perils of using the technology, including privacy, leadership, and future challenges.

SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies
J Bonneau, A Miller, J Clark, A Narayanan, J Kroll, EW Felten, 2015, [22], cited by 396
This research article is a survey of bitcoin from a research perspective. It starts with a well written history and technological analysis of bitcoin, highlighting for example the Nakamotos consensus algorithm, bitcoin mining, and its communication protocol. After the technical survey it focuses on research issues on the stability of Bitcoin. Including stability problem of the validity rules, the consensus protocol, mining pools, and the peer to peer layer. The article also highlight problems with client side security, different modifications to bitcoin, alternative consensus methods, and alternative puzzles. The survey also presents a number of alternative cryptocurrencies to bitcoin, as well as other potential research topics for extending bitcoin. Overall, the article is a good start for understanding a little more on the details on bitcoin works, the many issues with it, potential attacks, and future research challenges in the area of cryptocurrencies.

Blockchain technology: principles and applications
M. Pilkington, 2016, [23], cited by 232
This well cited reference is a book chapter inside the book Research handbook on digital transformations [24]. The whole book focuses on creating an understanding for digital transformation and is split into two parts. One that focuses on analyzing current areas and one that focuses on new and transversal topics. The first topic of the transversal topics is on blockchain technologies and this book chapter focuses on giving an short and understandable summary of the whole blockchain area, without going into technical details. It starts by summarizing the history of bitcoin and blockchain, continuing to presenting a holistic view of blockchain technology, and ending with a summary of different blockchain applications. Thus, giving a good summary and overview of the applications of blockchain technologies.

Where is current research on blockchain technology? a systematic review
J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, 2016, [25], cited by 232
This article presents a detailed review of the published papers up until 2016 in the blockchain area. In this article they use the challenges identified by Swan in [18] as mapping of the different articles they found. In this article they also categorized the papers they found in addition to mapping them into the challenges. These three three different categories were: blockchain report, blockchain improvement, and blockchain application. Because of this, the categories used in our article was inspired by the categorization used in this article. They also made numerous statistical discoveries regarding the trend of blockchain. For example the number of blockchain papers increased dramatically in 2014, most articles were written by academics from USA, aimed towards conferences or workshops, primarily on security topics, and that the articles on blockchain applications are primarily from 2015 and forward. Finally, they also identified that quite many of the challenges still remained unsolved in 2016. For example, regarding latency, throughput, bandwidth, developer support, versioning, and hard forks. This because they could not find any articles addressing these specific challenges in particular.

The business blockchain: promise, practice, and application of the next Internet technology
W. Mougayar, 2016, [26], cited by 107
This book explains the use of blockchain technologies for businesses and enterprises. Starting with summarizing what blockchain is, Satoshi Nakamotos paper, ledgers, and different application areas. Moving on to digital trust and how blockchains technology creates inherited trust. Including proofing methods and identity management, all from a more business perspective. Continuing into explaining how business need to start thinking different regarding blockchain and business challenges. Ending with an explanation of blockchain in financial systems and how these types of systems can be realized. Including the future of blockchain and other distributed system technologies in enterprises and businesses.

An overview of blockchain technology: Architecture, consensus, and future trends
Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, 2017, [27], cited by 96
This conference article gives an overview of blockchain technology with a specific focus on consensus algorithms and research related to them. But it start with giving an overview of a typical blockchain system, including key characteristics and the used taxonomy. To then follow with a more deeper study into blockchain consensus algorithms. Explaning how Proof-of-Work is executed, but also some alternatives to PoW. Such as Proof-of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Delegated Proof-of-Stake (DPOS), Ripple, and Tendermint. They also make a comparison between them in terms of energy saving, node management, and tolerated power adversary. Finally, it presents current challenges in terms of scalability, privacy leakage, selfish mining, and some other future directions of blockchain. Overall, this article gives a good view and perspective of consensus algorithms and their problems. Which is very interesting, because of the key position these hold for creating a well functional and future proof blockchain system.

