BRL Working Paper Series No. 10

Smart Contracts on the Blockchain – A Bibliometric Analysis and Review

Lennart Ante [1, 2, *]

[1] Blockchain Research Lab, Colonnaden 72, 22303 Hamburg
[2] University of Hamburg, Faculty of Business, Economics & Social Sciences, Von-Melle-Park 5, 20146 Hamburg, Germany

* Correspondence: ante@blockchainresearchlab.org

Published: 15 Apr 2020 (revised 15 Sep 2020)

Abstract: Smart contracts are decentrally anchored scripts on blockchains or similar infrastructures that allow the transparent execution of predefined processes. Using smart contracts, assets like money become programmable, which opens up previously inaccessible application potential. To date, smart contracts control billions in value. This paper analyzes 468 peer-reviewed articles on the topic of smart contracts and their 20,188 references, providing a summary and analysis of the current state of research on smart contracts. Using exploratory factor analysis for co-citation analysis, we identify six different strands of research that concern technical, social, economic and legal disciplines: I) technical foundations, development and open questions of blockchain networks, II) blockchain and smart contracts for the Internet of Things, III) smart contract standardization, verification and security, IV) blockchain and smart contracts for the disruption of existing processes and industries, V) potentials and challenges of smart contracts, and VI) smart contracts and the law. The interrelations between these groups are visualized using social network analysis. We thus obtain a structured overview of the main strands of research concerning smart contracts, their development over time, the relevance of smart contract platforms in research, and conceptual connections between publications and discourses. The results offer researchers and practitioners a substantial basis for their work on smart contracts.

Keywords: Distributed ledger; Ethereum; Informetric analysis; Internet of Things; Social network analysis

1 Introduction

The idea of Bitcoin was to enable private digital cash by solving the double-spending problem and thus allowing individuals to transfer money without the need for financial intermediaries (Nakamoto 2008). While Bitcoin aimed to disintermediate the financial industry, the underlying blockchain technology allows for some degree of disintermediation in almost any sector. Any asset or data can be transferred peer-to-peer (p2p) without the need for a 'trusted' intermediary. In addition, predefined

processes can be anchored decentrally on the blockchain by means of computer code that prescribes a certain reaction to new information, e.g. an incoming transaction. Such scripts are known as smart contracts. They take the scale and potential of decentralized systems to the next level, as predefined processes or even contracts can be executed in full transparency and without external influence. Such programmed processes can be of any degree of complexity. For example, a smart contract can simply forward a transaction to another entity or address. More complex structures for example anchor values on the blockchain through so-called token (smart) contracts. This way, digital tokens, i.e. cryptocurrencies, are issued and can then be transferred by users. The ten biggest blockchain-based tokens account for a combined market capitalization of over $11 billion in early 2020 (etherscan.com/tokens), which illustrates the relevance of this application. In sum, smart contracts enable the digital programming of values and self-enforceable processes on a distributed infrastructure. However, since smart contract applications have only been possible for a few years, the numerous potentials are faced with just as many challenges. Against this background, a systematic review and analysis of the state of research can offer clear added value.

There are different methods of analyzing literature data. In traditional literature analysis, a comparatively small number of publications on a certain topic are qualitatively examined in order to summarize research results, to look at a research area from different angles and to derive future research. There exist different approaches, such as scoping reviews or systematic reviews. In bibliometric analysis, comparatively large amounts of literature are analyzed using statistical software. The object of investigation are rather indicators and (visual) connections than the actual content of the publications under consideration. The goal is to identify intellectual structures and emerging trends. To date, various literature analyses, surveys or reviews on the topic of smart contracts are available: Alharby and Moorsel (2018) analyzed 24 papers from various databases, finding that two thirds of them relate to the identification and resolution of smart contract-related issues. Macrinici et al. (2018) grouped 64 smart contract-related papers based on publication sources, channels, methods and approaches, and concluded that common points of discussion relate to security, privacy and scaling of blockchains as well as smart contract programmability. The systematic review article of Udokwu et al. (2018) provides an analysis of the use of smart contracts in organizations. Other literature reviews analyze specific smart contract areas like blockchain-based reputation systems (Almasoud et al. 2020), verification (Almakhour et al. 2020), formalization (Singh et al. 2019) or the maintenance of smart contracts on the Ethereum blockchain (J. Chen et al. 2020). While bibliometric studies have analyzed blockchain technology (Ante 2020; Firdaus et al. 2019; Klarin 2020; Miau and Yang 2018), there is currently only one such study that explicitly addresses the topic of smart contracts. Salmerón-Manzano and Manzano-Agugliaro (2019) descriptively and visually analyzed literature on smart contracts extracted from the Scopus database and identified two research trends for smart contracts in the context of sustainability: e-commerce and power grids. However, so far there is no bibliometric study that analyses co-citation data on the smart contract literature using explorative factor analysis. Accordingly, we see a bibliometric analysis using empirical methods as a relevant basis for an objective investigation to better understand the scientific environment of smart contracts.

The present paper aims to provide a bibliometric analysis of the literature on smart contracts and thus to gain a fundamental overview of current research trends and statistics and the scientific discourses into which the research area is divided. The trend-setting publications on which research on smart contracts is based are reviewed to gain a detailed understanding of the higher-level intellectual

structures and to identify potential starting points for future research. For objective results, we rely on co-citation analysis and explorative factor analysis. In addition, (social) network analysis is applied to uncover and analyze relationships between keywords, jurisdictions and different discourses and their constituent publications. Smart contracts are an interdisciplinary topic that combine aspects of law, economics and technology. Our analysis is explicitly interdisciplinary in order to uncover connections and/or potential gaps in smart contract research discourses.

The paper is structured as follows: Section 2 provides an overview of the data extraction methodology and the statistical and visual methods of analysis. Section 3 introduces the concept of smart contracts (3.1). Subsequently, descriptive findings are derived from the primary data set extracted from the Web of Science (3.2). The fourth section presents our findings on research streams based on co-citation analysis and then describes and analyzes individual strands of research (Sections 4.1 through 4.6). Section 4.7 examines the interrelations of the different research streams via social network analysis. In Section 5, results on the state of smart contract research (5.1) and its intellectual foundations (5.2) are discussed. Future research paths are presented in Section 6. Finally, Section 7 contains concluding remarks.

2 Data and methods

2.1 Search strategy and primary data set

The bibliographic data set was collected in January 2020 from the Web of Science Core Collection using the search term *TS=("smart contract*")*. Web of Science represents a common source for bibliometric studies (Zupic and Čater 2015), while, for example, Scopus is a suitable alternative. By using a curated data base – and not a more open source like, for example, Google Scholar, - the initial quality of the data (i.e. only peer reviewed publications) is ensured. As bibliometric data is highly skewed, it is sufficient to focus on the most relevant studies of a discourse (Ye-Sho Chen and Leimkuhler 1986). Of course, this comes with the limitation that potentially relevant literature, like non-indexed research papers or grey literature is not included and the choice of a different database could lead to varying results. The search, which was constrained to peer-reviewed articles, conference proceedings and book chapters, returned 468 articles. All of them appeared to be related to our topic, so none were excluded after an initial screening of abstracts. Some articles included were published in legal journals that may not classify as 'peer reviewed' but use reviews of student editors (e.g. Werbach and Cornell (2017) published in the Duke Law Journal). These articles were not removed.

2.2 Co-citation analysis and secondary data set

The 468 articles in the primary data set contain 20,188 references (15,714 unique publications), which form the basis of the secondary data set and empirical investigation. Inconsistent references were standardized. For example, the Bitcoin whitepaper was referenced in five different ways. For the subsequent empirical investigation, we analyze (co-)citation data.

Co-citation analysis allows us to identify temporal relationships between the articles. If two articles refer to the same source, we speak of co-citation and conclude that these two articles were published after the article they both cite. The more co-citations an article has, the higher its relevance for a corresponding research field (Small 1973, 1977). As bibliometric data are generally highly skewed, a small proportion of the literature generates the highest added value. This makes it unnecessary to

analyze all of the cited articles; instead, it suffices to examine the most relevant ones. Therefore, as well as for the purpose of statistical significance via Kaiser-Meyer-Olkin (KMO) measure and Bartlett test statistic, we choose a cutoff value of 5 co-citations, which yields 381 publications. The primary data set thus consists of the 381 most-referred (co-cited) sources of the primary data set, which represent the top 2.4% of all unique references.

2.3 Exploratory factor analysis for co-citation analysis

In order to analyze co-citation data using factor analysis, a so-called co-citation matrix is created. Sources and their respective co-citation counts are transferred into a square similarity matrix, whose diagonal values are replaced with the means of the respective column (McCain 1990; Small 1973). For this purpose we use the Bibexcel software (Persson et al. 2009), which enables the simple preparation of data exported from Web of Science for subsequent use in SPSS for exploratory factor analysis. The final co-citation matrix comprises the 381 most relevant articles based on the number of co-citations.

To identify objective research streams on the basis of the available sources, we use exploratory factor analysis, a common method for the investigation of bibliometric data (e.g. Ante 2020; Wörfel 2019; Zuschke 2019). That way, we are able to identify the underlying structure of the data without the need for any prior hypotheses or assumptions. The symmetrical co-citation matrix is statistically divided into contiguous factors, which represent research streams if we assume that similar underlying sources suggest similar research areas and ideas. While a total of 46 factors are extracted, based on a scree plot and a relatively large drop in the eigenvalues and explained variance, we retain for further analysis six final factors, all of which have eigenvalues above 1. The factor analysis relies on principal component analysis and Varimax rotation with Kaiser normalization (Kaiser 1959).

In the further analysis of the factors, we employ two different metrics: factor loadings and factor scores. Factor loadings are numerical values between 1 and -1 that represent the strength and orientation of a variable (i.e. an article) with respect to a factor (i.e. a research stream). A factor loading above 0.4 indicates that a variable is part of a factor, i.e. that a publication fits into a research stream, and a factor loading above 0.7 indicates that a variable is highly relevant to a factor (McCain 1990). Factor scores, which we determine by means of regression, indicate how thematically relevant a variable is to a factor - regardless of whether it fits well into that factor (DiStefano et al. 2009; Gorsuch 1988). For example, the Bitcoin whitepaper may not fit well into a research stream on smart contracts but is nevertheless highly relevant to the discourse. Thus, we would expect the publication to have a low factor loading and a high factor score with respect to that particular research stream.

2.4 Network analysis

For the network analysis of the primary data set, we use the VOSviewer software (van Eck and Waltman 2010) to visualize co-occurrence networks. The VOSviewer mapping software uses the association strength similarity measure, also known as the proximity index or probabilistic affinity index (van Eck and Waltman 2007). The method calculates the similarity s_{ij} between items i and j as the number of co-occurrences (c_{ij}) of items divided by the sum of occurrences of the items (w_i and w_j): $s_{ij} = \frac{c_{ij}}{w_i w_j}$. The visualization of items is then mapped on a two-dimensional map, where similarity

of items is mapped as closely as possible by placing them in close proximity to each other. Colored clusters are then obtained based on similarity (van Eck and Waltman 2010).

Social network analysis can reveal dependencies and relationships between individual publications and the overall research streams. We use the UCINET software (specifically the NetDraw algorithm) (Borgatti et al. 2002) for analysis and visualization of the secondary data set. It displays the intellectual proximity between articles in two dimensions based on their number of co-citations (Biehl et al. 2006; Borgatti et al. 2002). The software generates a set of coordinates by arranging Euclidean distances in relation to the geodesic distance between the publications. The result is a network image of the entire research field (Carrington et al. 2005), where each publication is represented as a node, whose size corresponds to the article's number of citations and whose color indicates its association with a research stream. Lines between the nodes indicate co-citations.

3 Smart contracts

3.1 An introduction to smart contracts

A smart contract is a script that is anchored on a blockchain or similar distributed infrastructure. As soon as it is triggered by a blockchain transaction and validated across the network, predefined actions are executed. Since the conditions of a smart contract are transparently stored on the blockchain, it will always operate as all parties intend, which can reduce trust issues between the involved parties. Smart contracts are software scripts, just like scripts that run on non-blockchain applications.

The term smart contract and the underlying idea date from long before the emergence of Bitcoin and blockchain technology. Szabo (1994) defined a smart contract as a piece of computerized transaction protocol that satisfies contractual conditions such as payment terms, confidentiality or enforcement, reduces exceptions and minimizes the need for trusted intermediaries. He mentioned digital cash protocols as examples of smart contracts, as the mechanisms allow for online payment in combination with paper cash characteristics, like divisibility and confidentiality. In a later publication, Szabo (1997) described smart contracts as the combination of protocols with user interfaces to ensure formal and secure relationships via networks. The design of such systems builds on legal, economic and technical foundations. Thus, smart contracts require interdisciplinary analysis.

Both the term 'smart' and the term 'contract' are misleading, since a smart contract consists of 'dumb' computer code and rarely represents a legally binding construct. The founder of Ethereum fittingly stated: "I quite regret adopting the term *smart contracts*. I should have called them something more boring and technical, perhaps something like *persistent scripts*" (Buterin 2018). Regarding the quality of smart contracts as legally binding contracts, different degrees can be distinguished: Smart contracts may be 1) simple computer code that does not represent any legal contract but simply executes a predefined logic, 2) computer code that has certain legalese properties, i.e. a program with a predefined logic based on legal structures that is expected to act in a certain way or 3) the (partial) execution of legalese (e.g. a contract) through computer code, where the code resembles the legalese.

A simple example of a smart contract is an automated hotel room management system: As soon as a customer leaves the room, the smart contract is automatically notified. For example, a device connected to the room door acts as a so-called oracle that initiates transactions on the blockchain whenever the door is used. This in turn triggers predefined processes, such as billing or the automatic assignment of cleaning staff. Smart contracts may represent legally binding processes (e.g. billing)

but may also serve more mundane purposes (e.g. assigning cleaning staff). Figure 1 shows the basic working of a smart contract using the hotel room example. Managing a hotel room is essentially a centralized process executed by a single company, so the use of smart contracts on a blockchain may initially seem unnecessary. However, as soon as the process involves other entities (e.g. customers and external service providers), whom the hotel provider does not necessarily trust, a distributed infrastructure and smart contracts can help to reduce trust issues and improve processes efficiency. Information is logged transparently and forgery-proof on the blockchain and predefined processes are initiated without delay.

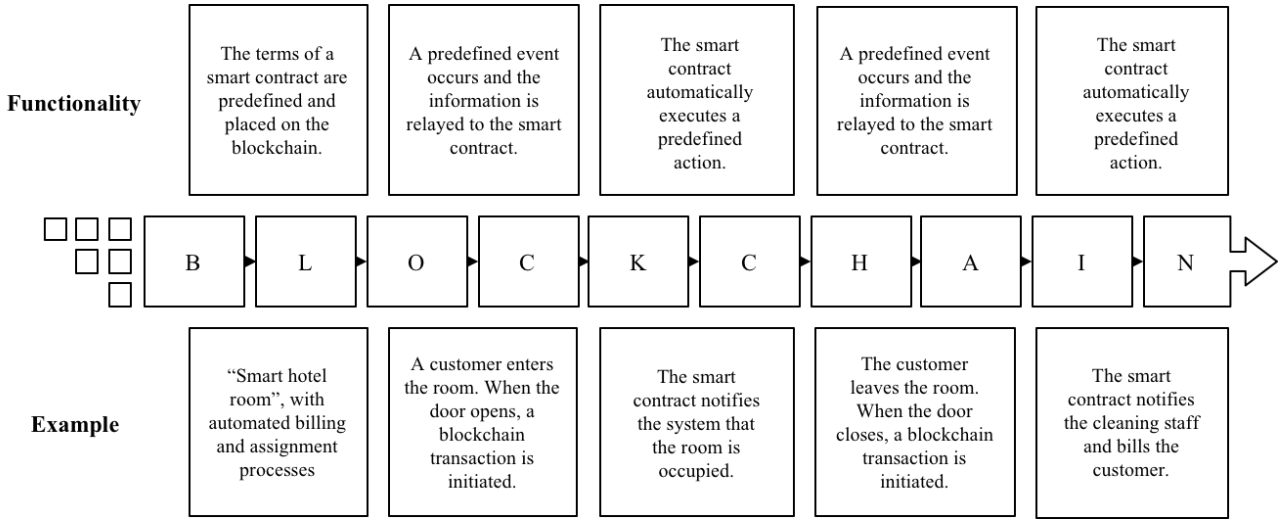

Figure 1. Exemplary functionality of a smart contract.

Blockchain technology, which enables the secure transfer of value p2p via the internet between non-confiding parties, for the first time offered a suitable distributed infrastructure for the application of smart contracts. Once the predefined terms are met, the blockchain will transparently execute the code, and no external entity can interfere. Any party with access to the blockchain can see the underlying code, which removes the need for counterparty trust. The use of one single shared 'contract' obviates the need to interpret terms and conditions, and processing can happen in real time. Additionally, digital signatures ensure transparency regarding the sender of the transactions that triggered the smart contract.

While smart contracts promise a wide range of benefits and potential, there are just as many challenges and risks. A smart contract cannot activate itself. It comes to life only when one of its functions is explicitly called in a transaction. Therefore, smart contracts are never autonomous but always require an external event (e.g. a transaction) to trigger them. One challenge of smart contract use cases concerns the issue of processing information and events that do not directly happen on the blockchain. While a smart contract can immediately react to a blockchain transaction as the whole process is handled 'on-chain', if the required information for example concerns a person leaving a hotel room ('off-chain'), the script cannot collect the information by itself. While the blockchain provides a trusted environment, participants of a smart contract may not trust the information that is transmitted to the blockchain. This is known as the oracle problem and applies to any individuals, software or hardware involved in these processes.

In principle, blockchain is not an efficient technology: All network participants must store a copy of the blockchain, which also applies to anchored computer code. In public blockchains, smart contracts

are executed globally, meaning that every blockchain node executes the contract each time. Since computation is a deterministic process, global execution may not be strictly necessary (Greenspan 2015). Another challenge that arises from the storage of all information by all network participants is data protection. The stored data is not easily deleted, which conflicts with legal requirements such as the right to be forgotten (Finck 2018; Politou et al. 2019).

Like all software, smart contracts are prone to bugs. If a flawed smart contract is anchored on the blockchain, it becomes difficult to correct. A good example is The DAO (Jentzsch 2016), a project that collected about $150 million in digital currency from over 11,000 investors and managed it in a smart contract on the Ethereum blockchain. The project was intended as a sort of digital venture capital fund, whose investors would be able to vote on how the funds were to be used. In return, they would receive dividends based on investment performance. Shortly after the start of the project, scientists began to point out potential risks and called for the code of the smart contract to be adapted (Mark et al. 2016). In June 2016, two months after its launch, a recursive call vulnerability in the smart contract's code was exploited, allowing a hacker to withdraw a third of the funds. This happened one day after that particular risk was highlighted by the community (Wen and Miller 2016) and led to a discussion about whether code is law. It was argued that the smart contract had worked exactly as programmed and the 'hacker' had only used the functionality of the smart contract. Ultimately, the event resulted in a hard fork of the Ethereum network into the two blockchains Ethereum and Ethereum Classic. On Ethereum, The DAO and the hack were unwound, while no changes were made on Ethereum Classic.

