

# WIP: The Design Principle of blockchain: An Initiative for the SoK of SoKs

LUYAO SUNSHINE ZHANG\*, Primitives Lane, Metaverse

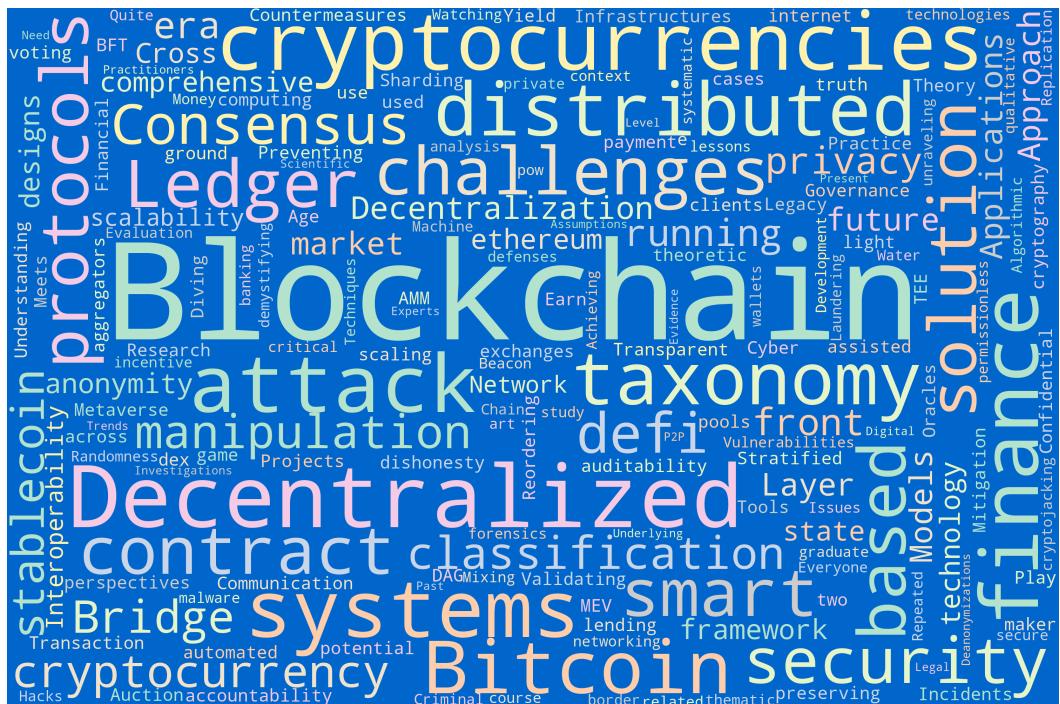


Fig. 1. The Word Cloud of blockchain Related SoK Titles

The Master said, "**virtue** is not left to stand alone. He who practices it will have neighbors."  
—Confucius, *Analects*

"You must contrive for your future rulers another and a better life than that of a ruler, and then you may have a well-ordered State; for only in the State which offers this, will they rule who are truly rich, not in silver and gold, but in **virtue** and wisdom, which are the true blessings of life."  
—Plato, *Republic*

Blockchain, also coined as decentralized AI, has the potential to empower AI to be more trustworthy by creating a decentralized trust of privacy, security, and audibility. However, systematic studies on the design principle of blockchain as a trust engine for an integrated society of cyber-physical-social-system (CPSS) are still absent. In this article, we provide an initiative for seeking the design principle of blockchain for a better digital world. Using a hybrid method of qualitative and quantitative studies, we examine the past origin, the current development, and the future directions of blockchain design principles. We have three findings. First, the answer to whether blockchain lives up to its original design principle as a distributed database is controversial. Second, the current development of the blockchain community reveals a taxonomy of 7 categories, namely, privacy and

\*Primitives Lane is a nonprofit research group focused on blockchain and other frontier technologies. We are dedicated to solving the most fundamental public issues in frontier fields, helping researchers grow steadily, and creating a friendly and supportive space for builders.

security, scalability, decentralization, applicability, governance and regulation, system design, and cross-chain interoperability. Both research and practice are more centered around the first category of privacy and security and the fourth category of applicability. Future scholars, practitioners, and policy-makers have vast opportunities in other, much less exploited facets and the synthesis at the interface of multiple aspects. Finally, in counter-examples, we conclude that a synthetic solution that crosses discipline boundaries is necessary to close the gaps between the current design of blockchain and the design principle of a trust engine for a truly intelligent world.