Blockchain challenges and opportunities: A survey
Z. Zheng, S. Xie, H.N. Dai, H. Wang, 2018, [28], cited by 90
This journal article is very similar to the previous conference article [27], made by many of the same authors. This seems to be a follow up article to it, presented a year later with more and updated information in almost all sections. It follow the same structure and has much of the same information, but because of its length of a journal article, it holds more details than the previous article. Most importantly explaining the consensus algorithms in more detail and presenting more examples of blockchain applications.

Blockchain for the Internet of Things: A systematic literature review

M. Conoscenti, A. Vetro, Antonio, M. De, C. Juan, 2016, [29], cited by 80
This article presents a study on the intersection of blockchain and IoT technologies. Primarily focusing on evaluating and presenting the research articles in this intersection. Thus, the major outcome from this article is a collection references. The articles they found was split into five categories: Use cases and IoT, implementation differences with Bitcoin, integrity problems, anonymity problems, and adaptability. With between 5 and 20 articles in each category. To then have a more deeper discussion on these categories, what implications they will have for IoT, future research, etc.

B. Articles that Analyze Blockchain Technology

This category of papers includes papers which investigates, highlights, or analyses the blockchain technology itself. Including studies on how it works in certain scenarios, analysis on the protocol, and performance of the technology. From all the papers that have been found in this survey, the following papers have been identified to fall under this specific category:

Majority is not enough: Bitcoin mining is vulnerable
I Eyal, EG Sirer, 2018, [30], cited by 621

Bitcoin: Economics, technology, and governance
R Bhme, N Christin, B Edelman, T Moore, 2015, [31], cited by 417

Information propagation in the bitcoin network
C Decker, R Wattenhofer, 2013, [32], cited by 386

The bitcoin backbone protocol: Analysis and applications
J Garay, A Kiayias, N Leonardos, 2015, [33], cited by 349

The truth about blockchain
M Iansiti, KR Lakhani, 2017, [34], cited by 254

The truth about blockchain
M Iansiti, KR Lakhani, 2017, [34], cited by 254

On the security and performance of proof of work blockchains
A Gervais, GO Karame, K Wst, V Glykantzis, H. Ritzdorf, S Capkun, 2016, [35], cited by 193

Bitcoin-asset or currency? revealing users' hidden intentions
Glaser, K Zimmermann, M Haferkorn, M Weber, M Siering, 2014, [36], cited by 168

Decentralized blockchain technology and the rise of lex cryptographia
A Wright, P De Filippi, 2015, [37], cited by 167

Bitcoin mining and its energy footprint
KJ O'Dwyer, D Malone, 2014, [38], cited by 153

Understanding Bitcoin: Cryptography, engineering and economics
P Franco, 2014, [39], cited by 150

Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab
K Delmolino, M Arnett, A Kosba, A Miller, E Shi, 2016, [40], cited by 140

Analysis of the blockchain protocol in asynchronous networks
R Pass, L Seeman, A Shelat, 2017, [41], cited by 135

Some simple economics of the blockchain
C Catalini, JS Gans, 2016, [42], cited by 97

Blockchain-the Gateway to Trust-Free Cryptographic Transactions
R Beck, JS Czepluch, N Lollike, S Malone, 2016, [43], cited by 80

Economics of blockchain
S Davidson, P De Filippi, J Potts, 2016, [44], cited by 76

The problem with Bitcoin
D Bradbury, 2013, [45], cited by 75

A taxonomy of blockchain-based systems for architecture design
X Xu, I Weber, M Staples, L Zhu, J Bosch, L Bass, C Pautasso, P Rimba, 2017, [46], cited by 75

Blockchain technology in healthcare: The revolution starts here
M Mettler, 2016, [47], cited by 74

C. Articles on Blockchain Improvements and Variants

This category of papers includes papers which investigates, or proposes improvement or variants of blockchains. Including studies on compairons between old and new systems, different enhancements, new cryptocurrencies, and new blockchain methods. From all the papers that have been found in this survey, the following papers have been identified to fall under this specific category:

Bitter to betterhow to make bitcoin a better currency
S Barber, X Boyen, E Shi, E Uzun, 2012, [48], cited by 409

Bitcoin-NG: A Scalable Blockchain Protocol
I Eyal, AE Gencer, EG Sirer, R Van Renesse, 2016, [49], cited by 293

The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication
M Vukoli, 2015, [50], cited by 232

Enhancing bitcoin security and performance with strong consistency via collective signing
EK Kogias, P Jovanovic, N Gailly, I Khoffi, L Gasser, B Ford, 2016, [51], cited by 146

Enabling blockchain innovations with pegged sidechains
A Back, M Corallo, L Dashjr, M Friedenbach, G Maxwell, A Miller, A Poelstra, T Jorge, P Wuille, 2014, [52], cited by 138

Bitiodine: Extracting intelligence from the bitcoin network
M Spagnuolo, F Maggi, S Zanero, 2014, [53], cited by 117

A fast and scalable payment network with bitcoin duplex micropayment channels
C Decker, R Wattenhofer, 2015, [54], cited by 105

Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability
X Liang, S Shetty, D Tosh, C Kamhoua, K Kwiat, L Njilla, 2017, [55], cited by 76

D. Articles on Different Blockchain Applications

This category of papers includes papers which investigates different applications of blockchains. Including proposal of new types of applications and applications areas. Both in terms of solving new types of problems and in terms of privacy or security enablers. From all the papers that have been found in this survey, the following papers have been identified to fall under this specific category:

Hawk: The blockchain model of cryptography and privacy-preserving smart contracts
A Kosba, A Miller, E Shi, Z Wen, C Papamanthou, 2016,[56], cited by 411

Decentralizing privacy: Using blockchain to protect personal data
G Zyskind, O Nathan, 2015, [57], cited by 388

Architecture of the hyperledger blockchain fabric
C Cachin, 2016, [58], cited by 176

The bitcoin lightning network: Scalable off-chain instant payments
J Poon, T Dryja, 2016, [59], cited by 170

A survey of attacks on ethereum smart contracts (sok)
N Atzei, M Bartoletti, T Cimoli, 2017, [60], cited by 168

Medrec: Using blockchain for medical data access and permission management
A Azaria, A Ekblaw, T Vieira, A Lippman, 2016, [61], cited by 167

Ouroboros: A provably secure proof-of-stake blockchain protocol
A Kiayias, A Russell, B David, R Oliynykov, 2017, [62], cited by 149

Blockchain for IoT security and privacy: The case study of a smart home
A Dorri, SS Kanhere, R Jurdak, G Praveen, 2017, [63], cited by 126

Blockstack: A Global Naming and Storage System Secured by Blockchains
M Ali, JC Nelson, R Shea, MJ Freedman, 2016, [64], cited by 123

Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control
X Yue, H Wang, D Jin, M Li, W Jiang, 2016, [65], cited by 116

Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams
NZ Aitzhan, D Svetinovic, 2018, [66], cited by 101

Untrusted business process monitoring and execution using blockchain
I Weber, X Xu, R Riveret, G Governatori, A Ponomarev, J Mendling, 2016, [67], cited by 98

An agri-food supply chain traceability system for China based on RFID and blockchain technology
F Tian, 2016, [68], cited by 96

The blockchain as a software connector
X Xu, C Pautasso, L Zhu, V Gramoli, V Ponomarev, AB Tran, S Chen, 2016, [69], cited by 95

Blockchain technology and decentralized governance: Is the state still necessary?
M Atzori, 2015, [70], cited by 90

Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems
T Swanson, 2015, [71], cited by 85

Trusting records: is Blockchain technology the answer?
VL Lemieux, 2016, [72], cited by 81

Towards blockchain-based intelligent transportation systems
Y Yuan, FY Wang, 2016, [73], cited by 74

E. Articles Discussing the Future of Blockchain

The final category of papers were articles that focuses on the future of blockchain, giving outlooks and predictions on how blockchain technologies will be used in the future. Hence, this category highlights future problems, challenges, and usages of the technology. The following papers have been identified to fall under this category:

Blockchain technology: Beyond bitcoin
M Crosby, P Pattanayak, S Verma, V Kalyanaraman, 2016, [74], cited by 194

Blockchain beyond bitcoin
S Underwood, 2016, [75], cited by 159

Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money
GW Peters, E Panayi, 2016, [76], cited by 159

Beyond bitcoin: Issues in regulating blockchain transactions
TI Kiviat, 2015, [77], cited by 103

IV. Blockchain and GDPR

The General Data Protection Regulation (GDPR) enacted by the European Union is a piece of legislation that was designed to protect the data of those living in the EU. It came into effect on may 25 2018 and has among many things made it illegal for companies to keep personal information about people living in EU, if they have been asked to be removed. However, the immutable nature of blockchain systems makes is almost impossible to adhere to these demands. Simply because data can never be removed from blockchains and that the data generally is open to everyone that can access the chain [78], [79]. The regulatory agencies have also been reluctant and skeptical to except blockchains from this legislation, so the legislation and technology stands in direct conflict to each other. However, both blockchains and GDPR somehow comes from the same spirit and way of thinking. Both have been created as a way to go forward, when the large companies or banks are not to be trusted to not to bad things with their power position or collected information. Hence, the two does not have to be enemies. Blockchains can also be seen as a great asset in data protection work [80], [81].

The solution to making blockchains GDPR compliant also lies in the technology and in the creation of a blockchain variant that have immutability but at the same time the ability to forget data [82], [83]. Firstly, there is a differences between public and private blockchains, especially on the accountability. Since no one is formally in control over the public blockchains, they should never be used to store personal information. But for private or permissioned blockchains, there are some options. Traditional databases follow the Create-Read-Update-Delete (CRUD) model for operations, with the common functions that we expect to see from a database system. Some GDPR compliant blockchains have been proposed and they generally follow a Create-Retrieve-Append-Burn model instead [84]. Meaning that it is impossible to update data and to delete data, but you can append and burn certain pieces of data. Where the burn part is most interesting from a GDPR perspective, what is the difference between burning and deleting data? Well one way of interpreting the burn operation is to see it as throwing away encryption keys so you are unable to decrypt the actual data that is written in the blockchain. Hence, the data remains in the blockchain, but is for all intents and purposes unable to be read since there is no one has the decryption key. This method is generally called cryptography data deletion, meaning that the data is still there on the distributed chain but can never be decrypted and used. Another way of creating GDPR complient blockchains is to use so called side chains or off chains. Meaning that the data itself is stored in an outside database, which then is linked to the blockchain via public and private encryption keys. This way of storing data also seems to be beneficial for other purposes, since it makes the blockchain not grow so much in size for each block. Since each block only contains links to data, not the data itself. Thus, avoiding storing personal information on the chain itself.

The effects of GDPR have not yet settled and the extent as well as the penalties have not been formally tested yet. But it is obvious that there are GDPR issues with blockchain technologies and the ways of circumventing them needs to be explored further in both research and in the extent of the legislation.

V. Conclusions and Outlook

This work has been a study of the state of the art of blockchain technology landscape. Which made an overview of the blockchain technology itself, as well as a deeper look into the existing research articles, and potential research areas. Including a look at the timeline of research publications, its hype curve, and interest in media. Hence, the intent of this work was to create understand of the technologies, as well as inspire further research work and identifying potential knowledge gaps.

From our perspective, the outlook for blockchain technologies are extremely interspersing but there are problems and challenges which needs to be solved before global proliferation. For example challenges in security, 51% attacks, authentication, data malleability, latency, throughput, size, and bandwidth. But also in terms of personal privacy, personal information, the right to be forgotten, and GDPR. Blockchains in its original form is also extremely energy wasteful. Proof-of-Work is not the future, we need to apply other forms of consensus and byzantine fault tolerance. There is also developer side problems, where there currently is no clear front runner among the different products that exists, not even a front running company. There is also no consensus on the usability, developer support, end user support, and how the blockchains should be integrated into other systems. Which also creates problems with versions of chains, forks of chains, multiple chains, side chains. etc.