To date, a multitude of smart contract platform exist. As Bitcoin's scripting language is severely limited, only simple smart contracts (e.g. locking a payment until a certain date) can be directly implemented on Bitcoin. Technical implementations allow the use of the Bitcoin blockchain for smart contracts via sidechains or overlay protocols. In 2013, the startup Mastercoin (today known as Omni Layer) built a protocol layer on Bitcoin that permits the generation and transfer of digital tokens, representations of value or information, via the Bitcoin network. In principle, a small amount of Bitcoin is sent and the respective information regarding the second-layer token is recorded in Bitcoin's OP Return field, which can be used to attach arbitrary data to individual transactions (Willett et al. 2015). Other solutions building on the Bitcoin network are sidechain protocols like Counterparty, which used a 1-way-peg mechanism, where Bitcoins were sent to a burn address[1] in return for the issuance of Counterparty tokens (Counterparty 2020), or Rootstock (now named RSK), which uses a 2-way-peg mechanism, where Bitcoins can be frozen to exchange them into the native token of Rootstock's sidechain, which can be used for smart contracts, and be unfrozen again to exchange them back into Bitcoins when needed (Lerner 2019).

The Ethereum project was introduced in late 2013 as a next-generation platform for smart contracts and decentralized applications (dApps) (Buterin 2013). Its blockchain infrastructure allows smart contracts of any complexity. It was essentially the first blockchain network to enable Turing-complete smart contracts, while existing solutions (e.g. Bitshares, Counterparty, Colored Coins, Mastercoin or Nxt) only allowed limited scripting functionality. Ethereum features two types of accounts: contracts

[1] In January 2014, 2,140 Bitcoins were sent to the address '1CounterpartyXXXXXXXXXXXXXXXUWLpVr' in a 'proof-of-burn' event. These were removed from circulation and Counterparty's native currency (XCP) was issued to individuals who burned Bitcoins.

and externally owned accounts. The latter work just like Bitcoin accounts and can be used to store tokens and send transactions. Accounts classified as contracts are smart contract scripts, which are in control of the account itself. Such contracts can store value, like deposited balances, and are meant to serve with specialized access policies, like automated messages, once a contract possesses sufficient funds. Blockchain transactions are used as trigger for smart contracts. Therefore, any entity can send Ether – the native currency of the Ethereum network – to the address of a contract in order to execute its code (Ethereum 2020). While Ethereum is a public smart contract platform, permissioned solutions, like the Hyperledger Project, allow smart contracts to be implemented in more secure ecosystems. For example, it is possible to determine who can participate in the network and who can confirm transactions.

Figure 2 shows the number of smart contracts created on the Ethereum blockchain between August 2015 and February 2020. The data was collected from bloxy.info, a blockchain analytics site, in March 2020. A total of 22.2 million individual smart contracts were created on Ethereum by February 2020. The spike of contracts created between October and December 2018 is likely associated with the concurrent price increase on the cryptocurrency markets. The numbers illustrate the relevance of the smart contract concept, which is employed by a large number of projects and companies. Yet, most of these contracts contain only very simple scripts. For example, 540,361 of such simple contracts have exactly the same code.[2] The biggest smart contract to date in terms of the monetary value being handled is associated with the project Tether, with a market capitalization of $4.65 billion and over 1 million Ethereum accounts holding tokens.[3] Tether is a stable coin project that issues digital tokens backed by 'off-chain' fiat currency. This way, USD-backed tokens can be transferred over the blockchain but are not subject to the same volatility risks as other cryptocurrencies.

Platforms like Mastercoin and Ethereum used initial coin offerings (ICOs) to collect funding. In ICOs, investors are sold blockchain-based tokens that represent some value. For example, in the case of Ethereum's native token Ether, the value consists in the ability to use the Ethereum platform, i.e. to transact and to deploy smart contracts (Ante et al. 2018). Financial instruments like stocks can also be issued as digital tokens on the blockchain, which entails various advantages due to further automation via smart contracts. Clearing and settlement processes can be rendered much more efficient (Fiedler et al. 2018), assets can be traded 24-7, and fraudulent behavior like dividend-stripping (cum-ex) can be prevented (Ante and Fiedler 2019). This approach to tokenization can be applied to a variety of sectors. The fact that blockchain-based tokens can represent any kind of value enables use cases that rely on the transparency and traceability of potentially critical goods, like for example (blood) diamonds (everledger.io). Furthermore, tokenization enables the creation of secondary markets for formerly illiquid goods, such as data, advertising and impressions (brave.com), or fractional ownership of real estate. Additional smart contract applications can then in turn build on these solutions. For example, the decentralized stable coin DAI (makerdao.com) was followed by a decentralized protocol that enables the lending of DAI tokens (compound.finance).

---

[2] The Ethereum blockchain explorer Etherscan enables users to search the blockchain for similar smart contracts. The contract address 0x14a610e5f709923eb4bbfb1eb4798cb7e65c95bb had 540,360 exact matches in March 2020 (https://etherscan.io/find-similar-contracts?a=0x14a610e5f709923eb4bbfb1eb4798cb7e65c95bb&lvl=5).

[3] For a current overview of token contracts on Ethereum, see https://etherscan.io/tokens, which provides a range of statistics such as trading volume, market capitalization, holders or transfers. In March 2020, 248,877 individual token contracts were identified by the tool; the top ten tokens accounted for a combined market capitalization of $11.26 billion.

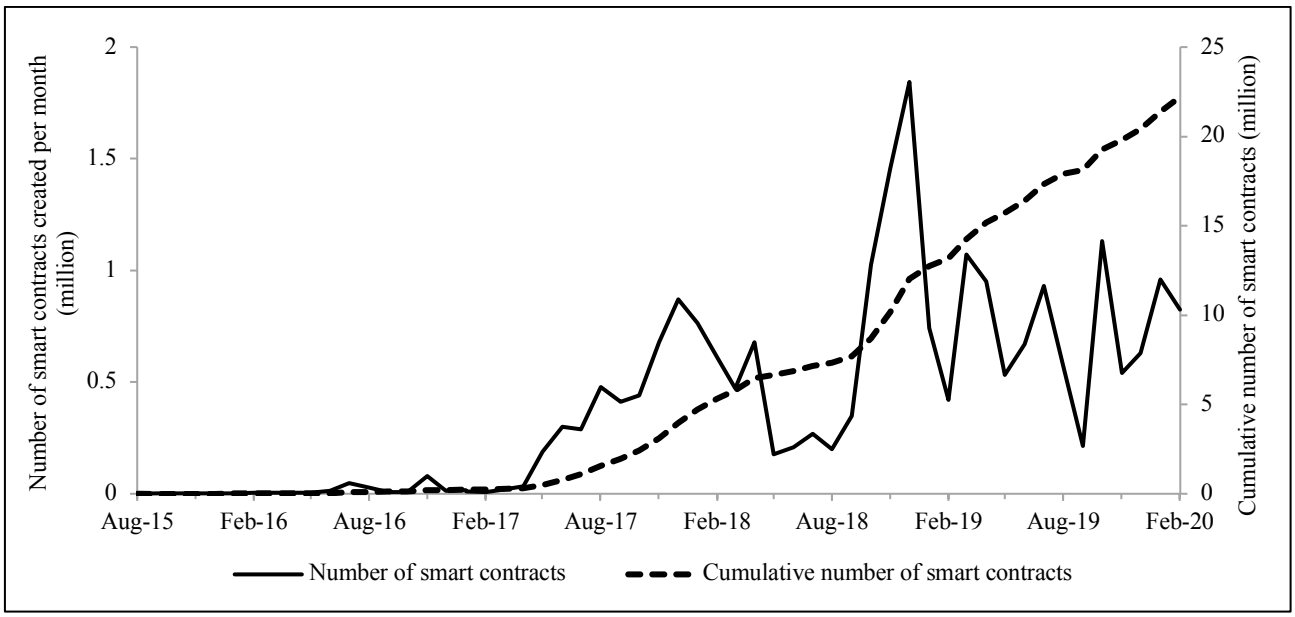

Figure 2. Number of smart contracts created on the Ethereum blockchain.

In sum, smart contracts are an innovative technological application form of programs, whose numerous potential benefits face just as many challenges. These potentials and challenges have been discussed at length in the literature, which will be reflected throughout the rest of this paper.

3.2 The state of smart contract research

3.2.1 Publication trends

Figure 3 shows the distribution of the extracted articles by year of publication. Research on smart contracts has evidently grown exponentially since 2016. 22 additional articles were published in the year 2020 by the month of February.

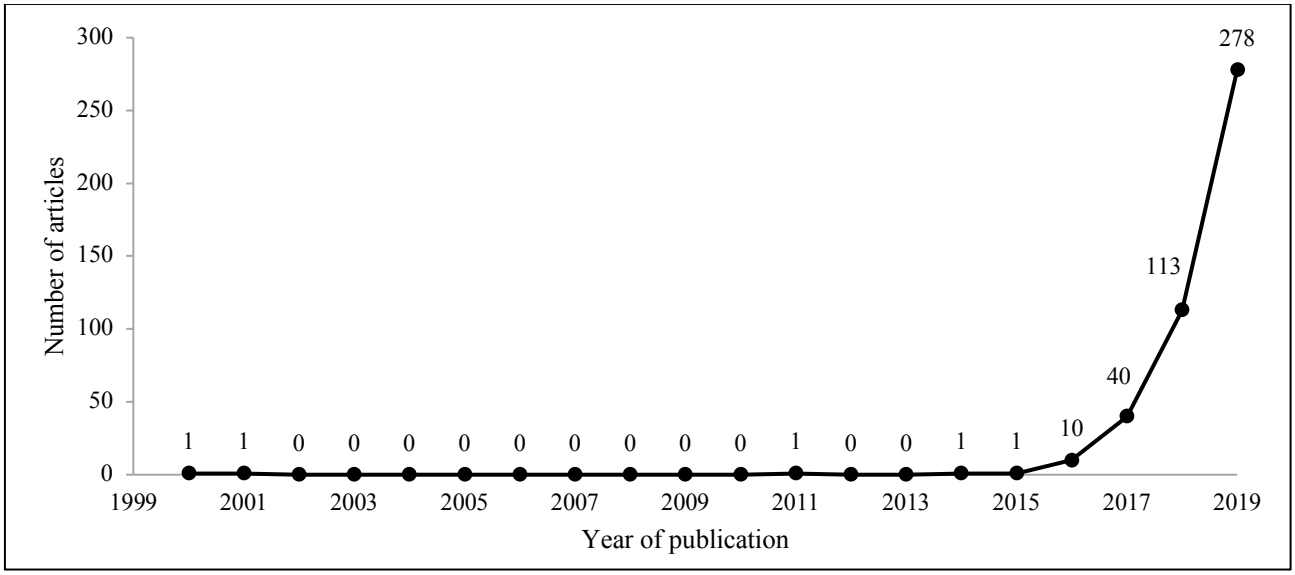

Figure 3. Articles on smart contracts by year of publication.

The 468 extracted articles are distributed across 233 academic outlets. Table 1 shows the 12 journals with the highest number of articles on smart contracts, along with their disciplines as classified in the

Web of Science database. The *IEEE Access* journal has the highest number of articles by far (63; 13.5% of all publications), with *Sensors* coming a distant second. Half of the journals can be assigned to computer science, three to chemistry, energy and engineering-related topics, and two to government & law. A single journal relates to environmental sciences. This distribution is evidence of the interdisciplinary approach to the topic of smart contracts. There is a notable absence of outlets from the economic sciences, which shows that the topic mostly attracts fundamental research by technical and legal scientists.

Table 1. Top journals based on the number of articles on smart contracts.

Number of articles	Journal	Disciplines (Web of Science)
63	IEEE Access	Computer Science; Engineering; Telecommunications
15	Sensors	Chemistry; Engineering; Instruments & Instrumentation
14	Future Generation Computer Systems	Computer Science
10	European Review of Private Law	Government & Law
10	IEEE Internet of Things Journal	Computer Science; Engineering; Telecommunications
8	Computer Law & Security Review	Government & Law
8	International Journal of Advanced Computer Science and Applications	Computer Science
8	Sustainability	Science & Technology - Other Topics; Environmental Sciences & Ecology
7	Computers & Security	Computer Science
6	Applied Sciences	Chemistry; Materials Science; Physics
6	Energies	Energy & Fuels
6	IEEE Transactions on Computational Social Systems	Computer Science

Table 2 shows the twenty most-cited publications. Again we see that the Internet of Things (IoT) represents a major use case – four of the top ten publications directly deal with the topic (Christidis and Devetsikiotis 2016; Novo 2018; Reyna et al. 2018; Y. Zhang and Wen 2017). Other sectors include healthcare (Dagher et al. 2018; Xia et al. 2017; P. Zhang et al. 2018), automotive (Dorri et al. 2017), fintech (Dai and Vasarhelyi 2017; Peters and Panayi 2016), smart grids (Brandstätt et al. 2011; Pop et al. 2018), smart cities (Sun et al. 2016) and supply chain management (Saberi et al. 2019).

Table 2. Most-cited articles on smart contracts.

Article	Citations	Title	Journal
Christidis and Devetsikiotis (2016)	517	Blockchains and Smart Contracts for the Internet of Things	IEEE Access
Xia et al. (2017)	99	MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain	IEEE Access
Novo (2018)	92	Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT	IEEE Internet of Things Journal
Dorri et al. (2017)	83	BlockChain: A Distributed Solution to Automotive Security and Privacy	IEEE Communications Magazine
Reyna et al. (2018)	81	On blockchain and its integration with IoT. Challenges and opportunities	Future Generation Computer Systems
Wang et al. (2018)	81	Blockchain challenges and opportunities: a survey	International Journal of Web and Grid Services
Peters and Panayi (2016)	68	Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money	Banking Beyond Banks and Money (book chapter)
Y. Zhang and Wen (2017)	63	The IoT electric business model: Using blockchain technology for the internet of things	Peer-to-Peer Networking and Applications
Pop et al. (2018)	63	Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids	Sensors
Dinh et al. (2018)	59	Untangling Blockchain: A Data Processing View of Blockchain Systems	IEEE Transactions on Knowledge and Data Engineering
Sun et al. (2016)	54	Blockchain-based sharing services: What blockchain technology can contribute to smart cities	Financial Innovation
Kshetri (2017)	51	Blockchain's roles in strengthening cybersecurity and protecting privacy	Telecommunications Policy
Risius and Spohrer (2017)	45	A Blockchain Research Framework - What We (don't) Know, Where We Go from Here, and How We Will Get There	Business & Information Systems Engineering
Dai and Vasarhelyi (2017)	44	Toward Blockchain-Based Accounting and Assurance	Journal of Information Systems
Saberi et al. (2019)	43	Blockchain technology and its relationships to sustainable supply chain management	International Journal of Production Research
Dagher et al. (2018)	42	Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology	Sustainable Cities and Society
Werbach and Cornell (2017)	36	Contracts Ex Machina	Duke Law Journal
Kim and Laskowski (2018)	36	Toward an ontology-driven blockchain design for supply-chain provenance	Intelligent Systems in Accounting Finance & Management
P. Zhang et al. (2018)	35	FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data	Computational and Structural Biotechnology Journal
Brandstätt et al. (2011)	32	Locational signals to reduce network investments in smart distribution grids: What works and what not?	Utilities Policy

Citation data refers to Web of Science (January 2020).

3.2.2 Keyword analysis

387 (82.7%) of the 468 articles had keywords – 1448 different ones in total. The most frequent keywords are shown in Table 3. 'Blockchain' ranks first, occurring in 74.2% of the articles that mention any keywords. In second and third position are 'smart contract' (38%) and 'smart contracts' (28.7%), respectively. It thus seems that no standard practice has yet emerged in the literature regarding the choice of keywords ('contract' vs. 'contracts'). Similarly, standardization would be in order regarding terms such as 'internet of things' (7.5%), 'iot' (2.8%) and 'internet of things (iot)' (2.6%), all of which describe the same thing.

Table 3. Distribution of keywords mentioned in the articles.

Keywords	Occurrences	%	Keywords	Occurrences	%
blockchain	287	74.2%	fairness	7	1.8%
smart contract	147	38.0%	cryptocurrencies	7	1.5%
smart contracts	111	28.7%	healthcare	6	1.3%
ethereum	46	11.9%	artificial intelligence	6	1.3%
internet of things	29	7.5%	contract law	6	1.3%
bitcoin	23	5.9%	industry 4.0	6	1.3%
cryptocurrency	20	5.2%	ipfs	6	1.3%
security	18	4.7%	supply chain management	6	1.3%
distributed ledger	15	3.9%	traceability	6	1.3%
privacy	12	3.1%	trust	6	1.3%
access control	12	3.1%	information security	6	1.3%
distributed ledger technology	11	2.8%	logistics	5	1.1%
iot	11	2.8%	fintech	5	1.1%
blockchain technology	11	2.8%	law	5	1.1%
internet of things (iot)	10	2.6%	sharing economy	5	1.1%
hyperledger fabric	9	2.3%	smart city	5	1.1%
supply chain	9	2.3%	solidity	5	1.1%
decentralization	8	2.1%	sustainability	5	1.1%
consensus	8	2.1%	game theory	5	1.1%
smart grid	8	2.1%	consortium blockchain	5	1.1%
cloud computing	7	1.8%	privacy-preserving	5	1.1%

The percentages refer to the total number of articles with keywords (n = 387).

The keywords can be divided into three distinct groups: 1) infrastructure and technologies, both in abstract (e.g. blockchain or smart contracts) and concrete (e.g. ethereum or bitcoin) terms, 2) characteristics of the technology (e.g. security or privacy), and 3) specific industries and use cases (e.g. healthcare or IoT). The keywords listed in the table include three specific blockchain infrastructures: Ethereum (11.9%), Bitcoin (5.9%) and Hyperledger Fabric (2.3%). While Ethereum and Hyperledger Fabric are smart contract solutions in and of themselves, second-layer protocols may be used to map smart contract functionalities to Bitcoin.