**Acknowledgments:** I am deeply indebted to all the pioneers in Web3 for their inspirations, especially for my mentors, coauthors, and students who jointly contribute to the interdisciplinary conversation around the applications of blockchain. *The name list is to be added.*

**CCS Concepts:** • **Applied computing → Economics;** • **Security and privacy → Distributed systems security;** • **Human-centered computing → Collaborative and social computing systems and tools.**

**Additional Key Words and Phrases:** blockchain, AI ethics, philosophy, economics, computer science

## 1 INTRODUCTION

The past one hundred years have witnessed incredible advancements in artificial intelligence (AI) [Littman et al., 2022, Stone et al., 2022]. These advancements are integrating cyberspace (CS), physical space (PS), and social space(SS), into the cyber-physical-social-system(CPSS), which extraordinarily expands the territories of human civilizations [Wang, 2010] extraordinarily. However, AI *per se* is not enough to establish trust in the CPSS [Jacovi et al., 2021, Jan et al., 2020], which is the cornerstone of prosperity in every civilized society. Blockchain, also coined as *decentralized AI*, has the potential to empower AI to be more trustworthy by creating a decentralized trust of privacy, security, and audit-ability [Adel et al., 2022, Harris and Waggoner, 2019, Hussain and Al-Turjman, 2021]. However, systematic studies on the design principle of blockchain as a trust engine for the CPSS are still absent. If we could decipher the philosophy of blockchain, we would build the infrastructure of a better digital world. In this article, we provide an initiative for seeking the design principle of blockchain for the betterment of human civilization. Unlike the existing systemization of knowledge (SoK) on blockchain that focuses on a specific discipline purpose or topic of interest, ours aims at opening an intellectual conversation beyond boundaries for the ultimate goal of a better digital world, namely, the SoK of SoKs. Specifically, we hope to initiate the answers to three questions for the past, the current, and the future of blockchain design.

- (1) *The past:* Does blockchain live up to its original design principles as a distributed database?
- (2) *The current:* How do the current blockchain literature, industry practices, and global standards address and develop the design principle of blockchain?
- (3) *The future:* What are the gaps between the current design of blockchain and the design principle of a trust engine for a truly intelligent world?

In Section 2, we examine the performance of blockchain according to its original design principle as a distributed database. We present the controversial answers in a dialog style of debate. In Section 3, we analyze the current research and practice of blockchain principles by investigating the current SoKs of emerging blockchain literature, the white papers that provide technique cornerstones for blockchain technology in the real world, and the discussions on global standards for blockchain. We identify a taxonomy of blockchain literature into the seven categories of privacy and security, scalability, decentralization, applicability, governance and regulation, system design, and cross-chain interoperability. Integrating the AI of natural language processing (NLP) [Bird et al., 2009] methods, we find that the current blockchain design principles, in both research and practice, are more centered around the first category of privacy and security and the fourth category of applicability. Future scholars, practitioners, and policy-makers have vast opportunities in the other much less exploited categories and the synthesis at the interface of multiple categories. In

The screenshot shows a conversation interface. Sunshine asks, "What is the design principle of blockchain?" Chat GPT-3 responds: "A blockchain is a decentralized, distributed database that is used to maintain a continuously growing list of records, called blocks. Each block contains a timestamp and a link to the previous block." Below this, Sunshine asks, "The design principles of blockchain technology include:" Chat GPT-3 lists five principles: 1. Decentralization, 2. Immutability, 3. Transparency, 4. Security, and 5. Efficiency.

What is the design principle of blockchain?

A blockchain is a decentralized, distributed database that is used to maintain a continuously growing list of records, called blocks. Each block contains a timestamp and a link to the previous block.