Finally, blockchain systems are highly dependent on the currently available hash puzzles and asymmetric encryption. So if anyone of these fails, or if a weakness is discovered, the chain is no longer trusted and is useless. For example, what will happen in the future with quantum computers? Or some other yet unknown and undiscovered weakness.

ACKNOWLEDGMENT

This work was done as a part of pre-study project into blockchain technologies (MIUN-2018/1011), financed by the Swedish Social Insurance Agency (Försäkringskassan) and Mid Sweden University. This work has also partially been financed by project 17-336 by the Åforsk foundation. Finally, the author would like to thank Lars Våge and Johanna Österåker for their aid with the historical database searches for this research and Mehrzad Lavassani for her aid in classifying all the blockchain articles.

REFERENCES

[1] D. Drescher, *Blockchain basics*. Apress, 2017.

[2] B. Singhal, G. Dhameja, and P. S. Panda, *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*. Apress, 2018.

[3] B. Marr, "A short history of bitcoin and crypto currency everyone should read," Dec 2017. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/

[4] "Bitcoin history: The complete history of bitcoin [timeline]." [Online]. Available: http://historyofbitcoin.org/

[5] "History of bitcoin," Nov 2018. [Online]. Available: https://en.wikipedia.org/wiki/History_of_bitcoin

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[7] J. I. Wong, "Bitcoin's latest record high makes satoshi nakamoto the 247th richest person in the world," Oct 2017. [Online]. Available: https://qz.com/1107843/bitcoins-btc-new-record-price-of-6000-means-satoshi-nakamoto-is-worth-5-9-billion/

[8] "Satoshi nakamoto institute." [Online]. Available: https://nakamotoinstitute.org/

[9] D. Chaum, "Blind signatures for untraceable payments," in *Advances in cryptology*. Springer, 1983, pp. 199–203.

[10] D. Chaum and S. Brands, "'minting'electronic cash," *IEEE spectrum*, vol. 34, no. 2, pp. 30–34, 1997.

[11] A. Back, "Hashcash - a denial of service counter-measure," 09 2002.

[12] [Online]. Available: http://www.weidai.com/bmoney.txt

[13] N. Szabo, "Unenumerated," Jan 1970. [Online]. Available: http://unenumerated.blogspot.com/2005/12/bit-gold.html

[14] D. Oberhaus, "The world's oldest blockchain has been hiding in the new york times since 1995," Aug 2018. [Online]. Available: https://motherboard.vice.com/en_us/article/j5nzx4/what-was-the-first-blockchain

[15] N. Bie, "Ny piratvaluta kan hota finanssystemen," May 2011. [Online]. Available: https://www.svt.se/2.22584/1.2439316/ny_piratvaluta_kan_hota_finanssystemen

[16] ——, "Hr kan man spendera piratpengar," May 2011. [Online]. Available: https://www.svt.se/2.22584/1.2439344/har_kan_man_spendera_piratpengar

[17] A. Lotsson, "Bitcoin-valutan blir notarie," May 2013. [Online]. Available: https://computersweden.idg.se/2.2683/1.509172/bitcoin-valutan-blir-notarie

[18] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[19] A. M. Antonopoulos, *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2014.

[20] ——, *Mastering Bitcoin: Programming the open blockchain*. " O'Reilly Media, Inc.", 2017.

[21] D. Tapscott and A. Tapscott, *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin, 2016.

[22] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE, 2015, pp. 104–121.

[23] M. Pilkington, "Blockchain technology: principles and applications," *Research handbook on digital transformations*, p. 225, 2016.

[24] F. X. Olleros and M. Zhegu, *Research handbook on digital transformations*. Edward Elgar Publishing, 2016.

[25] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?a systematic review," *PloS one*, vol. 11, no. 10, p. e0163477, 2016.

[26] W. Mougayar, *The business blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons, 2016.