The most frequently mentioned benefit or property of using blockchain and smart contracts is 'security' (18 occurrences; 4.7%), following by 'privacy' and 'privacy-preserving' (4.2% in total),

'access control' (3.1%), 'decentralization' (2.1%), 'fairness' (1.8%), 'traceability' (1.3%), 'trust' (1.3%), 'information security' (1.3%) and 'sustainability' (1.1%). This enumeration of characteristics provides an apt picture of what smart contracts potentially make possible. The analysis of the keywords also yields conclusions about promising use cases and industries. The keyword 'Internet of Things' (in various forms) is mentioned most frequently (12.9% in total). Other oft-mentioned areas are supply chain (management) and logistics (4.7% in total), (contract) law (2.4%), smart grids (2.1%), cloud computing (1.8%), healthcare (1.3%), artificial intelligence (1.3%), fintech (1.1%), sharing economy (1.1%) and smart city (1.1%).

Figure 4 shows the most frequently used keywords clustered by co-occurrence. Keywords that are often used together form colored clusters, while geographical distance represents the relation between keywords and lines visualize co-occurrences.

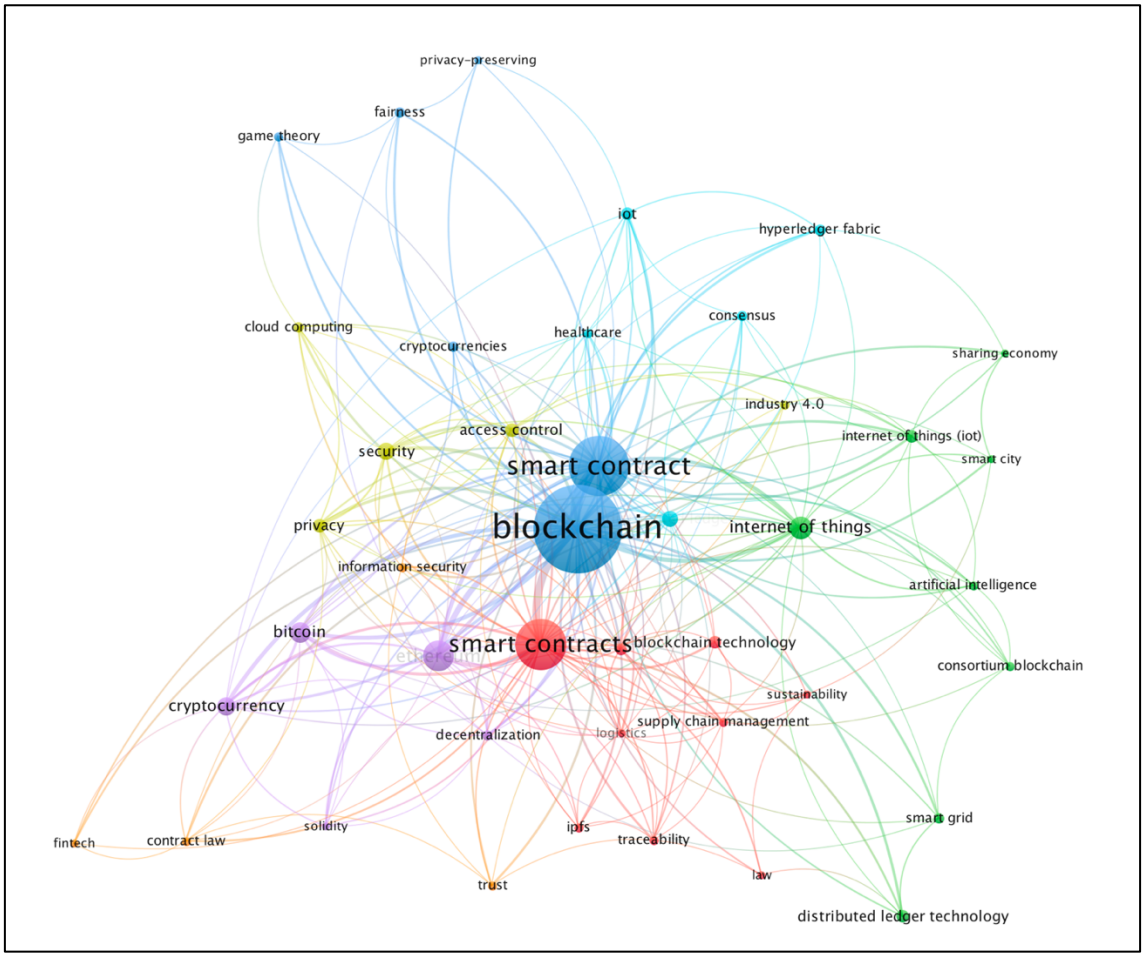

Figure 4. Co-occurrence of author keywords. A minimal number of 5 occurrences across publications (n = 42) is used as cutoff value. Node size is based on the number of occurrences of a keyword. The distance between nodes indicates the relatedness of the keywords, with co-occurrences being represented by lines between the nodes. Created with VOSviewer.

Seven clusters are identified. Almost identical keywords like plural and singular of the word smart contract(s) are divided into other clusters, which shows how young the research environment still is. Nevertheless, clear demarcations can already be seen. For example, there is a cluster surrounding the topics IoT, artificial intelligence and sharing economy (green), while the red cluster includes the topics logistics and supply chain tracking. Understandably, the two clusters are arranged side by side. Other clusters deal with underlying characteristics or methods, such as privacy, security or access

control (yellow) or game theory, fairness or privacy-preserving (blue). The purple cluster includes cryptocurrency-specific keywords.

3.2.3 Geographical and organizational analysis

Figure 5 shows a network visualization of smart contract-related publications by country and the relatedness of countries based on (co-)authorship. The two countries with the largest number of publications, China (134 publications; 29%) and the US (93 publications; 20%), are located close together in the middle of the network and are part of the same cluster. This suggests that scientists from these two countries collaborate, e.g. co-author various publications. The other three clusters are twice European or Western in character, with England (8%) and Germany (5%) representing the nations with the most publications in the respective clusters. The remaining red cluster is rather Asian in character.

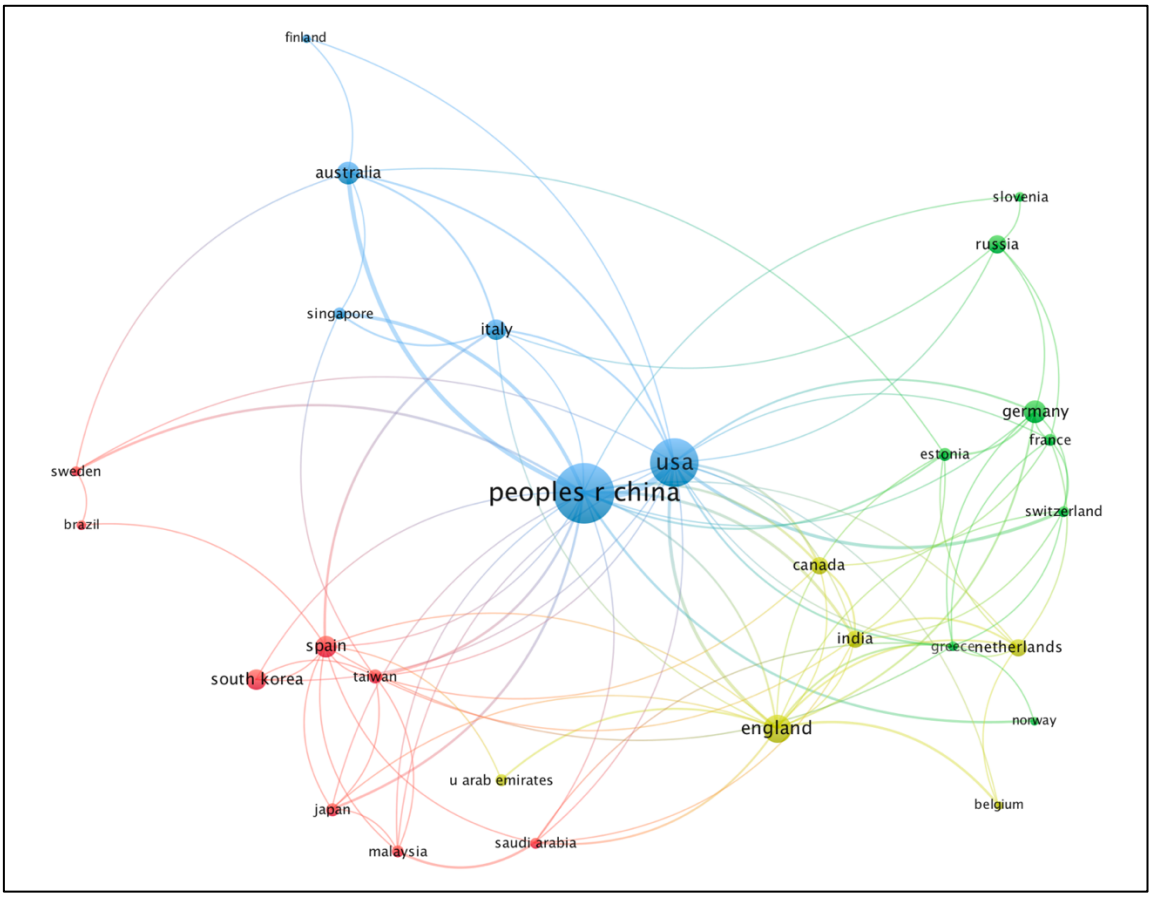

Figure 5. Co-authorship per country. A minimal number of 5 publications per country (n = 28) is used as cutoff value. Node size is based on the number of publications of a country. The distance between nodes indicates the relatedness of the country's publications, with co-authorship being represented by lines between the nodes. Created with VOSviewer.

The 468 publications relate to researchers from 643 distinct organizations. The seventeen organizations with the greatest number of publications on smart contracts (five or more articles) are shown in Table 4. Nine out of the organizations are Chinese (including Hong Kong) and account for 37% of all Chinese articles, while 'only' two organizations belong in the US and account for 14% of the country's smart contract articles. Thus, Chinese smart contract research seems more centralized in comparison. We additionally looked at the connection between organizations, i.e. performed

network analysis, but did not identify relationships worth reporting. This indicates that research on smart contracts is not yet being exchanged, which could be a sign of inefficiency or at least immaturity.

Table 4. Scientific organizations with the greatest number of smart contract publications.

Organization	Number of articles	Jurisdiction
Chinese Academy of Sciences	8	China
Purdue University	7	USA
Beijing University of Posts and Telecommunications	7	China
Commonwealth Scientific and Industrial Research Organisation	7	Australia
Tallinn University of Technology	7	Estonia
University of Ljubljana	7	Slovenia
Xi'an University of Technology	7	China
Chulalongkorn University	6	Thailand
University of Electronic Science and Technology of China	6	China
Sun Yat-sen University	6	China
University of the Chinese Academy of Sciences	5	China
National University of Defense Technology	5	China
University of Tartu	5	Estonia
Temple University	5	USA
City University of Hong Kong	5	Hong Kong / China
Tsinghua University	5	China
University of Cagliari	5	Italy

Sample size: N = 468 publications.

4 Findings on research streams

Table 5 provides an overview of the results of the exploratory factor analysis. We obtain six factors (research streams), which in total cover 213 articles, or 56% of the underlying dataset. The factors jointly explain 48.4% of the variance, i.e. just below half of the research environment on smart contracts. The analysis relies on principal component analysis and Varimax rotation with Kaiser normalization. A KMO measure of 0.519 and a Bartlett test statistic of $p < .001$ confirm that exploratory factor analysis is a suitable method of analysis. These test statistics also apply to each of the Tables 7 through 12.

Table 5. Overview of research streams and factor analysis results.

Research streams (factors)	Share of articles assigned to research stream		Explained variance	Main topics	Important examples
	FL > 0.4	FL > 0.7			
I. Technical foundations, development and open questions of blockchain networks	18.4%	5.8%	25.6%	− Chances and risks regarding Bitcoin and other p2p networks − Introduction of blockchain and/or cryptocurrency protocols − Anonymity of transactions and peers − Network consensus mechanisms, incentives and mining	Nakamoto (2008) Heilman et al. (2015) Ben-Sasson et al. (2014)
II. Blockchain and smart contract applications for the Internet of Things	9.2%	3.1%	6.0%	− Technical application areas of blockchain for IoT (e.g. automation, security, access management and authentication, updates, network architecture) − Practical use cases and applications for blockchain and IoT (e.g. energy markets, charging services, supply chain, edge computing)	Christidis and Devetsikiotis (2016) Hammi et al. (2018) Novo (2018)
III. Smart contract standardization, verification and security	6.8%	3.9%	5.5%	− Ethereum as smart contract infrastructure − Smart contract (code) and virtual machine design, improvements and security analysis − Semantics and formal verification of smart contracts − Smart contract characteristics (e.g. updates, deletion)	Luu, Chu, et al. (2016) Hildenbrandt et al. (2018) Bhargavan et al. (2016)
IV. Blockchain and smart contracts for the disruption of existing processes and industries	7.1%	3.7%	4.8%	− Potential impact of blockchain and smart contracts on industry and society − Social change, open collaboration, exchange networks − Transformation of energy markets, healthcare, finance, governments and the law	Goertzel et al. (2017) Ølnes et al. (2017) Shermin (2017)
V. Potentials and challenges of smart contracts	7.6%	1.3%	3.3%	− Integration of smart contracts as / into business processes − Technical potentials and challenges of scripting languages / smart contracts − Technological solutions to verify or enhance scripting languages and thus smart contracts	Seijas et al. (2017) Weber et al. (2016)
VI. Smart contracts and the law	6.6%	3.7%	3.2%	− Examination of smart contracts from a legal perspective − Mapping and digitization of law via computer code − Contract law, contractual relations and relational thought	Werbach and Cornell (2017) Raskin (2017) Levy (2017)

FL = factor loading; FS = factor score; factor analysis: principal component analysis and Varimax rotation with Kaiser normalization; KMO measure: 0.519; Bartlett test: p<.001.

The research streams are ordered and discussed in the following according to their ranking in terms of variance explained. The first one comprises 18.4% of the examined publications and explains 25.66% of the total variance in the sample. It deals with the technical foundations, development and open questions of blockchain networks. This also includes basic aspects of the technology such as consensus mechanisms, i.e. scientific findings that were published many years before the Bitcoin white paper. Further topics in the stream are the anonymity of transactions in digital systems and the introduction of new blockchain and cryptocurrency protocols. The second stream explains 6% of the variance, covers 9.2% of the publications and deals with blockchain and smart contract applications for IoT. It covers specific technical applications such as automation, security, access rights and network structures. In addition, specific use cases are explained, including energy markets, charging services, supply chain or edge computing. Stream III deals with smart contract standardization, verification and security, explains 5.5% of the variance and covers 6.8% of all publications. There is a clear focus on the blockchain infrastructure Ethereum and the scripting languages and virtual machine used for smart contracts. Further topics are the semantics and formal verification of smart contracts, as well as special characteristics such as the deletion of decentralized code or the possibility to update smart contracts. The fourth stream deals with the societal potential of blockchain technology and smart contracts. 7.1% of the papers are assigned to the stream, which explains 4.8% of variance. The publications in the stream analyze the potential impact of blockchain and smart contracts on society and the economy, social change and open collaboration – and how it could be fostered via the use of blockchain and smart contracts and the transformation of industries. Stream V deals with the potential and challenges of smart contracts. It covers 7.6% of the publications and has the smallest share of publications with a factor loading above 0.7 (1.3% across all publications; 17.2% across this stream). Its articles jointly account for 3.3% of the variance and deal with the integration of smart contracts into business processes, the technical potential and challenges of smart contracts, and solutions to enhance the scripting languages that are used for smart contract applications. The sixth stream explains 3.2% of the variance and accounts for 6.6% of the papers. It covers the examination of smart contracts (and blockchain technology) from a legal perspective, the mapping and digitization of law and legalese, as well as basic studies on contractual relations between parties.

Figure 6 shows the temporal development of the research streams. Note that the time axis represents different intervals. The first period begins in 1963, when the earliest paper in the sample (Macaulay 1963) was published. The next period begins with Szabo's (1994) first conceptual description of smart contracts and ends in 2012, the year before the first trend-setting publication on Turing-complete smart contracts – the Ethereum whitepaper (Buterin 2013). From then on, we consider individual years.

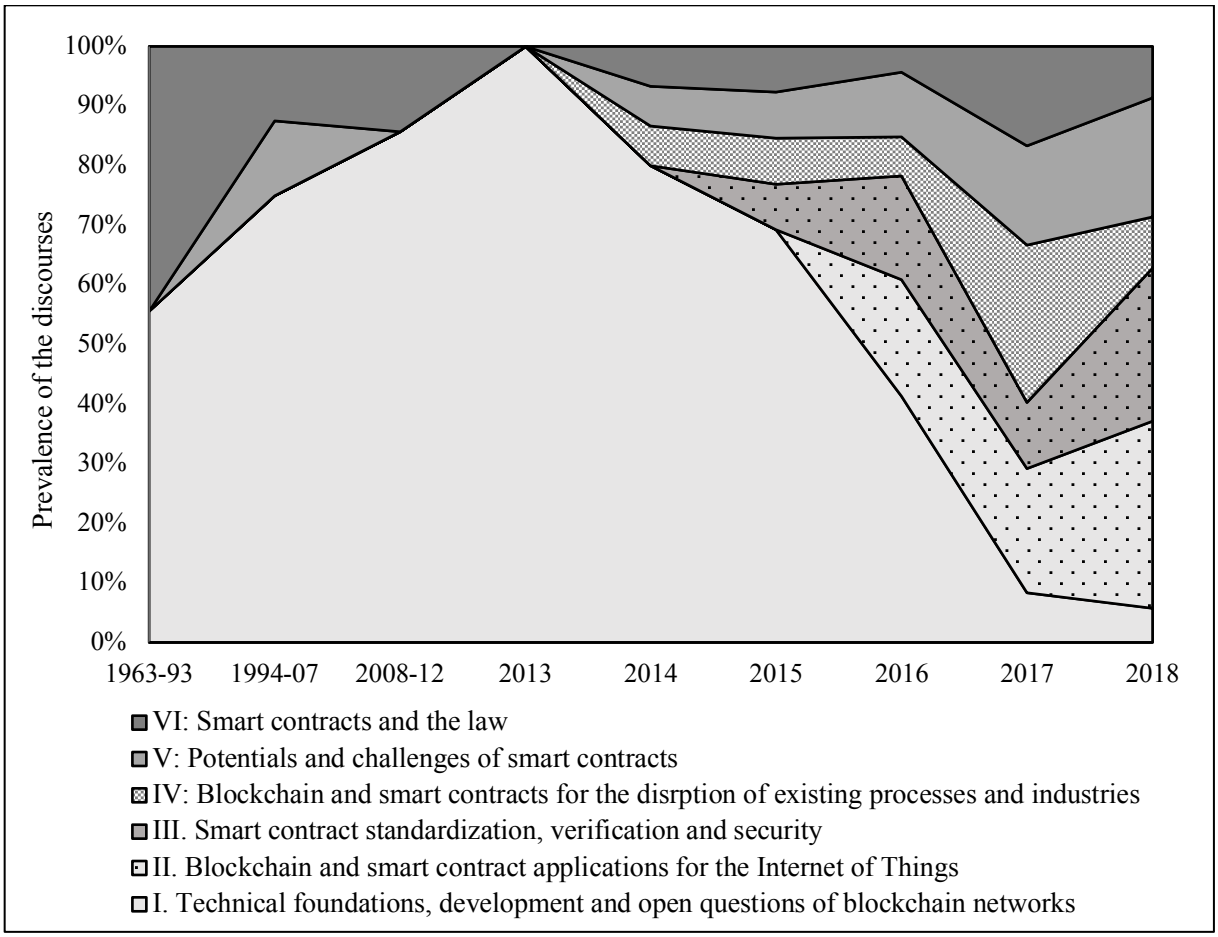

Figure 6. Temporal development of the research streams.