The design principles of blockchain technology include:

1. Decentralization: A blockchain is decentralized, meaning it is not controlled by any single entity or organization. Instead, it is maintained by a network of users who validate and record transactions on the blockchain.
2. Immutability: Once data has been recorded on a blockchain, it cannot be altered. This ensures the integrity and security of the data on the blockchain.
3. Transparency: Transactions on a blockchain are visible to all participants in the network. This transparency helps to build trust among users and enables the blockchain to function as a transparent and secure record-keeping system.
4. Security: Blockchain technology uses advanced cryptographic techniques to secure the data on the network. Each block contains a cryptographic hash of the previous block, which helps to ensure the integrity and security of the data on the blockchain.
5. Efficiency: By using a decentralized network and eliminating the need for intermediaries, blockchain technology can help to streamline and improve the efficiency of many different types of transactions.

Fig. 2. A Conversation Between Sunshine and Chat GPT-3 on 2022/12/30

Section 4, we envision the future of blockchain technology by pointing out the gaps between the current design of blockchain and the design principle of a trust engine for a truly intelligent world. By providing counterexamples, we question the possibility of developing a plausible solution of singularity to the gaps without crossing the current boundaries of domain expertise.

Sages in both the West and East have been craving an ideal society. In the *Book of Rites*, one of the Confucian (551–479 B.C.E.) classics [Csikszentmihalyi, 2020], the *Great Unity* is a Chinese vision of an ideal world in which men of virtue and ability rule. In ancient Greece, Plato [Kraut, 2022] (429–347 B.C.E.) envisioned an ideal city-state ruled by a philosopher-king of justice in the *Republic*, a Socratic dialog. By such a coincidence, both Confucius and Plato place the foundation of an ideal society on cultivating or selecting the men of virtue to be the administrators whom people can trust. Nevertheless, the existence of a benevolent ruler might not be guaranteed. In contrast, blockchain enables a new way of trust creation empowered by computer intelligence beyond human ethics. However, the current blockchain technology is evidently not a panacea for doubts about human trust. Then, why "throw the baby out with the bathwater?" Existing mechanisms for cultivating human trust have created economic prosperity and human civilizations for thousands of years. How then can we integrate blockchain technology into the existing governance, economics, and ethics to create an ideal society in the new era of CPSS? We initiate an open dialog of synthetic solutions.

## 2 THE PAST

What was blockchain originally designed for? How does blockchain live up to the design principle of its original purpose? [Sherman et al. \[2019\]](#) introduce the origin of blockchain for establishing a distributed database trusted by mutually suspicious groups. [Haber and Stornetta \[1990\]](#), [Narayanan et al. \[2016\]](#), and [Bayer et al. \[1993\]](#) further elaborate on the follow-up development of blockchain technology for a series of desired properties such as decentralization, immutability, transparency, security, and efficiency. Figure 2 shows the answer returned by the Generative Pre-trained Transformer (ChatGPT), <https://openai.com/blog/chatgpt/>, a chatbot launched by OpenAI in November 2022, to the question of "what is the design principle of blockchain?" The answer accurately matches elaborations provided in earlier blockchain literature. We now examine the performance of blockchain on each principle in a dialog style of debate in the spirit of Confucius's *the Analects* [[Ames and Rosemont Jr, 2010](#)] and Plato's *the Republic* [[Plato, 2005](#)]. We find the answer to be controversial. Moreover, the desired principles might either conflict with each other or lead to other undesired consequences.

### Question 1: Does blockchain live up to its promise of decentralization?

2.0.1 *Pros.* Yes, blockchain is decentralized. Compared with centralized ledgers, blockchain is not subject to the single point failure of a centralized entity [[Puthal et al., 2018](#)]. Blockchain records and validates data by a consensus protocol involving decentralized entities, which has the fault tolerance of minorities [[Zhang and Tian, 2022](#)].

2.0.2 *Cons.* No, blockchain is not decentralized. [Sai et al. \[2021\]](#) provide a taxonomy of blockchain centralization in 13 aspects. For example, [Sai et al. \[2021\]](#) show that the top four mining pools in Ethereum (Bitcoin) consist of 63.04% (50.36%) of the hashing power, which is enough to conduct a successful malicious attack. Moreover, [Zhang et al. \[2022\]](#) and the references therein show that the usage of blockchain at the application layer has the trend of converging to centralization.