[27] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Big Data (BigData Congress), 2017 IEEE International Congress on*. IEEE, 2017, pp. 557–564.

[28] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web and Grid Services*, vol. 14, no. 4, 2018.

[29] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the internet of things: A systematic literature review," in *Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of*. IEEE, 2016, pp. 1–6.

[30] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Communications of the ACM*, vol. 61, no. 7, pp. 95–102, 2018.

[31] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213–38, 2015.

[32] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*. IEEE, 2013, pp. 1–10.

[33] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2015, pp. 281–310.

[34] M. Iansiti and K. R. Lakhani, "The truth about blockchain," *Harvard Business Review*, vol. 95, no. 1, pp. 118–127, 2017.

[35] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 3–16.

[36] F. Glaser, K. Zimmermann, M. Haferkorn, M. Weber, and M. Siering, "Bitcoin-asset or currency? revealing users' hidden intentions," *SSRN*, 2014.

[37] A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," *SSRN*, 2015.

[38] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," *IET Conference Proceedings*, 2014.

[39] P. Franco, *Understanding Bitcoin: Cryptography, engineering and economics*. John Wiley & Sons, 2014.

[40] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, "Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab," in *International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 79–94.

[41] R. Pass, L. Seeman, and A. Shelat, "Analysis of the blockchain protocol in asynchronous networks," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2017, pp. 643–673.

[42] C. Catalini and J. S. Gans, "Some simple economics of the blockchain," National Bureau of Economic Research, Tech. Rep., 2016.

[43] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, "Blockchain-the gateway to trust-free cryptographic transactions." in *ECIS*, 2016, p. ResearchPaper153.

[44] S. Davidson, P. De Filippi, and J. Potts, "Economics of blockchain," *SSRN*, 2016.

[45] D. Bradbury, "The problem with bitcoin," *Computer Fraud & Security*, vol. 2013, no. 11, pp. 5–8, 2013.

[46] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, "A taxonomy of blockchain-based systems for architecture design," in *Software Architecture (ICSA), 2017 IEEE International Conference on*. IEEE, 2017, pp. 243–252.

[47] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on*. IEEE, 2016, pp. 1–3.

[48] S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to betterhow to make bitcoin a better currency," in *International Conference on Financial Cryptography and Data Security*. Springer, 2012, pp. 399–414.

[49] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol." in *NSDI*, 2016, pp. 45–59.

[50] M. Vukolić, “The quest for scalable blockchain fabric: Proof-of-work vs. bft replication,” in *International Workshop on Open Problems in Network Security*. Springer, 2015, pp. 112–125.

[51] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, “Enhancing bitcoin security and performance with strong consistency via collective signing,” in *25th USENIX Security Symposium (USENIX Security 16)*, 2016, pp. 279–296.

[52] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, “Enabling blockchain innovations with pegged sidechains,” *URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*, 2014.

[53] M. Spagnuolo, F. Maggi, and S. Zanero, “Bitiodine: Extracting intelligence from the bitcoin network,” in *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 457–468.

[54] C. Decker and R. Wattenhofer, “A fast and scalable payment network with bitcoin duplex micropayment channels,” in *Symposium on Self-Stabilizing Systems*. Springer, 2015, pp. 3–18.

[55] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, “Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability,” in *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*. IEEE Press, 2017, pp. 468–477.

[56] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 839–858.

[57] G. Zyskind, O. Nathan *et al.*, “Decentralizing privacy: Using blockchain to protect personal data,” in *Security and Privacy Workshops (SPW), 2015 IEEE*. IEEE, 2015, pp. 180–184.

[58] C. Cachin, “Architecture of the hyperledger blockchain fabric,” in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, vol. 310, 2016.

[59] J. Poon and T. Dryja, “The bitcoin lightning network: Scalable off-chain instant payments,” *See https://lightning. network/lightning-network-paper. pdf*, 2016.