Research stream I, which deals with the fundamental properties of networks such as Bitcoin and Ethereum, evidently takes up a considerable proportion of the research environment until 2015 (>50% in each period). Until 2013, we find only publications belonging to research streams I, V and VI. From then onwards, the relevance of stream I steadily declines, while the other three streams emerge and continue to grow over time.

We also find patterns regarding the practical use or relevance of blockchain and smart contracts. Table 6 shows the share of publications in each stream that refer to specific smart contract platforms, solutions or mechanisms. Bitcoin is also listed for comparison, although it constitutes such a platform not in and of itself but only when supplemented with protocols or sidechains like Rootstock or Open Assets Protocol.

Being mentioned in 52% of the publications, Ethereum is the most frequently cited smart contract platform by far. This accords with our earlier findings on keywords (cf. Table 2) Two of Ethereum's clones, forks or adaptions are also frequently named: Hydrachain (2%) and Eris (1%). Trailing Ethereum are Hyperledger (16%) and the smart contract solution Codius by Ripple (6%), whose development ceased in 2015. The Corda project initiated by the private consortium R3CEV is in fourth place (5%). Also listed are several on-top solutions for Bitcoin: Counterparty (3%), Rootstock (2%) and Mastercoin/Omni Layer (2%). Three quarters of all

publications mention Bitcoin; only in stream III is Ethereum (96 %) mentioned more frequently than Bitcoin (77 %).

Table 6. Occurrence of smart contract infrastructure and solutions across the research streams.

Platform	All	Research stream					
		I.	II.	III.	IV.	V.	VI.
Ethereum[a]	52%	27%	46%	96%	52%	77%	52%
Hyperledger[b]	16%	6%	31%	12%	19%	33%	8%
Ripple/Codius[c]	6%	1%	3%	15%	4%	17%	0%
Corda	5%	1%	3%	4%	7%	10%	8%
Counterparty	3%	1%	0%	15%	4%	3%	0%
Hydrachain	2%	0%	3%	0%	7%	7%	0%
Rootstock (RSK)	2%	0%	3%	8%	0%	3%	0%
Stellar	2%	0%	3%	8%	0%	3%	0%
Hawk	2%	0%	3%	8%	0%	3%	0%
Nxt	2%	0%	3%	4%	0%	7%	0%
Mastercoin (Omni Layer)	2%	1%	3%	0%	4%	3%	0%
Multichain	2%	1%	0%	0%	4%	7%	0%
EOS	1%	0%	3%	4%	0%	3%	0%
Everledger	1%	0%	3%	4%	4%	0%	0%
Tendermint	1%	1%	3%	0%	0%	3%	0%
Openchain	1%	0%	3%	0%	4%	3%	0%
Tezos	1%	0%	0%	4%	0%	7%	0%
Eris	1%	0%	3%	4%	0%	0%	0%
Chain.com	1%	0%	0%	0%	0%	7%	0%
Digital Asset Modeling Language (DAML)	1%	1%	0%	4%	0%	0%	0%
Bitcoin	75%	66%	83%	77%	89%	80%	64%
Observations	213	70	35	26	27	30	25

21 other smart contracts solutions with only one occurence across all research streams are omitted for brevity: Achain, Aeternity, Algorand, Ardor, AxCore, BitHalo, Dogeparty, Lisk, Monax, NEO (Antshares), Open Assets Protocol, OriginChain, Polkadot, Qtum, Quorum, SmartContract, Stellar, Stratis, Symbiont, TRON, Waves.

a: includes both Ethereum and Ethereum Classic

b: includes various Hyperledger implementations (Fabric, Sawtooth, Burrow, Iroha, Indy)

c: Codius' smart contract development was halted in 2015.

A total of 28 different smart contract solutions were found in the 30 publications of stream V, while only three were found in stream VI. This considerable difference is due to stream VI containing disproportionally more old publications that have no connection to smart contracts or blockchain technology, while stream V has a clear focus on these technologies.

The following subsections provide detailed information on each of the six research streams before their interrelations are analyzed using social network analysis.

4.1 Technical foundations, development and open questions of blockchain networks

Table 7 shows the ten publications with the highest factor loadings and four others with very high factor scores from research stream I. The research area explains 25.6% of the variance and accounts for 18.4% (70) of the publications in the sample. 22 of them (i.e. 5.8% of all publications or 31% of those in the stream) have factor loadings above 0.7. The publications concern the opportunities and risks associated with blockchain networks, the presentation of new or improved cryptocurrency or blockchain protocols, questions regarding the potential or actual anonymity of transactions and peers, as well as technical questions regarding consensus mechanisms or mining. Other publications additionally concern the practical and theoretical foundations of p2p and blockchain networks. Generally, there is a strong thematic reference to Bitcoin and how it could be improved.

Table 7. Articles on the development and open questions of blockchain and p2p networks.

Publication	Factor loading	Factor score
Sompolinsky and Zohar (2013)	0.864	2.557
Heilman et al. (2015)	0.863	3.755
Ben-Sasson et al. (2014)	0.854	3.616
Miers et al. (2013)	0.850	3.268
Biryukov et al. (2014)	0.840	2.539
Buterin (2013)	0.827	1.474
Eyal et al. (2015)	0.820	3.515
Bentov et al. (2014)	0.810	2.752
Pease et al. (1980)	0.810	1.641
Nayak et al. (2016)	0.809	2.891
...	...	...
Nakamoto (2008)	0.473	6.123
Zyskind et al. (2015)	0.671	4.908
Tschorsch and Scheuermann (2016)	0.653	4.389
Kosba et al. (2016)	0.613	3.759
12 other publications with factor loading > 0.7		

Explained variance: 25.6%; number of articles with factor loading > 0.4: 70 (18.4%); number of articles with factor loading > 0.7: 22 (5.8%).

With a factor score of 6.12, the Bitcoin whitepaper (Nakamoto 2008) has the greatest influence on the research stream. The study with the highest factor loading, i.e. the one that fits best with the research area, deals with the question to what extent Bitcoin can achieve greater scalability (Sompolinsky and Zohar 2013). The authors present a modification of the blockchain as data structure, which improves the level of security and reduces the confirmation time of transactions. The scalability of Bitcoin, or blockchain networks more generally, is also the central topic of various other publications in the research stream. For example, Eyal et al. (2015) describe a new cryptocurrency protocol, Bitcoin-NG (Next Generation), which uses Byzantine fault tolerance as a consensus mechanism for greater scalability. Luu, Narayanan, et al. (2016) describe a blockchain protocol, ELASTICO, which increases transaction rates almost in

proportion to the miners' computing power. This is done via sharding, the secure division of a network into smaller, more efficient parts, each with a discounted set of transactions (shards).

The most relevant publications contain a variety of other approaches for new cryptocurrencies or modifications of Bitcoin. This includes protocols that focus on the anonymity of users and transactions (Ben-Sasson et al. 2014; Miers et al. 2013), the energy market (Mihaylov et al. 2014) or specific consensus mechanisms, such as proof-of-stake (King and Nadal 2012) or proof-of-activity (Bentov et al. 2014). The stream also includes the Ethereum whitepaper (Buterin 2013), which describes the 'most successful' public blockchain to date with a focus on Turing-complete smart contracts.

Network consensus, the procedure by which transactions are secured and processed, is a highly relevant topic of the stream. Lamport et al. (1982) and Pease et al. (1980) scientifically substantiate Byzantine fault tolerance, which creates trust in networks whose participants may otherwise be weary of each other. The literature subsequently moved on to blockchain-specific publications on network consensus. This includes the introduction of HoneyBadgerBFT, an asynchronous Byzantine fault tolerance protocol that ensures network operations without any assumptions regarding timing (Miller et al. 2016). The authors show that the protocol runs independently of the underlying network, as illustrated by a test using the Tor network. Closely related to a network's consensus mechanism is its security. We find a much-cited publication on potential threats to p2p networks from the pre-blockchain era: Douceur (2002) describes sybil attacks, where one entity presents itself as several identities to capture a p2p system. Other related literature focuses on blockchain, showing for example how eclipse attacks can be used to exclude other nodes in the network, which creates risks like selfish mining, double spending or adversarial forks (Heilman et al. 2015). However, Nayak et al. (2016) show that these same attacks can sometimes even entail economic advantages for the entity under attack.

As mentioned above, anonymity is a highly relevant topic for the research stream. This is also evident from the fact that a study on decentralized privacy and the use of blockchain for the protection of personal data (Zyskind et al. 2015) has the second highest factor score within the stream, and a study on privacy-preserving smart contracts (Kosba et al. 2016) ranks fourth. Biryukov et al. (2014) present a method of deanonymizing users of the Bitcoin network. Their process has a success rate of between 11% and 60%, and the authors point out various countermeasures. Reid and Harrigan (2013) analyze the degree of anonymity of the Bitcoin network by linking transactions with Bitcoin addresses and conclude that it is possible for public keys to be associated with users, whose activity can then be observed.

In summary, the first and most important research stream in terms of the variance explained by factor analysis is dedicated to technical fundamentals. In this respect, the high factor score of Tschorsch and Scheuermann (2016), a publication on the technical principles of decentralized digital currencies, stands to reason. While some of the topics discussed in the papers may no longer be of the highest relevance for practice, they still provide the scientific basis for research on smart contracts.

4.2 Blockchain applications for the Internet of Things

The second research stream comprises 35 publications (9.2% of the sample) and explains 6.03% of the variance. Table 8 shows the ten publications with the highest factor loadings and four

others with high factor scores. 12 publications (34%) have factor loadings above 0.7. The papers mainly deal with blockchain and smart contracts as applied to IoT. Many of them examine the suitability of blockchain technology to ensure certain critical characteristics, including authentication, distribution, commissioning of devices and/or data, and the guarantee of technical security and anonymity.

Table 8. Articles on blockchain and smart contract applications for the Internet of Things.

Publication	Factor loading	Factor score
Hammi et al. (2018)	0.852	2.342
Herbaut and Negru (2017)	0.799	2.589
Hardjono and Smith (2016)	0.782	2.323
Turkanović et al. (2018)	0.782	2.498
Sharma et al. (2017)	0.773	2.680
Stanciu (2017)	0.753	2.464
Banerjee et al. (2018)	0.749	2.609
Knirsch et al. (2018)	0.720	2.373
Subramanian (2018)	0.708	2.559
Egelund-Müller et al. (2017)	0.707	2.459
Casado-Vara et al. (2018)	0.705	2.376
...	...	...
Christidis and Devetsikiotis (2016)	0.485	4.492
Khan and Salah (2018)	0.496	3.502
Novo (2018)	0.665	3.228
Boudguiga et al. (2017)	0.698	3.001
2 other publications with factor loading > 0.7		

Explained variance: 6.03%; number of articles with factor loading > 0.4: 35 (9.2%); number of articles with factor loading > 0.7: 12 (3.1%).

The article with the highest factor score (4.492) is Christidis and Devetsikiotis (2016), a publication entitled 'Blockchain and Smart Contracts for the Internet of Things'. The authors examine whether blockchains are a suitable technology for IoT. They show how the interaction of the technology and its application can promote the sharing of services and data, which may create new markets, and how smart contracts can help to automate time-consuming processes. The authors conclude that the interaction of blockchain and IoT can significantly affect a range of sectors and give rise to new business models. The three other publications with high factor scores also deal with the implications of blockchain technology, and thus also smart contracts, and IoT. More specifically, they examine what solutions in the areas of security (Khan and Salah 2018), scalable access management (Novo 2018) and the availability and accountability of updates (Boudguiga et al. 2017) could look like. Most of the publications with high factor loadings also investigate how blockchain can add value for various characteristics of IoT. These include technical areas, like authentication and commissioning (Hammi et al. 2018; Hardjono and Smith 2016; Ouaddah et al. 2017), network architecture (Sharma et al. 2017) and (data) security (Banerjee et al. 2018; Dorri et al. 2017; Esposito et al. 2018), but also more use-case centered aspects like edge computing (Stanciu 2017), supply chain (Casado-Vara et al. 2018),

the sharing economy (Herbaut and Negru 2017) or energy-related markets, applications and charging services (Knirsch et al. 2018; Mengelkamp et al. 2018; Munsing et al. 2017; Sikorski et al. 2017).

As with research stream I, blockchain as a basis for privacy-preserving mechanisms is a common topic in the stream. Hardjono and Smith (2016) propose the use of a blockchain system architecture called ChainAnchor that permits privacy-preserving commissioning of IoT devices, while Knirsch et al. (2018) describe privacy-preserving vehicle charging leveraged by blockchain. Other studies focus on privacy issues regarding cloud-based data (Esposito et al. 2018) and access control (Ouaddah et al. 2017).

4.3 Smart contract standardization, verification and security

Research stream III explains 5.53% of the variance and consists of 26 (6.8%) publications, of which 15 have a factor loading above 0.7. The overall topic of the stream can be summarized as smart contract standardization, verification and security. The publications focus on smart contracts on the Ethereum blockchain. Almost all publications (96%) mention Ethereum, while the second most frequently mentioned platform, Counterparty, appears in only 15% of the publications. Ethereum is also referenced significantly more often than Bitcoin (77%). The ten publications with the highest factor loadings and two further publications with high factor scores are shown in Table 9.

Table 9. Articles on smart contract standardization, verification and security.

Publication	Factor loading	Factor score
Hildenbrandt et al. (2018)	0.919	4.484
Grishchenko et al. (2018)	0.881	3.836
Bartoletti and Pompianu (2017)	0.869	3.279
Destefanis et al. (2018)	0.860	4.620
Hirai (2017)	0.857	2.705
Clack et al. (2016)	0.835	3.118
Marino and Juels (2016)	0.819	2.354
Bigi et al. (2015)	0.791	2.799
Bhargavan et al. (2016)	0.778	5.356
Wohrer and Zdun (2018)	0.759	3.758
...	...	...
Luu, Chu, et al. (2016)	0.569	7.786
Atzei et al. (2017)	0.507	4.391
5 other publications with factor loading > 0.7		

Explained variance: 5.53%; number of articles with factor loading > 0.4: 26 (6.8%); number of articles with factor loading > 0.7: 15 (3.9%).

Luu, Chu, et al. (2016) is the study with the highest factor score (7.786), and its title provides a fitting summary of the scope of research stream III: ‘Making Smart Contracts Smarter’. The authors analyze the security of Ethereum smart contracts against a hypothetical manipulating and profit-driven adversary. They identify various bugs that are due to the semantics of the

Ethereum network. In response, the authors suggest how the operational semantics of the network could be improved. In addition, they present a tool called Oyente, by which they analyze 19,366 smart contracts, of which 8,833 prove to be vulnerable.

Semantics and formal analysis play a major role in the discourse. Clack et al. (2016) explore a semantic smart contract framework and show what legally enforceable smart contracts could look like, while Bartoletti and Pompianu (2017) assess programming patterns of Ethereum smart contracts. Bigi et al. (2015) analyze validation aspects of smart contracts using game-theoretic and formal methods, while Marino and Juels (2016) develop standards based on contract law to let the parties alter or undo smart contracts. Hirai (2017) formally defines the Ethereum Virtual Machine (EVM) in higher order logic (HOL) using the proof assistant Isabelle. This definition is extended by Amani et al. (2018) by using a program logic to reason about structured bytecode sequences. Hildenbrandt et al. (2018) present KEVM, a formal specification of EVM bytecode that provides a foundation for formal analyses. Bhargavan et al. (2016) translate Ethereum smart contracts to the proof assistant F* for the purpose of verification. Grishchenko et al. (2018) present a semantic framework for smart contract analysis by formalizing EVM bytecode via F*. The authors define several central security properties for smart contracts: 1) call integrity, 2) atomicity, 3) independence of the mutable account state and 4) independence of the transaction environment (i.e. miners).

A thematically related but much more practical topic is the development of tools to verify smart contracts. Besides the Oyente tool used by Luu, Chu, et al. (2016), Securify is presented by Tsankov et al. (2018). The fully automated tool analyzes smart contracts in a two-step process, examining first the dependency graph of a contract and then compliance and violation patterns. Another tool, the static analyzer SmartCheck, converts solidity code before checking it for XPath patterns. The tool is limited in its scope but allows the swift identification (and subsequent correction) of simple bugs (Tikhomirov et al. 2018).

The topic of attacks, bugs and errors that pose a risk to smart contracts is an overarching theme of the stream. Wohrer and Zdun (2018) point to and describe common security patterns for Solidity that can mitigate attack risks. Atzei et al. (2017) and Luu, Chu, et al. (2016) provide overviews of vulnerabilities and potential attacks on three different levels (blockchain, EVM, and Solidity). Grishchenko et al. (2018) provide an overview of the general security-related bugs: Reentrancy, call to the unknown, mishandled exceptions, transaction order dependency, unpredictable state, timestamp dependency, time constraints and generating randomness. In addition to the comprehensive analysis of potential weaknesses, a detailed analysis of individual relevant events is also carried out. Destefanis et al. (2018) analyze the Parity ‘hack’ as a case study, an event where $150 million in cryptocurrency was frozen in a smart contract.

4.4 Blockchain and smart contracts for the disruption of existing processes and industries

Research stream IV deals with societal and economic potentials of blockchain and smart contracts. It explains 4.79% of variance. 27 (7.1%) publications can be assigned to the stream, of which 14 have factor loadings in excess of 0.7. The publications in the stream deal with the disruptive potential of blockchain technology and automation via smart contracts. The publications show how the technology could change entire sectors (e.g. energy markets;

healthcare) or mechanisms (e.g. governance; collaboration). Table 10 shows the ten publications with the highest factor loadings of the stream. Additionally, three publications with high factor scores are shown.

Table 10. Articles on blockchain and smart contracts for the disruption of existing processes and industry sectors.