[60] N. Atzei, M. Bartoletti, and T. Cimoli, “A survey of attacks on ethereum smart contracts (sok),” in *Principles of Security and Trust*. Springer, 2017, pp. 164–186.

[61] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “Medrec: Using blockchain for medical data access and permission management,” in *Open and Big Data (OBD), International Conference on*. IEEE, 2016, pp. 25–30.

[62] A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A provably secure proof-of-stake blockchain protocol,” in *Annual International Cryptology Conference*. Springer, 2017, pp. 357–388.

[63] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for iot security and privacy: The case study of a smart home,” in *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*. IEEE, 2017, pp. 618–623.

[64] M. Ali, J. C. Nelson, R. Shea, and M. J. Freedman, “Blockstack: A global naming and storage system secured by blockchains.” in *USENIX Annual Technical Conference*, 2016, pp. 181–194.

[65] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control,” *Journal of medical systems*, vol. 40, no. 10, p. 218, 2016.

[66] N. Z. Aitzhan and D. Svetinovic, “Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams,” *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2018.

[67] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, and J. Mendling, “Untrusted business process monitoring and execution using blockchain,” in *International Conference on Business Process Management*. Springer, 2016, pp. 329–347.

[68] F. Tian, “An agri-food supply chain traceability system for china based on rfid & blockchain technology,” in *Service Systems and Service Management (ICSSSM), 2016 13th International Conference on*. IEEE, 2016, pp. 1–6.

[69] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen, “The blockchain as a software connector,” in *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*. IEEE, 2016, pp. 182–191.

[70] M. Atzori, “Blockchain technology and decentralized governance: Is the state still necessary?” *SSRN*, 2015.

[71] T. Swanson, “Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems,” *Report, available online, Apr*, 2015.

[72] V. L. Lemieux, “Trusting records: is blockchain technology the answer?” *Records Management Journal*, vol. 26, no. 2, pp. 110–139, 2016.

[73] Y. Yuan and F.-Y. Wang, “Towards blockchain-based intelligent transportation systems,” in *Intelligent Transportation Systems (ITSC), 2016 IEEE 19th International Conference on*. IEEE, 2016, pp. 2663–2668.

[74] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: Beyond bitcoin,” *Applied Innovation*, vol. 2, pp. 6–10, 2016.

[75] S. Underwood, “Blockchain beyond bitcoin,” *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[76] G. W. Peters and E. Panayi, “Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money,” in *Banking Beyond Banks and Money*. Springer, 2016, pp. 239–278.

[77] T. I. Kiviat, “Beyond bitcoin: Issues in regulating blockchain tranactions,” *Duke LJ*, vol. 65, p. 569, 2015.

[78] D. Pollock, “How can blockchain thrive in the face of european gdpr blockade?” Oct 2018. [Online]. Available: https://www.forbes.com/sites/darrynpollock/2018/10/03/how-can-blockchain-thrive-in-the-face-of-european-gdpr-blockade/#66b754f861df

[79] “The gdpr and blockchain,” Aug 2018. [Online]. Available: https://www.insideprivacy.com/international/european-union/the-gdpr-and-blockchain/

[80] L. Mearian, “Will blockchain run afoul of gdpr? (yes and no),” May 2018. [Online]. Available: https://www.computerworld.com/article/3269750/blockchain/will-blockchain-run-afoul-of-gdpr-yes-and-no.html

[81] C. Sweden, “Krockar blockkedjan med gdpr? ja och nej,” May 2018. [Online]. Available: https://computersweden.idg.se/2.2683/1.702061/blockkedjan-gdpr

[82] “Tre nycklar till framgng i blockchain-revolutionen.” [Online]. Available: https://computersweden.idg.se/2.2683/1.697424/blockchain-framgang

[83] B. D. Journal, “Here’s how gdpr and the blockchain can coexist,” Jul 2018. [Online]. Available: https://thenextweb.com/syndication/2018/07/26/gdpr-blockchain-cryptocurrency/

[84] A. V. Humbeeck, “The blockchain-gdpr paradox wearetheledger medium,” Nov 2017. [Online]. Available: https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047