Publication	Factor loading	Factor score
Tai et al. (2016)	0.922	3.485
Goertzel et al. (2017)	0.904	3.713
Peck (2017)	0.892	3.624
Peck and Wagman (2017)	0.873	3.500
Shermin (2017)	0.871	3.723
Benchoufi et al. (2017)	0.868	3.757
Roehrs et al. (2017)	0.824	3.805
Larios-Hernández (2017)	0.791	3.350
Khaqqi et al. (2018)	0.773	3.495
Cuccuru (2017)	0.731	3.715
...	...	...
Ølnes et al. (2017)	0.624	4.133
Magazzeni et al. (2017)	0.651	3.909
Nakamoto (2008)	0.326	3.862
4 other publications with factor loading > 0.7		

Explained variance: 4.79%; number of articles with factor loading > 0.4: 27 (7.1%); number of articles with factor loading > 0.7: 14 (3.7%).

Goertzel et al. (2017) is characteristic of stream IV, describing how a 'more utopian existence' could be achieved. For this purpose, a multitude of possibilities are enumerated. These include centrally planned and managed socialism, mutualist economics and sharing of land, open production networks, transparent currencies and open collaboration, or offer networks for the exchange of goods and services. It is explained how blockchain can assist with the implementation of such systemic changes. Peck (2017) shows the potential that the technology many have for various industries and draws a comparison to existing data management systems. Further publications describe in detail how the technology can be used beyond the application to Bitcoin or cryptocurrency (Cuccuru 2017; Magazzeni et al. 2017).

Tai et al. (2016) is one of three publications in the stream that specifically deal with energy markets. The authors describe how direct energy trading between prosumers leads to new business models but also coordination problems. The management of such a system could be ensured by a blockchain, which reduces the central provider's problems, including high costs, low information security and privacy. Peck and Wagman (2017) describe the uncertainty as to how individuals would behave in open energy markets – would they be willing to pay slightly more for green energy from a neighbor? The authors expect this uncertainty to decline, as various projects are working on blockchain-based solutions to such market designs. The last energy-specific publication proposes a reputation-based emission trading scheme that uses blockchain technology to address management and fraud issues (Khaqqi et al. 2018).

For the healthcare sector, the literature predicts that blockchain and smart contracts will enable significant improvements in efficiency. The potential benefits include the transparency and traceability of approvals for clinical trials (Benchoufi et al. 2017), the management of personal health data (Roehrs et al. 2017), and authentication and data management in healthcare systems (Yue et al. 2016; J. Zhang et al. 2016). Other sectors and industries that these technologies may transform include governance (Shermin 2017), financial inclusion (Larios-Hernández 2017), accounting and assurance (Dai and Vasarhelyi 2017), e-residency (Sullivan and Burger 2017), and government applications (Ølnes et al. 2017).

4.5 Potentials and challenges of smart contracts

Research stream V deals with the potentials and challenges of smart contracts. The publications directly concern smart contract applications – rather than merely in passing or in a figurative sense, as in other discourses. The stream accounts for 3.29% of the variance in the sample. 29 publications can be assigned to the stream, of which only 5 have factor loadings in excess of 0.7. Table 11 shows those five publications and six additional articles with high factor scores. Only few studies can be assigned very precisely to this discourse. The highest individual factor loading of 0.783 shows that the stream is still relatively immature.

Table 11. Articles on the potentials and challenges of smart contracts.

Publication	Factor loading	Factor score
Seijas et al. (2017)	0.783	2.872
Shae and Tsai (2017)	0.752	2.463
Grossman et al. (2017)	0.736	2.715
T. Chen et al. (2017)	0.727	2.759
Al-Bassam (2017)	0.715	2.526
...	...	...
Weber et al. (2016)	0.443	3.056
Castro and Liskov (2002)	0.576	3.015
Lemieux (2016)	0.683	2.841
Nikolić et al. (2018)	0.688	2.782
S. Chen et al. (2017)	0.664	2.767

Explained variance: 3.29%; number of articles with factor loading > 0.4: 30 (7.9%); number of articles with factor loading > 0.7: 5 (1.3%).

The study with the highest factor score, Weber et al. (2016), deals with trust in collaborative processes and introduces a technique to integrate smart contract solutions for business processes. The authors demonstrate the feasibility of their solution by implementing three use cases on the Ethereum blockchain. Various studies in the stream deal with technical potentials and shortcomings of smart contracts. Seijas et al. (2017) provide an overview of the scripting languages used in blockchain networks, focusing on Bitcoin, Ethereum and Nxt. They emphasize the need to understand unanticipated events and consider a series of potential security problems of smart contracts: reentrancy, implicit runtime exceptions, incomplete handling of preconditions (no reimbursement), unilateral abortion, unpredictable state, secrecy, immutable bugs, lost currency, non-randomness and the question whether a scripting language

should be Turing complete. Additionally, the authors describe technological solutions that could be used to verify or enhance scripting languages and thus smart contracts: verifiable computation, verifiable bounds and reusable libraries, multiparty computation, zero knowledge proofs, proof-carrying code, use of combinators, use of polymorphic dependent types, formal verification, static analysis and merkelized abstract syntax trees. The in-depth technical analysis may explain the high factor score of Castro and Liskov (2002), an article on the performance of Practical Byzantine Fault Tolerance. Referring to the famous hack (or bug) of The DAO, Grossman et al. (2017) deal with callbacks in smart contracts. They define a mechanism of correctness for callbacks called Effective Callback Freedom and show how it can be used to prevent bugs in the Ethereum environment. Other analyses concern transaction cost optimization of Ethereum smart contracts (T. Chen et al. 2017), vulnerabilities and exploits (Nikolić et al. 2018), and a smart contract-based public key infrastructure system, which enables a web-of-trust approach, where one entity can verify another's identity (Al-Bassam 2017).

Shae and Tsai (2017) is the only study of the discourse with a factor loading above 0.7 that explicitly deals with an industry-specific use case. The paper presents a blockchain architecture for clinical studies and precision medicine. Various technological design aspects are discussed in terms of prerequisites and open questions. The authors list components of a system architecture which are prerequisites for the use of the blockchain platform. Other studies with lower factor loadings focus on the preservation of digital records (Lemieux 2016), supply chain management (S. Chen et al. 2017), pharma supply chains (Bocek et al. 2017) or healthcare use cases in general (Hölbl et al. 2018). Many of the industry-specific publications concern the area of health and medicine, or at least related processes (e.g. supply chain and digital records).

4.6 Smart contracts and the law

The sixth research stream explains 3.16% of the variance and comprises 25 (6.6%) publications, 14 of which have a factor loading in excess of 0.7. The most relevant publications based on our factor analysis results are shown in Table 12. The discourse covers legal aspects of smart contracts. This includes in particular the question to what extent smart contracts can represent, replace or supplement classical contracts and to what extent legal institutions should cooperate or engage with developers and users of the blockchain and smart contract technologies (e.g. Werbach 2016). The stream also comprises a large body of basic literature, including for example articles on classical contract law and associated economic issues (Macaulay 1963; Macneil 1978, 1985), on the regulation of the internet (Lessig 1999) and on the digitization of the law or the digital representation of contracts (Surden 2012).

The article by Werbach and Cornell (2017) has the highest factor score of a publication in any of the six streams (8.826). It explains how startups are developing smart contract applications that may replace traditional contract law. The authors discuss the question whether smart contracts can be applied in conformity with the law and conclude that new commercial opportunities arise from this but will not replace traditional contract law. Several other studies also address the question of the compatibility or the potential displacement of classic contracts by smart contracts. Raskin (2017) highlights the potential of the technology and recommends that legislators and courts be open to this new and innovative form of contracting (Raskin 2017). Other studies indicate, on the basis of a number of limitations and risks related to smart

contracts, that popular claims about the automation and disintermediation of contract law, lawyers and courts are unrealistic (Mik 2017), while yet others find that smart contracts solely focus on technical aspects of contracts but lack social context, as real word contracts are also enforced through social mechanisms (Levy 2017). Sklaroff (2017) compares smart contracts to an electronic data interchange (EDI), a technology proposed in the 1970s that gained a lot of momentum, and points out that smart contracts lack flexibility, which is a necessary feature of efficient contracts. Fairfield (2014) discusses how smart contracts may help to improve consumer protection, e.g. in online contracting. Right now, companies dictate terms online, which consumers can then only accept or decline. Smart contracts could introduce the possibility to bargain about the terms.

Table 12. Articles on smart contracts and the law.

Publication	Factor loading	Factor score
Fairfield (2014)	0.871	2.979
Raskin (2017)	0.866	5.340
Mik (2017)	0.860	4.079
Levy (2017)	0.844	5.647
Macneil (1985)	0.801	2.646
Werbach (2016)	0.799	1.982
Sklaroff (2017)	0.785	3.529
Scholz (2016)	0.781	2.235
Werbach and Cornell (2017)	0.764	8.826
Macaulay (1963)	0.763	3.937
...	...	...
Surden (2012)	0.743	5.968
Savelyev (2017)	0.569	3.451
Szabo (1997)	0.443	3.111
3 other publications with factor loading > 0.7		

Explained variance: 3.16%; number of articles with factor loading > 0.4: 25 (6.6%); number of articles with factor loading > 0.7: 14 (3.7%).

4.7 Social network analysis

Figure 7 illustrates the relationships among the publications in the form of a social network. Stream I clearly makes up a considerable part of the scientific discourse, as also evidenced by the large proportion of explained variance in the factor analysis. The spatial separation of the discourses is not very distinct. The largest publications based on node size belonging to stream II are placed next to those of streams I and IV, which reflects their thematic proximity. This illustrates that the research environment is still very young, and the scientific directions, ideas and theories have not yet strongly distinguished themselves from each other.

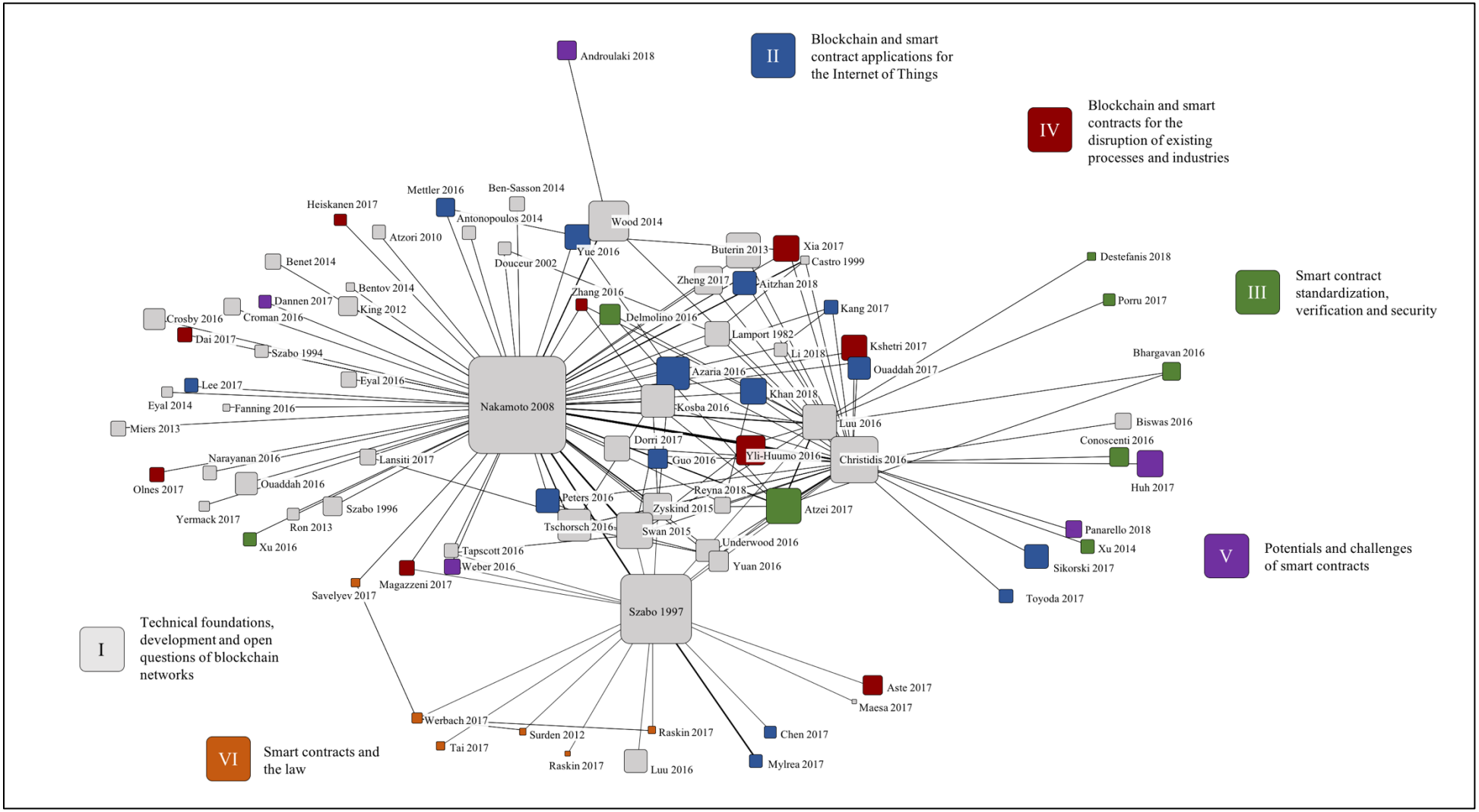

Figure 7. Visualization of research stream interrelations. The size of a node represents the absolute number of citations, lines between articles represent at least six co-citations between articles. For readability, only first authors are shown. The color of each node reflects its likeliest research stream affiliation. Created with UCINET software.

The highest relevance of Nakamoto (2008) is immediately evident. A large number of publications are distributed around the Bitcoin whitepaper, which is a constant of the research field. Szabo (1997) likewise has great relevance across the network, a fact that was not indicated through factor analysis. With a factor loading of 0.454, the study is most closely associated with stream I, though it also has a factor loading of 0.443 and factor score of 3.11 in stream VI. Publications on smart contracts and the law (stream VI) are more closely related to Szabo (1997) than Nakamoto (2008), which makes sense given Nick Szabo's legal background. Stream VI is an emerging cluster that develops at a certain distance from other streams. Here – unsurprisingly, since it is a separate discipline – the publications are thematically more remote from the other strands of research. There are also initial signs that streams III and V are forming into independent clusters, which in turn have a clear link to Christidis and Devetsikiotis (2016), the publication with the most citations (cf. Table 3).

The visualization of the research field shows that the ideas and scientific approaches are still relatively close to each other thematically. A likely explanation is that smart contracts are a very young technology, whose potential, benefits and sustainability have not yet been fully clarified. Much of the research still centers on fundamental questions.

5 Discussion

5.1 Reflections on the state of smart contract research

The analysis of the primary data set allowed us to gain an overview of the current state of research on smart contracts. Smart contracts represent a technological basis for the reliable handling of decentralized business processes. As described above, they entail various benefits that can unleash untapped potential. These relate to security, privacy, access control, decentralization, fairness, traceability, trust and sustainability. Research on smart contracts has already produced substantial findings, but the discourse is still at an early stage, as indicated by the exponential growth in the number of publications (see Figure 3).

At present, the majority of publications on the topic belong to the fields of computer sciences and engineering. This is because smart contracts are at first a technological application rather than a concept. In order to assess the implications of the technology and to discuss and design appropriate applications, basic technical research is required. To a certain extent this is also transferable for legal aspects, where, in the context of research, there is an intensive debate about the compatibility of law and smart contracts and their potential implications. However, so far there is hardly any actual case law or draft legislation on smart contracts.

The articles with the greatest number of citations in the field of smart contracts often treat smart contracts as a side issue. Rather, topics such as IoT (e.g. Christidis and Devetsikiotis 2016; Novo 2018; Reyna et al. 2018; Y. Zhang and Wen 2017) or healthcare and data sharing (e.g. Dagher et al. 2018; Xia et al. 2017; P. Zhang et al. 2018) are in the foreground. Accordingly, the question arises as to whether "the" smart contract research environment actually exists or whether it rather represents a technology or method that is mentioned and relevant, but hardly in the foreground of science. Presumably future investigations will be able to provide more clarity in this regard. Will there be major smart contract-specific publications or will topics like blockchain technology, IoT oder underlying characteristics like security, privacy or access

management stand in the foreground? The keywords “smart contract” and “smart contracts” were used in 66% of the publications, while 74% of articles mentioned “blockchain” as keyword. This suggests that smart contracts could currently still be “assigned” to the overarching research discourse of blockchain technology. This is basically not surprising, since blockchain technology, or distributed ledger technology, is currently the only truly decentralized infrastructure for the application of smart contracts.

The two most important countries in terms of the number of publications are China and the US. They have a clear proximity as they belong to the same cluster and are very close to each other in the network (see Figure 5). On the basis of the network analysis, a European-character cluster seems to be closer to the US, while an Asian-character cluster seems to be closer to China. Other countries that form links between different clusters, i.e. represent central points in the research environment are England, Canada and Italy. It is important to observe whether research is moving further apart or whether the network can become denser. Based on the identified results, there is, for example, only little smart contract-related scientific exchange between countries of the green cluster (e.g. Germany, France, Estonia, Switzerland, Russia) and the red cluster (e.g. Spain, Taiwan, South Korea, Japan, Malaysia). An implication of this could be to push explicitly scientific exchange between these far apart countries in order to increase the efficiency of the research environment, output and the dissemination of results.

It should be noted that we could not identify any relevant results regarding the academic exchange between organizations, i.e. via co-author network analysis. With 8 publications, the Chinese Academy of Science is the institution with the comparatively largest number of smart contract publications. However, this corresponds to "only" 1.7% of all publications. Research on smart contracts is currently widely distributed. In view of the fact that smart contracts have only gained in relevance through the invention of blockchain technology, which in turn has emerged in 2008, there is still little research, research groups or professorships that deal exclusively with smart contracts. Accordingly, it is important to observe the extent to which such research clusters form and the extent to which individual organizations can achieve outstanding positions in the smart contract discourse.

In summary, it can be said that the scientific discourse on smart contracts is still in its infancy, as is evident from the exploding number of publications on the subject in recent years. Accordingly, no “final” statements can be made about the discourse’s development – only that it is progressing in rapid steps.

5.2 Reflections on the intellectual structure of smart contract research

Factor analysis has helped us to identify six prominent research streams that form the intellectual structure of smart contract research. The first one – basic research on blockchain technology (and smart contracts) – accounts for over 25% of the scientific discourse. This high level of concentration on basics shows that the research is still in its infancy. It is important to point out that smart contracts are by no means the main topic of discussion, but rather Bitcoin, p2p networks/protocols, anonymity and consensus mechanisms. It is evident that the discourse became relatively less relevant from 2013 onwards (see Figure 6) - about when the publication of the Ethereum whitepaper made the potential of smart contracts widely known. Accordingly, the publications in stream I are trend-setting basic works that present relevant aspects,

characteristics and theories. This is also made clear by the fact that older trend-setting publications such as Lamport et al. (1982) and Pease et al. (1980), which obviously had nothing to do with blockchain or smart contracts at the time of publication, are located in the stream and now represent a highly relevant scientific basis for the research environment. Accordingly, we assume that stream one will continue to represent the most relevant (based on the explained variance) scientific discourse and stream over time.

Various other streams deal with detailed aspects but explain significantly lower shares in the research discourse. Stream II comprises publications on the application of smart contracts to IoT. As in stream one, the overall focus is by no means on smart contracts in general but on IoT. Research focuses on technical attributes such as automation, security, access management or network architectures. The topic of privacy in connection with these attributes is also addressed. Smart contracts are discussed as a technology that can help to ensure or appropriately implement these attributes. Assuming that the topic of IoT will increase in relevance in the future, it can be concluded that the topic of smart contracts in IoT will continue to be a significant factor in this environment. This depends, of course, on the extent to which fundamental open issues of blockchains and smart contracts such as scalability, upgrades, transaction costs or data protection can be resolved.

The third stream focuses on the public blockchain infrastructure Ethereum, specifically how Ethereum smart contracts can be standardized, secured and verified. This shows the high relevance of the Ethereum blockchain for smart contracts. While 52% of the literature examined in the secondary data set referred to Ethereum, this is the case for 96% of the publications assigned to stream III. Immutability as a key characteristic of blockchain technology and smart contracts also represents a general risk or challenge. Computer code is almost never error-free, so it could be argued that scripts that cannot be updated may not be such a smart idea. Prominent examples like The DAO show that smart contracts have considerable security risks that are exploited by attackers. It is accordingly understandable that the standardization, semantics and formal verification of smart contracts represents a significant and distinct scientific discourse - the largest one that explicitly refers to the topic of smart contracts. At present, there is no reason to believe that this topic will become less relevant in the future.

In stream IV, social and economic aspects and implications of smart contracts are discussed: How can this new technology lead to social change, collaboration or the transformation of industries? This is the first scientific discourse that has no technical focus, but rather deals specifically with fields of application such as energy markets or the healthcare sector, as well as relevant underlying mechanisms such as governance and collaboration. This shows that the technological basis and understanding of smart contracts at least to some extent is sufficient to make relevant forecasts and implications. To what extent these forecasts are compatible with the actual (short-term) applicability of smart contracts remains to be seen. What is clear is that smart contracts can reduce incentive problems and uncertainty and allow disintermediation. While 'more utopian existences' according to Goertzel et al. (2017) seem to be far away, it is conceivable that smart contracts could be an essential basis for system changes or the change of industries as described by Peck (2017). It remains to be seen to what extent the sectors discussed in the stream's literature (e.g. energy, healthcare, governance, data, finance, e-government) will be disrupted or changed by smart contracts in the short or long term.

The fifth stream deals with challenges and potentials of smart contracts and focuses on use cases. In view of the comparatively low number of publications with a high fit (factor loading > 0.7) in the stream, it is quite possible that this stream will dissolve, consolidate or change drastically with time. This is also well visualized in the social network (see Figure 7). The relevant publications are spread all over the place and do not (yet) form a “real” cluster.

Finally, the sixth stream deals not with technological but with legal issues. The articles are primarily concerned with the extent to which smart contracts can and should be legally binding contracts. Building on basic legal literature, the topic of smart contracts is critically discussed. There seems to be an overall consensus that smart contracts cannot replace classic law (e.g. Werbach and Cornell 2017; Mik 2017). As described in Section 3.1, the use of the terms "smart" and "contract" is rather misleading, as a smart contract is first and foremost only computer code and not a contract. The question arises how big the scientific debate and output on the topic would be, if the term "contract" would not be part of its name. Legally binding smart contracts are conceivable, but computer code has no flexibility, i.e. is not smart, while real contracts are enforced by social mechanisms and often leave room for interpretation of certain clauses (e.g. Levy 2017). Even if smart contract will not replace the law as such, it is important to observe and further explore the extent to which different forms of smart contract designs are suitable for binding legal agreements or processes.

The results illustrate the interdisciplinary importance of the technology. While the literature is currently dominated by technical and legal issues, economic publications on the topic are comparatively rare. Social network analysis has shown that some scientific discourses are quite interrelated, which suggests that knowledge is being shared across the streams. However, individual clusters are also emerging, so the exchange of knowledge with the other discourses continues to be important. Most of the research is currently of a technical nature (streams I, II, III and V), but social (IV) and legal (VI) issues are also being addressed. By implication, economic aspects are currently receiving little attention – a starting point for future research.

Blockchain technology and smart contracts are highly innovative environments that are developing rapidly outside of scientific research. This becomes clear not least from the social network analysis. Neither of the two largest nodes are peer reviewed publications. This suggests that researchers should not hesitate to collaborate with in active projects and to review grey literature outside of academic research to monitor current developments. While the peer review provides the desired security and seal of approval for this analysis, the process also involves a considerable time lag. For this reason, future research should always bear in mind the blockchain/smart contract ecosystem and the grey literature on the topic.

6 Future research avenues

In the following, future research avenues for smart contract research are discussed. Table 13 shows a summary of the various avenues for future research that are described in the following sub-sections.

Table 13. Future avenues of smart contract research

Research topic	Description / sub-topic	Examples of methodology, approaches or preparatory work
A holistic definition of smart contracts	Development of a holistic definition or description.	Rotolo et al. (2015)
Quō vādis smart contract research?	Literature reviews (systematic/scoping/qualitative)	Macrinici et al. (2018); Almasoud et al. (2020); Almakhour et al. (2020)
	Bibliometric reviews (including network and text analysis)	*This study;* Zupic and Čater (2015); Glenisson et al. (2005)
	Knowledge diffusion paths	Yu and Sheng (2020)
Who uses smart contracts and why?	On-chain smart contract (address) analysis	Bartoletti and Pompianu (2017); Pinna et al. (2019)
	Technology acceptance and analysis	Davis (1985); Lee et al. (2003)
	Motives and profiles of smart contract users	Fisch et al. (2019)
Smart contract infrastructure	Smart contract platforms (i.e. blockchains and distributed ledgers)	Kuo et al. (2019); Le Pennec (2020)
	Irreversibility / upgrades	OpenZeppelin (2020)
	Scaling (layer 1 and layer 2)	Poon and Buterin (2017); Teutsch and Reitwießner (2017)
	Mining / transactions / transaction fees	Daian et al. (2020); Strehle and Ante (2020)
	(Pseudo-)Anonymity / privacy / data security	Finck (2018); Zyskind et al. (2015); Stokkink and Pouwelse (2018)
	Oracles, i.e. information transmission between smart contracts and the real world	Al-Breiki et al. (2020); Beniiche (2020)
	Languages / semantics, standardization and (formal) verification	Clack et al. (2016); Atzei et al. (2017); Harz and Knottenbelt (2018)
	Automated smart contract creation	Frantz and Nowostawski (2016)
	Attacks and vulnerabilities	Luu, Chu, et al. (2016)
Legal analysis and implications	Legal analysis and regulation of specific smart contracts applications	
	Embedding existing law into smart contracts	Marino and Juels (2016); Clack et al. (2016)
Decentralized applications, markets, organizations and ecosystems	Disintermediation and transformation of existing industries and processes; Decentralized Finance (DeFi)	Chen and Bellavitis (2019); Schär (2020)
	Decentralized applications (dApps), blockchain games/gambling and Decentralized autonomous organizations (DAOs)	Jentzsch (2016); Grossman et al. (2017)

6.1 A holistic definition of smart contracts?

Szabo (1994) defined a smart contract as a piece of computerized transaction protocol that satisfies contractual conditions such as payment terms, confidentiality or enforcement, reduces exceptions and minimizes the need for trusted intermediaries. In this article, we defined smart

contracts as decentrally anchored scripts on blockchains or similar infrastructures that allow the transparent execution of predefined processes. But do scripts need to be decentrally anchored and does it really need blockchain or similar infrastructures for smart contracts? Is the term "transparent" suitable? Do processes need to be fully predefined? While the definition chosen here is sufficient with regard to the questions examined in this study, it is probably not a final or conclusive statement. So where does computer code end and smart contracts begin – or is that a continuum? Underlying blockchain infrastructures clearly differ. While some platforms, such as Ethereum, are public and permissionless, other blockchains, or distributed ledgers, are private or permissioned. Are we still talking about smart contracts when code is executed on private blockchains? In order to better understand the concept of smart contracts, basic research should be carried out at the very highest level, which can provide a basis for a better definition of these topics.

Research should deal in detail with characteristics, properties and requirements of smart contracts in order to come closer to a holistic definition of the construct. Such an investigation should be interdisciplinary, since technical, economic and legal topics must be covered accordingly. Scientometric methods can be a suitable basis for clarifying this very question (e.g. Rotolo et al. 2015). A study could systematically analyze literature on the topic of smart contracts according to author's definitions and, based on this, collect and analyze underlying attributes in a structured way and develop a holistic definition or description.

6.2 Quō vādis smart contract research?

The topic of smart contracts is a rather new and rapidly developing topic (cf. Figure 2). The scientific discourse has clearly changed in recent years and has become more diverse (cf. Figure 6), so it seems realistic that this will also be the case in the future. For this reason, we see a starting point for future research in the analysis of the research environment using scientometric methods. At the current time, clusters are not yet clearly distinguishable in the research environment (cf. Figure 7). This will likely change with more scientific output.

Research can investigate specific application areas, topics or mechanisms in literature reviews, as has, for example, already been done for reputation systems using smart contracts (Almasoud et al. 2020) or smart contract verification (Almakhour et al. 2020). Further specific bibliometric analyses can also generate important findings. While this study takes a holistic view of smart contracts, specific topics could also be examined. This includes, for example, a focus on legal, technical or economic issues or use cases/sectors or attributes of smart contracts. Besides the methods used in this thesis, co-word or co-author analyses can be performed (Zupic and Čater 2015) as well as abstract or manuscript text data analysis (Glenisson et al. 2005). Finally, the detailed analysis of knowledge diffusing paths, i.e. path analysis, can contribute to the understanding of scientific discourses and related developments (Yu and Sheng 2020).

6.3 Who uses smart contracts?

Smart contracts are currently used, but hardly for the use cases that are most discussed in the literature (i.e. IoT, healthcare, supply chains). In fact, smart contracts are mostly used for the issuance of blockchain tokens, corporate and project financing in the form of token sales, decentralized exchanges (DEXes) for trading of blockchain tokens, multi-signature wallets (to

securely store tokens), blockchain games and gambling applications (e.g. Bartoletti and Pompianu 2017; Pinna et al. 2019). Since applications of smart contracts and the resulting ecosystems are constantly changing, research should further advance the topic of blockchain or smart contract data analysis to understand who uses smart contracts, when and why. While blockchain analysis sites like *dappradar.com* track decentralized applications and their (daily active) users, it remains unclear how many how many people in a population use and understand smart contracts and what their perceptions towards the technology are.

A representative survey of population data or survey data from businesses on the adoption, understanding and use of smart contracts (or corresponding applications and methods using smart contracts) could provide a much clearer picture of the overall relevance of smart contracts for society, business and regulators. For example, the technology acceptance model (TAM) (Davis 1985) or related theories could be used to analyze which characteristics are most relevant for the future use of smart contracts (Lee et al. 2003). This can help to support future adoption of smart contract applications, since essential criteria (e.g. the relevance of perceived ease of use, usefulness, risks etc.) are known and understood.

Given that the proportion of smart contract users in a population – be it consumers or businesses – is likely very low (a subset of blockchain users), addressing smart contract users directly as part of a survey could also yield exciting findings. For consumers, it would be possible to identify the motives and factors underlying the use of (specific) smart contracts. For example, an investigation could focus on users of gambling smart contracts to find out whether the motives for participating in the applications are based, for example, on the decentralized nature of the service, the verifiable chances of winning, or the high degree of anonymity. It would also be interesting to ask companies about their use and experience with smart contracts. From this it could be deduced to what extent companies use public (e.g. Ethereum) or private (e.g. Hyperledger) blockchains for smart contract applications and why this is the case.

6.4 Smart contract infrastructure

6.4.1 Blockchains and other distributed ledger technologies

Smart contracts run on blockchains and other distributed or decentralized systems. Our analysis has uncovered 41 different smart contract platforms (cf. Table 6) - and this only in the underlying discourses of smart contract research. It can be assumed that there are significantly more platforms that either do not play such a large role in the scientific discourse or are simply too new to be included in the peer reviewed literature. While there are several scientific publications that provide an overview and comparison of blockchain infrastructures (e.g. Kuo et al. 2019; Le Pennec 2020), they do not explicitly focus on smart contract platforms or characteristics of smart contracts. Technology evaluation is an important and time-consuming process in blockchain projects. Independent and objective comparisons of different smart contract platforms not only offer added value for research, but can also reduce search costs for businesses and regulators. Currently the ‘blockchains of choice’ are mostly Ethereum (for public blockchain projects) or Hyperledger (for private blockchain projects). The respective scientific publications or whitepapers of these two projects can also be found among the research streams and in the social network (Androulaki et al. 2018; Buterin 2013; Wood 2014).

A detailed analysis of technologies can help determine whether this is due to network effects, technology aspects, documentation quality or other factors.

6.4.2 Blockchain challenges: irreversibility, scalability, transactions, privacy, oracles

Blockchain transactions are irreversible, which also means that once smart contracts are anchored in the blockchain, they cannot be changed. If a bug is discovered in a smart contract at a later date, it cannot be easily fixed. In theory, the faulty smart contract can be replaced by a new one, but this in turn brings with it new complex challenges, such as the transfer of old data. While research deals intensively with the verification and standardization of smart contracts, upgrades have so far played a minor role. There are already implementations, such as OpenZeppelin (2020), which allow updates of smart contracts. For this purpose, users must consider the option of a future upgrade during the initial implementation. However, this leads to the problem that the smart contract is not an autonomous, decentralized structure, as the idea of the blockchain envisages, but a decentralized, centrally managed structure. Various blockchain projects use governance tokens to determine changes in their protocols, i.e. the central control over the upgrade function is placed in the hands of a community or investors. Research should deal in detail with the question of the upgradability of smart contracts and respective entitlements to conduct such upgrades (i.e. governance and reputation systems).

Public blockchains like Ethereum suffer from performance issues because every node in the network processes every transaction. The network regularly slows down due to specific events like, for example, the rapid growth of the blockchain game CryptoKitties (BBC 2017). One potential solution is sharding, where the network is separated into different “shards” that confirm transactions independent from each other. This way, the performance of the blockchain can be increased (Luu, Narayanan, et al. 2016). Sharding is referred to as a layer 1 solution, as it is implemented on the blockchain. Layer 2 solutions like Plasma (Poon and Buterin 2017) or Truebit (Teutsch and Reitwießner 2017) aim at scaling blockchains by outsourcing some “work” off-chain using cryptographic methods. For example, complex computation of smart contracts could be processed off-chain. Since the scalability of blockchain or similar systems is a highly relevant factor for the use of smart contracts, we conclude that this very research has high future relevance.

Another blockchain-related challenge is the mining process, i.e. the way transactions are broadcasted and confirmed. Public smart contract platforms like Ethereum do not use transaction ordering or confidentiality, which can result in frontrunning attacks, i.e. bots analyzing initiated but not yet confirmed transactions and trying to push themselves with higher transaction costs before the initiated transaction. This has been identified as an ongoing problem for decentralized exchanges (Daian et al. 2020). Additionally, fee stability on public blockchains represents an open issue (e.g. Hammi et al. 2018). Exclusive mining (Strehle and Ante 2020) or layer 2 scaling may represent solutions to tackle such challenges. Another mining or blockchain-related challenge for smart contracts are initiation fees. Blockchain network require transaction initiators to submit fees in order to process transfers. However, if a method could be developed that would allow fees to be paid by the recipient of a transaction, the efficiency and potential of smart contracts could be significantly increased. Another promising avenue of research are meta-transactions, i.e. transaction fees being paid in other (non-native) cryptocurrencies (Seres 2020).

The degree of anonymity or privacy of blockchains is a major topic in research stream I (e.g. Ben-Sasson et al. 2014; Miers et al. 2013), which illustrates the high relevance of the topic. While initial approaches had rather anonymous behavior on the internet in mind, further topics such as legal provisions on data protection (e.g. the EU's General Data Protection Regulation (GDPR)) or the secrecy of information in an industrial context (e.g. supply chain data) became relevant aspects (Finck 2018). Currently, insecurity surrounding data protection and confidentiality is likely a major obstacle to companies using smart contracts on (public) blockchains. Accordingly, research should analyze to what extent personal data (Zyskind et al. 2015), (self-sovereign) identities (Stokkink and Pouwelse 2018) or firm data can be used securely on blockchains and in smart contracts.

Smart contracts do not execute themselves but must always be triggered in some way – the term "self-executing" is often used in the context of smart contracts, but does not fit. If this trigger is external data (off-chain), one speaks of oracles. Oracles serve as a bridge between the on-chain and off-chain world. However, as soon as external information is transmitted to a smart contract, the question of security arises. How is the validity of this information assured? Can it be manipulated? Beniiche (2020) outlines a classification of types of oracles based on source, direction of information and trust. The author additionally describes seven different types of oracles and discusses centralized versus decentralized oracles. There are currently a large number of different oracle solutions, which in turn rely on different mechanisms (Al-Breiki et al. 2020). We see it as an important task of future research to investigate oracles more closely. Such studies could aim to define more precisely how data security can be guaranteed for oracles and which methodology, governance scheme, incentive mechanisms or degree of centralization are most suitable for which application, i.e. work on the development of standards and best practices for oracles.

6.5 Standardization, automation and formal analysis

Standards are essential for the success and application of smart contracts. While Ethereum already has individual standards (such as the ERC-20 standard for tokens) or audited smart contract libraries (such as OpenZeppelin), these are community or private approaches rather than regulated public standards. The continuous development of tools for the standardization and verification of smart contracts is extremely important. There is not yet "the" smart contract infrastructure. Against this background, future research should holistically evaluate and develop the security of smart contracts.

Further topics of interest for research are semantics and (automated) formal analysis (e.g. Clack et al. 2016). If research is able to further develop automated formal analysis and verification tools, risks associated with smart contracts can be reduced in the future. Accordingly, it is also necessary to investigate the extent to which different smart contract languages are suitable for this purpose (cf. Atzei et al. 2017) or whether new smart contract languages should be developed. Harz and Knottenbelt (2018)’s survey provides an overview and introduction of the topic. Another promising research approach is to extend research on the automation of smart contracts creation, as initially described by Frantz and Nowostawski (2016). The analysis of different vulnerabilities and attack vectors of smart contracts, as well as the development of auditing tools and use of theorem provers (e.g. Luu, Chu, et al. 2016; T. Chen et al. 2017; Hildenbrandt et al. 2018) will remain a major research direction.

6.6 Legal analysis and challenges

To effectively regulate smart contracts, it needs to be defined what smart contracts are (cf. Section 6.1). Only if it is explicitly defined what exactly smart contracts are, lawyers can deal in detail with the question of regulation. At the same time, the question arises whether (direct) regulation of smart contracts is necessary at all. In the end, it is only computer code. Rather, it might make more sense to regulate smart contracts against the background of the respective applications, risks and implications. For example, if the smart contract is a decentralized gambling application, regulation should potentially be different than if a smart contract is a protocol for the issuance and trading of securities. Accordingly, we see it as a future research approach to delve much more specifically into the respective application cases and evaluate their legal classification. A holistic view and evaluation of the concept of smart contracts is already quite advanced. More specific analyses can pave the way to actual (widespread) applicability.

The compatibility of existing (contract) law and smart contracts is an important research question. As described above, research generally agrees that smart contracts will not replace the law as such, but they may well represent specific legally binding contracts. Therefore, it is necessary to understand how smart contract technology can or cannot represent law. The study of Marino and Juels (2016) represents a basis for the further development of a technical smart contract framework that bases on contract law and lets parties alter or undo smart contracts based on defined conditions. However, research should not be based solely on contract law - a possible mistake associated with the term "smart contract". It is necessary to define to what extent smart contracts can be designed in such a way that, for example, securities or insurance policies can be created and processed using them. For example, there is already a draft bill for digital securities in Germany (BMJV and BMF 2020), which however does not refer to the term smart contract (but blockchain).

6.7 Decentralized business models, markets, organizations and ecosystems

Smart contract research has identified a variety of target industries and use cases, such as IoT, logistics and healthcare. Besides these rather obvious fields of application, it seems likely that more complex use cases are around the corner, including for example the decentralized finance (DeFi) ecosystem (e.g. Chen and Bellavitis 2019; Schär 2020). Price-stable digital currencies (so-called stablecoins) are issued and managed through smart contract protocols, and can be transferred, borrowed and lent among the users via other smart contracts without the need for any central entity like a bank. While this form of decentralized, programmable money and financial system is still in its infancy and obviously still faces many challenges, it is a suitable example of where the journey could go. It does not end with an innovative product – other projects base on it, which results in the creation of own ecosystems. At present, this can be observed for a DeFi system whose long-term success is completely unclear. Nevertheless, this leads to innovation pressure and a similar development is conceivable for other industries, sectors and applications – a question for future studies.

In addition to superordinate markets or ecosystems, the detailed examination and analysis of individual smart contract applications allows a better understanding of the potentials and challenges associated with the technology. Especially smart contracts that manage large

amounts of assets (e.g. decentralized exchanges, gambling dApps or multi-signature wallets) are of interest. These can be single dApps or more complex constructs like DAOs. Research around the project and the hack of The DAO can be a basis for this (e.g. Jentzsch 2016; Grossman et al. 2017).

7 Conclusion

The results of this study offer researchers and practitioners a substantial basis from which to understand and further pursue the topic of smart contracts. Based on bibliometric methods, the current state of research on smart contracts and its underlying scientific foundations are analyzed and reviewed. We have shown that research on the topic has rapidly grown in recent years and which journals, jurisdictions, keywords and publications are of the greatest relevance. Furthermore, we saw which blockchain infrastructure solutions receive the most research attention – Ethereum and Hyperledger. Factor analysis has allowed us to conduct an objective evaluation of the intellectual foundations of the research discourse, which has yielded six subcategories of research on smart contracts. These make it clear that smart contracts are not just a technology but rather an interdisciplinary concept that must be viewed from various angles. While we uncover various findings on the topic of smart contracts, it becomes clear that there is still a great deal of uncertainty. Accordingly, we derive various paths for future investigations. While the potentials of smart contracts seem clear it remains unclear if, when and to what degree these potentials can be used.

Literature

Al-Bassam, M. (2017). SCPKI: A smart contract-based PKI and identity system. In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts* (pp. 35–40). doi:10.1145/3055518.3055530

Al-Breiki, H., Rehman, M. H. U., Salah, K., & Svetinovic, D. (2020). Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges. *IEEE Access*, *8*, 85675–85685. doi:10.1109/ACCESS.2020.2992698

Alharby, M., & Moorsel, A. van. (2018). Blockchain Based Smart Contracts: A Systematic Mapping Study. In *2018 International Conference on Cloud Computing, Big Data and Blockchain* (pp. 1–6). doi:10.5121/csit.2017.71011

Almakhour, M., Sliman, L., Samhat, A. E., & Mellouk, A. (2020). Verification of smart contracts: A survey. *Pervasive and Mobile Computing*, *67*, 101227. doi:https://doi.org/10.1016/j.pmcj.2020.101227

Almasoud, A. S., Hussain, F. K., & Hussain, O. K. (2020). Smart contracts for blockchain-based reputation systems: A systematic literature review. *Journal of Network and Computer Applications*, *170*, 102814. doi:https://doi.org/10.1016/j.jnca.2020.102814

Amani, S., Bortin, M., Bégel, M., & Staples, M. (2018). Towards verifying ethereum smart contract bytecode in Isabelle/HOL. In *Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs* (pp. 66–77). doi:10.1145/3167084

Androulaki, E., Barger, A., Bortnikov, V., Muralidharan, S., Cachin, C., Christidis, K., et al. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, *2018-Janua*. doi:10.1145/3190508.3190538

Ante, L. (2020). A place next to Satoshi: scientific foundations of blockchain and cryptocurrency in business and economics. *Scientometrics*, *124*(2), 1305–1333. doi:10.1007/s11192-020-03492-8

Ante, L., & Fiedler, I. (2019). Cheap Signals in Security Token Offerings (STOs). doi:10.2139/ssrn.3356303

Ante, L., Sandner, P., & Fiedler, I. (2018). Blockchain-Based ICOs: Pure Hype or the Dawn of a New Era of Startup Financing? *Journal of Risk and Financial Management*, *11*(4), 80. doi:10.3390/jrfm11040080

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). In *International conference on principles of security and trust* (pp. 164–186).

Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A blockchain future for internet of things security: a position paper. *Digital Communications and Networks*, *4*(3), 149–160. doi:10.1016/j.dcan.2017.10.006

Bartoletti, M., & Pompianu, L. (2017). An Empirical analysis of smart contracts: Platforms, applications, and design patterns. In *Lecture Notes in Computer Science* (pp. 494–509). doi:10.1007/978-3-319-70278-0_31

BBC. (2017). CryptoKitties craze slows down transactions on Ethereum. https://www.bbc.com/news/technology-42237162. Accessed 12 August 2020
Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. *Proceedings - IEEE Symposium on Security and Privacy*, 459–474. doi:10.1109/SP.2014.36
Benchoufi, M., Porcher, R., & Ravaud, P. (2017). Blockchain protocols in clinical trials: Transparency and traceability of consent. *F1000Research*, *6*, 1–66. doi:10.12688/f1000research.10531.1
Beniiche, A. (2020). A Study of Blockchain Oracles. http://arxiv.org/abs/2004.07140
Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract]. *ACM SIGMETRICS Performance Evaluation Review*, *42*(3), 34–37. doi:10.1145/2695533.2695545
Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., Gonthier, G., Kobeissi, N., et al. (2016). Formal verification of smart contracts: Short paper. In *PLAS 2016 - Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security* (pp. 91–96). doi:10.1145/2993600.2993611
Biehl, M., Kim, H., & Wade, M. (2006). Relationships among the academic business disciplines: A multi-method citation analysis. *Omega*, *34*(4), 359–371. doi:10.1016/j.omega.2004.12.002
Bigi, G., Bracciali, A., Meacci, G., & Tuosto, E. (2015). Validation of decentralised smart contracts through game theory and formal methods. *Lecture Notes in Computer Science*, *9465*, 142–161. doi:10.1007/978-3-319-25527-9_11
Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014). Deanonymisation of clients in bitcoin P2P network. In *Proceedings of the ACM Conference on Computer and Communications Security* (pp. 15–29). doi:10.1145/2660267.2660379
BMJV, & BMF. (2020). Entwurf eines Gesetzes zur Einführung von elektronischen Wertpapieren. https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Einfuehrung_elektr_Wertpapiere.pdf?__blob=publicationFile&v=1. Accessed 1 September 2020
Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017). Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain. In *2017 IFIP/IEEE symposium on integrated network and service management* (pp. 772–777). IEEE. doi:10.23919/INM.2017.7987376
Borgatti, S. P., Everett, M. G., & Freeman, L. C. (2002). Ucinet for Windows: Software for social network analysis. *Harvard MA: analytical technologies*, *6*.
Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., & Sirdey, R. (2017). Towards better availability and accountability for IoT updates by means of a blockchain. In *Proceedings - 2nd IEEE European Symposium on Security and Privacy Workshops* (pp. 50–58). doi:10.1109/EuroSPW.2017.50
Brandstätt, C., Brunekreeft, G., & Friedrichsen, N. (2011). Locational signals to reduce network investments in smart distribution grids: What works and what not? *Utilities Policy*, *19*(4), 244–254. doi:10.1016/j.jup.2011.07.001
Buterin, V. (2013). *Ethereum White Paper - A Next Generation Smart Contract & Decentralized Application Platform*. http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
Buterin, V. (2018). Twitter Post on 13. October 2018. https://twitter.com/VitalikButerin/status/1051160932699770882?s=20. Accessed 14 February 2020
Carrington, P. J., Scott, J., & Wassermann, S. (2005). *Models and methods in social network analysis*. New York, NY: Cambridge University Press.
Casado-Vara, R., Prieto, J., La Prieta, F. De, & Corchado, J. M. (2018). How blockchain improves the supply chain: Case study alimentary supply chain. *Procedia Computer Science*, *134*, 393–398. doi:10.1016/j.procs.2018.07.193
Castro, M., & Liskov, B. (2002). Practical Byzantine Fault Tolerance and Proactive Recovery. *ACM Transactions on Computer Systems*, *20*(4), 398–461. doi:10.1145/571637.571640
Chen, J., Xia, X., Lo, D., Grundy, J., & Yang, X. (2020). *Maintaining Smart Contracts on Ethereum: Issues, Techniques, and Future Challenges*.
Chen, S., Shi, R., Ren, Z., Yan, J., Shi, Y., & Zhang, J. (2017). A Blockchain-Based Supply Chain Quality Management Framework. In *Proceedings - 14th IEEE International Conference on E-Business Engineering* (pp. 172–176). doi:10.1109/ICEBE.2017.34
Chen, T., Li, X., Luo, X., & Zhang, X. (2017). Under-optimized smart contracts devour your money. In *24th IEEE International Conference on Software Analysis, Evolution, and Reengineering* (pp. 442–446). IEEE. doi:10.1109/SANER.2017.7884650
Chen, Yan, & Bellavitis, C. (2019). Blockchain Disruption and Decentralized Finance: The Rise of Decentralized Business Models. *Journal of Business Venturing Insights*, *13*. doi:10.1016/j.jbvi.2019.e00151
Chen, Ye-Sho, & Leimkuhler, F. F. (1986). A relationship between Lotka's Law, Bradford's Law, and Zipf's

Law. *Journal of the American Society for Information Science*, *37*(5), 307–314.
Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. doi:10.1109/ACCESS.2016.2566339
Clack, C. D., Bakshi, V. A., & Braine, L. (2016). Smart Contract Templates: foundations, design landscape and research directions, 1–15. http://arxiv.org/abs/1608.00771
Counterparty. (2020). Counterparty documentation. https://counterparty.io/docs. Accessed 18 February 2020
Cuccuru, P. (2017). Beyond bitcoin: An early overview on smart contracts. *International Journal of Law and Information Technology*, *25*(3), 179–195. doi:10.1093/ijlit/eax003
Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, *39*, 283–297. doi:10.1016/j.scs.2018.02.014
Dai, J., & Vasarhelyi, M. A. (2017). Toward Blockchain-Based Accounting and Assurance. *Journal of Information Systems*. doi:10.2308/isys-51804
Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., et al. (2020). Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 910–927). doi:10.1109/SP40000.2020.00040
Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. Massachusetts Institute of Technology.
Destefanis, G., Marchesi, M., Ortu, M., Tonelli, R., Bracciali, A., & Hierons, R. (2018). Smart contracts vulnerabilities: A call for blockchain software engineering? *2018 IEEE 1st International Workshop on Blockchain Oriented Software Engineering - Proceedings*, 19–25. doi:10.1109/IWBOSE.2018.8327567
Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering*, *30*(7), 1366–1385. doi:10.1109/TKDE.2017.2781227
DiStefano, C., Zhu, M., & Mîndrilă, D. (2009). Understanding and using factor scores: Considerations for the applied researcher. *Practical Assessment, Research and Evaluation*, *14*(20).
Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017). BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Communications Magazine*, *55*(12), 119–125. doi:10.1109/MCOM.2017.1700879
Douceur, J. R. (2002). The Sybil Attack. In *International workshop on peer-to-peer systems* (pp. 251–260). doi:10.1145/984622.984660
Egelund-Müller, B., Elsman, M., Henglein, F., & Ross, O. (2017). Automated Execution of Financial Contracts on Blockchains. *Business and Information Systems Engineering*, *59*(6), 457–467. doi:10.1007/s12599-017-0507-z
Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, *5*(1), 31–37. doi:10.1109/MCC.2018.011791712
Ethereum. (2020). Ethereum frontier guide. https://ethereum.gitbooks.io/frontier-guide. Accessed 18 February 2020
Eyal, I., Gencer, A. E., Sirer, E. G., & van Renesse, R. (2015). Bitcoin-NG: A Scalable Blockchain Protocol. In *Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation*.
Fairfield, J. (2014). Smart Contracts, Bitcoin Bots, and Consumer Protection. *Washington and Lee Law Review Online*, *71*(2), 35–50.
Fiedler, I., Ante, L., Steinmetz, F., & Häseler, S. (2018). Distributed Ledger Technology: A Possible Way Forward for Securities Clearing. *Binary District*. https://journal.binarydistrict.com/distributed-ledger-technology-a-possible-way-forward-for-securities-clearing. Accessed 8 September 2019
Finck, M. (2018). Blockchains and Data Protection in the European Union. *European Data Protection Law Review*, *4*(1), 17–35. doi:10.21552/edpl/2018/1/6
Firdaus, A., Razak, M. F. A., Feizollah, A., Hashem, I. A. T., Hazim, M., & Anuar, N. B. (2019). The rise of "blockchain": bibliometric analysis of blockchain study. *Scientometrics*, *120*(3), 1289–1331. doi:10.1007/s11192-019-03170-4
Fisch, C., Masiak, C., Vismara, S., & Block, J. (2019). Motives and profiles of ICO investors. *Journal of Business Research*. doi:10.1016/j.jbusres.2019.07.036
Frantz, C. K., & Nowostawski, M. (2016). From Institutions to Code: Towards Automated Generation of Smart Contracts. In *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W)* (pp. 210–215). IEEE. doi:10.1109/FAS-W.2016.53
Glenisson, P., Glänzel, W., & Persson, O. (2005). Combining full-text analysis and bibliometric indicators. A pilot study. *Scientometrics*, *63*(1), 163–180. doi:10.1007/s11192-005-0208-0
Goertzel, B., Goertzel, T., & Goertzel, Z. (2017). The global brain and the emerging economy of abundance: Mutualism, open collaboration, exchange networks and the automated commons. *Technological Forecasting and Social Change*, *114*, 65–73. doi:10.1016/j.techfore.2016.03.022
Gorsuch, R. L. (1988). Exploratory Factor Analysis. In J. R. Nesselroade & R. B. Cattell (Eds.), *Handbook of*

Multivariate Experimental Psychology (pp. 231–258). Boston, MA: Springer US. doi:10.1007/978-1-4613-0893-5_6
Greenspan, G. (2015). Smart contracts: The good, the bad and the lazy. https://www.multichain.com/blog/2015/11/smart-contracts-good-bad-lazy. Accessed 26 March 2020
Grishchenko, I., Maffei, M., & Schneidewind, C. (2018). A Semantic Framework for the Security Analysis of Ethereum Smart Contracts. In *International Conference on Principles of Security and Trust* (pp. 243–269). Springer, Cham. doi:10.1007/978-3-319-89722-6
Grossman, S., Abraham, I., Golan-Gueta, G., Michalevsky, Y., Rinetzky, N., Sagiv, M., & Zohar, Y. (2017). Online detection of effectively callback free objects with applications to smart contracts. In *Proceedings of the ACM on Programming Languages* (Vol. 2, pp. 1–28). doi:10.1145/3158136
Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers and Security*, *78*, 126–142. doi:10.1016/j.cose.2018.06.004
Hardjono, T., & Smith, N. (2016). Cloud-based commissioning of constrained devices using permissioned blockchains. In *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security* (pp. 29–36). doi:10.1145/2899007.2899012
Harz, D., & Knottenbelt, W. (2018). Towards Safer Smart Contracts: A Survey of Languages and Verification Methods. https://arxiv.org/pdf/1809.09805
Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse Attacks on Bitcoin's Peer-to-Peer Network. *24th {USENIX} Security Symposium*, *14*, 129–144.
Herbaut, N., & Negru, N. (2017). A Model for Collaborative Blockchain-Based Video Delivery Relying on Advanced Network Services Chains. *IEEE Communications Magazine*, *55*(9), 70–76. doi:10.1109/MCOM.2017.1700117
Hildenbrandt, E., Saxena, M., Rodrigues, N., Zhu, X., Daian, P., Guth, D., et al. (2018). KEVM: A complete formal semantics of the ethereum virtual machine. In *Proceedings - IEEE Computer Security Foundations Symposium* (pp. 204–217). doi:10.1109/CSF.2018.00022
Hirai, Y. (2017). Defining the ethereum virtual machine for interactive theorem provers. *Lecture Notes in Computer Science*, 520–535. doi:10.1007/978-3-319-70278-0_33
Hölbl, M., Kompara, M., Kamišalić, A., & Zlatolas, L. N. (2018). A systematic review of the use of blockchain in healthcare. *Symmetry*, *10*(10). doi:10.3390/sym10100470
Jentzsch, C. (2016). Decentralized autonomous organization to automate governance. *White paper*.
Kaiser, H. F. (1959). Computer Program for Varimax Rotation in Factor Analysis. *Educational and Psychological Measurement*, *19*(3), 413–420. doi:10.1177/001316445901900314
Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. doi:10.1016/j.future.2017.11.022
Khaqqi, K. N., Sikorski, J. J., Hadinoto, K., & Kraft, M. (2018). Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. *Applied Energy*, *209*, 8–19. doi:10.1016/j.apenergy.2017.10.070
Kim, H. M., & Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance and Management*, *25*(1), 18–27. doi:10.1002/isaf.1424
King, S., & Nadal, S. (2012). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. http://peerco.in/assets/paper/peercoin-paper.pdf. Accessed 5 February 2020
Klarin, A. (2020). The decade-long cryptocurrencies and the blockchain rollercoaster: Mapping the intellectual structure and charting future directions. *Research in International Business and Finance*, *51*(January 2019), 101067. doi:10.1016/j.ribaf.2019.101067
Knirsch, F., Unterweger, A., & Engel, D. (2018). Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. *Computer Science - Research and Development*, *33*(1–2), 71–79. doi:10.1007/s00450-017-0348-5
Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In *Proceedings - 2016 IEEE Symposium on Security and Privacy* (pp. 839–858). doi:10.1109/SP.2016.55
Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027–1038. doi:10.1016/j.telpol.2017.09.003
Kuo, T.-T., Rojas, H. Z., & Ohno-Machado, L. (2019). Comparison of blockchain platforms: a systematic review and healthcare examples. *Journal of the American Medical Informatics Association, 26*(5), 462–478. doi:10.1093/jamia/ocy185
Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, *4*(3), 382–401.
Larios-Hernández, G. J. (2017). Blockchain entrepreneurship opportunity in the practices of the unbanked. *Business Horizons*, *60*(6), 865–874. doi:10.1016/j.bushor.2017.07.012
Le Pennec, G. (2020). *Choosing a Distributed Ledger Technology: Looking at the Popularity and Activity of*

Major Players. https://www.blockchainresearchlab.org/wp-content/uploads/2020/05/BRL-Report-No-5-DLT-Popularity.pdf
Lee, Y., Kozar, K. A., & Larsen, K. R. T. (2003). The Technology Acceptance Model: Past, Present, and Future. *Communications of the Association for information systems*, *12*(1), 50. doi:10.17705/1CAIS.01250
Lemieux, V. L. (2016). Trusting records: is Blockchain technology the answer? *Records Management Journal*. doi:10.1108/RMJ-12-2015-0042
Lerner, S. D. (2019). RSK - Rootstock Platform - Bitcoin Powered Smart Contracts - Whitepaper. doi:10.1017/CBO9781107415324.004
Lessig, L. (1999). The Limits in Open Code Regulatory Standards and the Future of the Net. *Berkeley Technology Law Journal*.
Levy, K. E. C. (2017). Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law. *Engaging Science, Technology, and Society*, *3*, 1. doi:10.17351/ests2017.107
Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. In *Proceedings of the ACM Conference on Computer and Communications Security* (pp. 254–269). doi:10.1145/2976749.2978309
Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016). A secure sharding protocol for open blockchains. In *Proceedings of the ACM Conference on Computer and Communications Security* (pp. 17–30). doi:10.1145/2976749.2978389
Macaulay, S. (1963). Non-Contractual Relations in Business: A Preliminary Study. *Americal Sociological Review*, *28*(1), 55–67.
Macneil, I. R. (1978). Contracts: Adjustment of Long-Term Economic Relations under Classical, Neoclassical, and Relational Contract Law. *Northwestern University Law Review*, *72*(6), 854–905.
Macneil, I. R. (1985). Relational Contract: What We Do and Do Not Know. *Wisconsin Law Review*, *1985*(3), 483–526.
Macrinici, D., Cartofeanu, C., & Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, *35*(8), 2337–2354. doi:10.1016/j.tele.2018.10.004
Magazzeni, D., McBurney, P., & Nash, W. (2017). Validation and Verification of Smart Contracts: A Research Agenda. *Computer*, *50*(9), 50–57. doi:10.1109/MC.2017.3571045
Marino, B., & Juels, A. (2016). Setting Standards for Altering and Undoing Smart Contracts. In *International Symposium on Rules and Rule Markup Languages for the Semantic Web* (Vol. 9718, pp. 167–183). Springer, Cham. doi:10.1007/978-3-319-42019-6
Mark, D., Zamfir, V., & Sirer, E. G. (2016). A Call for a Temporary Moratorium on "The DAO." *Hacking Distributed [Blog de Gun Sirer]*. https://blog.bitmex.com/wp-content/uploads/2017/11/A-Call-for-a-Temporary-Moratorium-on-The-DAO.pdf
McCain, K. W. (1990). Mapping authors in intellectual space: A technical overview. *Journal of the American Society for Information Science*, *41*(6), 433–443. doi:10.1002/(SICI)1097-4571(199009)41:6<433::AID-ASI11>3.0.CO;2-Q
Mengelkamp, E., Gärttner, J., Rock, K., Kessler, S., Orsini, L., & Weinhardt, C. (2018). Designing microgrid energy markets: A case study: The Brooklyn Microgrid. *Applied Energy*, *210*, 870–880. doi:10.1016/j.apenergy.2017.06.054
Miau, S., & Yang, J. M. (2018). Bibliometrics-based evaluation of the Blockchain research trend: 2008–March 2017. *Technology Analysis and Strategic Management*, *30*(9), 1029–1045. doi:10.1080/09537325.2018.1434138
Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous distributed e-cash from bitcoin. In *Proceedings - IEEE Symposium on Security and Privacy* (pp. 397–411). IEEE. doi:10.1109/SP.2013.34
Mihaylov, M., Jurado, S., Avellana, N., Van Moffaert, K., De Abril, I. M., & Nowé, A. (2014). NRGcoin: Virtual currency for trading of renewable energy in smart grids. In *International Conference on the European Energy Market, EEM*. doi:10.1109/EEM.2014.6861213
Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. *Law, Innovation and Technology*, *9*(2), 269–300. doi:10.1080/17579961.2017.1378468
Miller, A., Xia, Y., Croman, K., Shi, E., & Song, D. (2016). The Honey Badger of BFT protocols. In *Proceedings of the ACM Conference on Computer and Communications Security* (pp. 31–42). doi:10.1145/2976749.2978399
Munsing, E., Mather, J., & Moura, S. (2017). Blockchains for decentralized optimization of energy resources in microgrid networks. In *1st Annual IEEE Conference on Control Technology and Applications* (pp. 2164–2171). doi:10.1109/CCTA.2017.8062773
Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
Nayak, K., Kumar, S., Miller, A., & Shi, E. (2016). Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In *Proceedings - 2016 IEEE European Symposium on Security and Privacy* (pp. 305–320). doi:10.1109/EuroSP.2016.32
Nikolić, I., Kolluri, A., Sergey, I., Saxena, P., & Hobor, A. (2018). Finding the greedy, prodigal, and suicidal contracts at scale. *ACM International Conference Proceeding Series*, 653–663.

doi:10.1145/3274694.3274743
Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal*, *5*(2), 1184–1195. doi:10.1109/JIOT.2018.2812239
Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, *34*(3), 355–364. doi:10.1016/j.giq.2017.09.007
OpenZeppelin. (2020). Upgrading Smart Contracts. https://docs.openzeppelin.com/learn/upgrading-smart-contracts. Accessed 12 August 2020
Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2017). Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT. In *Europe and MENA Cooperation Advances in Information and Communication Technologies* (pp. 523–533). Springer, Cham. http://link.springer.com/10.1007/978-3-319-46568-5
Pease, M., Shostak, R., & Lamport, L. (1980). Reaching Agreement in the Presence of Faults. *Journal of the ACM (JACM)*, *27*(2), 228–234. doi:10.1145/322186.322188
Peck, M. E. (2017). Blockchain World - Do You Need a Blockchain? *IEEE Spectrum*, *54*(10), 38–60. doi:10.1109/MSPEC.2017.8048838
Peck, M. E., & Wagman, D. (2017). Energy Trading for Fun and Profit. *IEEE Spectrum*, *54*(10), 54–55. doi:10.1109/MSPEC.2017.8048841
Persson, O., Danell, R., & Schneider, J. W. (2009). How to use Bibexcel for various types of bibliometric analysis. *Celebrating scholarly communication studies: A Festschrift for Olle Persson at his 60th Birthday*, 9–24. http://lup.lub.lu.se/record/1458990/file/1458992.pdf
Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. *New Economic Windows*, 239–278. doi:10.1007/978-3-319-42448-4_13
Pinna, A., Ibba, S., Baralla, G., Tonelli, R., & Marchesi, M. (2019). A Massive Analysis of Ethereum Smart Contracts Empirical Study and Code Metrics. *IEEE Access*, *7*, 78194–78213. doi:10.1109/ACCESS.2019.2921936
Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain Mutability: Challenges and Proposed Solutions. *IEEE Transactions on Emerging Topics in Computing*, 1–13. doi:10.1109/TETC.2019.2949510
Poon, J., & Buterin, V. (2017). *Plasma: Scalable Autonomous Smart Contracts Scalable Multi-Party Computation*.
Pop, C., Cioara, T., Antal, M., Anghel, I., Salomie, I., & Bertoncini, M. (2018). Blockchain based decentralized management of demand response programs in smart energy grids. *Sensors*, *18*(1). doi:10.3390/s18010162
Raskin, M. (2017). The Law and Legality of Smart Contracts. *Georgia Law Technology Review*, *1*(305).
Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. *Security and Privacy in Social Networks*, 197–223. doi:10.1007/978-1-4614-4139-7_10
Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*(2018), 173–190. doi:10.1016/j.future.2018.05.046
Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework: What We (Don't) Know, Where We Go from Here, and How We Will Get There. *Business and Information Systems Engineering*, *59*(6), 385–409. doi:10.1007/s12599-017-0506-0
Roehrs, A., da Costa, C. A., & da Rosa Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics*, *71*, 70–81. doi:10.1016/j.jbi.2017.05.012
Rotolo, D., Hicks, D., & Martin, B. R. (2015). What is an emerging technology ? *Research Policy*, *44*(10), 1827–1843. doi:10.1016/j.respol.2015.06.006
Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117–2135. doi:10.1080/00207543.2018.1533261
Salmerón-Manzano, E., & Manzano-Agugliaro, F. (2019). The role of smart contracts in sustainability: Worldwide research trends. *Sustainability*, *11*(11). doi:10.3390/su11113049
Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. *Information and Communications Technology Law*, *26*(2), 116–134. doi:10.1080/13600834.2017.1301036
Schär, F. (2020). Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets. doi:10.13140/RG.2.2.18469.65764
Scholz, L. (2016). Algorithmic Contracts. *Stanford Technology Law Review*, *20*, 128.
Seijas, P. L., Thompson, S., & McAdams, D. (2017). Scripting smart contracts for distributed ledger technology. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10323 LNCS*, 631–632. doi:10.1007/978-3-319-70278-0
Seres, I. A. (2020). On Blockchain Metatransactions. https://arxiv.org/pdf/2004.08094
Shae, Z., & Tsai, J. J. P. (2017). On the Design of a Blockchain Platform for Clinical Trial and Precision

Medicine. *Proceedings - International Conference on Distributed Computing Systems*, 1972–1980. doi:10.1109/ICDCS.2017.61
Sharma, P. K., Singh, S., Jeong, Y. S., & Park, J. H. (2017). DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks. *IEEE Communications Magazine*, *55*(9), 78–85. doi:10.1109/MCOM.2017.1700041
Shermin, V. (2017). Disrupting governance with blockchains and smart contracts. *Strategic Change*, *26*(5), 499–509. doi:10.1002/jsc.2150
Sikorski, J. J., Haughton, J., & Kraft, M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy*, *195*, 234–246. doi:10.1016/j.apenergy.2017.03.039
Singh, A., Parizi, R. M., Zhang, Q., Choo, K.-K. R., & Dehghantanha, A. (2019). Blockchain Smart Contracts Formalization: Approaches and Challenges to Address Vulnerabilities Computers & Security. *Computers & Security*, *88*. doi:10.1016/j.cose.2019.101654
Sklaroff, J. M. (2017). Smart Contracts and the Cost of Inflexibility. *University of Pennsylvania Law Review*, *166*(1).
Small, H. G. (1973). Co-citation in the scientific literature: A new measure of the relationship between two documents. *Journal of the American Society for Information Science*, *24*, 265–269. doi:10.1002/asi.4630240406
Small, H. G. (1977). A Co-Citation Model of a Scientific Specialty: A Longitudinal Study of Collagen Research. *Social Studies of Science*, *7*(2), 139–166. doi:10.1177/030631277700700202
Sompolinsky, Y., & Zohar, A. (2013). Accelerating Bitcoin's Transaction Processing - Fast Money Grows on Trees, Not Chains. *IACR Cryptology ePrint Archive*, *881*.
Stanciu, A. (2017). Blockchain Based Distributed Control System for Edge Computing. In *Proceedings - 2017 21st International Conference on Control Systems and Computer* (pp. 667–671). doi:10.1109/CSCS.2017.102
Stokkink, Q., & Pouwelse, J. (2018). Deployment of a Blockchain-Based Self-Sovereign Identity. In *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology* (pp. 1336–1342). doi:10.1109/Cybermatics_2018.2018.00230
Strehle, E., & Ante, L. (2020). *Exclusive Mining of Blockchain Transactions*. doi:10.13140/RG.2.2.22494.05442
Subramanian, H. (2018). Decentralized Blockchain-Based Electronic Marketplaces. *Communications of the ACM*, *61*(1), 78–84. doi:10.1145/3158333
Sullivan, C., & Burger, E. (2017). E-residency and blockchain. *Computer Law and Security Review*, *33*(4), 470–481. doi:10.1016/j.clsr.2017.03.016
Sun, J., Yan, J., & Zhang, K. Z. K. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, *2*(1). doi:10.1186/s40854-016-0040-y
Surden, H. (2012). Computable Contracts. *U.C. Davis Law Review*.
Szabo, N. (1994). Smart Contracts. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. Accessed 14 February 2020
Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). doi:10.5210/fm.v2i9.548
Tai, X., Sun, H., & Guo, Q. (2016). Electricity Transactions and Congestion Management Based on Blockchain in Energy Internet. *Power Syst. Technol*, 3630–3638.
Teutsch, J., & Reitwießner, C. (2017). A scalable verification solution for blockchains. https://arxiv.org/pdf/1908.04756
Tikhomirov, S., Voskresenskaya, E., Ivanitskiy, I., Takhaviev, R., Marchenko, E., & Alexandrov, Y. (2018). SmartCheck: Static analysis of ethereum smart contracts. In *Proceedings - International Conference on Software Engineering* (pp. 9–16). doi:10.1145/3194113.3194115
Tsankov, P., Dan, A., Drachsler-Cohen, D., Gervais, A., Bünzli, F., & Vechev, M. (2018). Securify: Practical security analysis of smart contracts. In *Proceedings of the ACM Conference on Computer and Communications Security* (pp. 67–82). doi:10.1145/3243734.3243780
Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys and Tutorials*, *18*(3), 2084–2123. doi:10.1109/COMST.2016.2535718
Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access*, *6*, 5112–5127. doi:10.1109/ACCESS.2018.2789929
Udokwu, C., Kormiltsyn, A., Thangalimodzi, K., & Norta, A. (2018). The State of the Art for Blockchain-Enabled Smart-Contract Applications in the Organization. In *2018 Ivannikov Ispras Open Conference (ISPRAS)* (pp. 137–144). doi:10.1109/ISPRAS.2018.00029
van Eck, N. J., & Waltman, L. (2007). *VOS: A New Method for Visualizing Similarities between Objects*. Springer, Berlin, Heidelberg.

van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, *84*(2), 523–538. doi:10.1007/s11192-009-0146-3
Wang, H., Zheng, Z., Xie, S., Dai, H. N., & Chen, X. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, *14*(4), 352. doi:10.1504/ijwgs.2018.10016848
Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., & Mendling, J. (2016). Untrusted business process monitoring and execution using blockchain. In *International Conference on Business Process Management* (pp. 329–347).
Wen, Z. A., & Miller, A. (2016). Scanning Live Ethereum Contracts for the "Unchecked-Send" Bug. *Hacking Distributed*.
Werbach, K. D. (2016). Trust, But Verify: Why the Blockchain Needs the Law. *Berkeley Technology Law Journal*, *487*(33). doi:10.2139/ssrn.2844409
Werbach, K. D., & Cornell, N. (2017). Contracts Ex Machina. *Duke Law Journal*, *67*(2), 313–382.
Willett, J., Hidskes, M., Jonston, D., Gross, R., & Schneider, M. (2015). Omni Protocol Specification. https://github.com/OmniLayer/spec. Accessed 18 February 2020
Wohrer, M., & Zdun, U. (2018). Smart contracts: Security patterns in the ethereum ecosystem and solidity. In *2018 IEEE 1st International Workshop on Blockchain Oriented Software Engineering, IWBOSE 2018 - Proceedings* (pp. 2–8). doi:10.1109/IWBOSE.2018.8327565
Wood, G. (2014). *Ethereum: a secure decentralised generalised transaction ledger*. https://ethereum.github.io/yellowpaper/paper.pdf
Wörfel, P. (2019). Unravelling the intellectual discourse of implicit consumer cognition : A bibliometric review. *Journal of Retailing and Consumer Services*, (September), 101960. doi:10.1016/j.jretconser.2019.101960
Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain. *IEEE Access*, *5*(August), 14757–14767. doi:10.1109/ACCESS.2017.2730843
Yu, D., & Sheng, L. (2020). Knowledge diffusion paths of blockchain domain: the main path analysis. *Scientometrics*. doi:10.1007/s11192-020-03650-y
Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, *40*(10), 218.
Zhang, J., Xue, N., & Huang, X. (2016). A Secure System for Pervasive Social Network-Based Healthcare. *IEEE Access*, *4*(c), 9239–9250. doi:10.1109/ACCESS.2016.2645904
Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Computational and Structural Biotechnology Journal*, *16*, 267–278. doi:10.1016/j.csbj.2018.07.004
Zhang, Y., & Wen, J. (2017). The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications*, *10*(4), 983–994. doi:10.1007/s12083-016-0456-1
Zupic, I., & Čater, T. (2015). Bibliometric Methods in Management and Organization. *Organizational Research Methods*, *18*(3), 429–472. doi:10.1177/1094428114562629
Zuschke, N. (2019). An analysis of process-tracing research on consumer decision-making. *Journal of Business Research*, 1–16. doi:10.1016/j.jbusres.2019.01.028
Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *Proceedings – 2015 IEEE Security and Privacy Workshops, SPW 2015* (pp. 180–184). doi:10.1109/SPW.2015.27

Declarations

Availability of data and materials

The datasets used and/or analyzed during the current study are available from the corresponding author on request.

Conflicts of interest

Not applicable.

Funding

Not applicable.

Acknowledgements

Not applicable.

About the Blockchain Research Lab

The Blockchain Research Lab promotes independent science and research on blockchain technologies and the publication of the results in the form of scientific papers and contributions to conferences and other media. The BRL is a non-profit organization aiming, on the one hand, to further the general understanding of the blockchain technology and, on the other hand, to analyze the resulting challenges and opportunities as well as their socio-economic consequences.

www.blockchainresearchlab.org