### Question 2: Does blockchain live up to its promise of immutability?

2.0.3 *Pros.* Yes, blockchain is immutable. [Narayanan et al. \[2016\]](#) elaborate on the difficulty of manipulating recorded data due to the chain structure of Merkle trees.

2.0.4 *Cons.* No, blockchain is mutable. [Hofmann et al. \[2017\]](#) show that the immutability of blockchain can be breached by various attacks. [Politou et al. \[2019\]](#) even address the conflicts between blockchain immutability and the new European data protection regulation on the right to be forgotten (RtBF), according to which individuals have the right to delete their personal data under certain conditions.

### Question 3: Does blockchain live up to its promise of transparency?

2.0.5 *Pros.* Yes, blockchain is transparent. [Monrat et al., 2019](#) explains that all the transactions on blockchain are recorded and auditable by each replica node in the network.

2.0.6 *Cons.* No, blockchain is not transparent. [Sai et al. \[2021\]](#) demonstrates the centralization in node operation, which is required to audit the blockchain data due to technique barriers. [Feng et al. \[2019\]](#) even point out the transparency of blockchain as a negative feature and a threat to user privacy.

### Question 4: Does blockchain live up to its promise of security?

2.0.7 *Pros.* Yes, blockchain is secure. [Zhang et al. \[2019\]](#) address the blockchain security property of consistency and integrity achieved by the main techniques of consensus algorithms and hash-chained storage.

2.0.8 *Cons.* No, blockchain is not secure. [Lin and Liao \[2017\]](#) evidence a long list of real attacks on blockchain together with an analysis of potential security issues. [Budish \[2022\]](#) even establishes a conclusion that the mechanism supporting blockchain security is either vulnerable or not worth the economic cost.

### Question 5: Does blockchain live up to its promise of efficiency?

2.0.9 *Pros.* Yes, blockchain is efficient. [Wang et al. \[2019a\]](#) analyze how blockchain improves efficiency in human interactions by automating and streamlining business operations using smart contracts.

2.0.10 *Cons.* No, blockchain is not efficient. Current major blockchains can only sustain tens of transactions per second (TPS), which is not comparable to the centralized platforms, which have a throughput of thousands of TPS [[Chauhan et al., 2018](#)].

## 3 THE CURRENT

How do the current blockchain literature, industry practices, and global standards address and develop the design principle of blockchain? We collect all the systemization of knowledge (SoK) papers related to facets of blockchain or surveys and review articles that satisfy the defining features of SoKs. We refer the readers to the JSys website, [https://www.jsys.org/type\\_SoK/](https://www.jsys.org/type_SoK/), for background information on SoKs and the Oakland Conference GitHub site, <https://oaklandsok.github.io/>, for the histories of SoKs in computer security and privacy literature. We present a taxonomy of the collected SoKs in Table 1 and Table 2, broken into seven categories based on the topic of research questions:

- *Category 1: Privacy and Security.* We include literature that answers questions about private information protection and attacks on blockchain systems. We refer the readers to [DeCew \[2018\]](#) for a philosophical symposium on *privacy* and [Bishop \[2003\]](#) for the computer science insights on *security*.
- *Category 2: Scalability.* We include literature that answers questions related to the scalable deployment of blockchain, usually measured in throughput and quality of service. We refer the readers to [Jogalekar and Woodside \[2000\]](#) for the definition and measurement of scalability in the distributed system literature.
- *Category 3: Decentralization.* We include the literature that answers questions related to the designed and realized decentralization of blockchain. We refer the readers to [Zhang et al. \[2022\]](#) for an interdisciplinary synthesis of a taxonomy of blockchain decentralization.
- *Category 4: Applicability.* We include literature that answers questions related to the application of blockchain to solve social and economic issues in various of human interactions. Table 2 shows that the major applications are in financial services [[Chen and Bellavitis, 2020](#), [Harvey et al., 2021](#), [Zetzsche et al., 2020](#)].
- *Category 5: Governance and Regulation.* We include literature that answers questions related to utilizing blockchain as a new way of governance, the process of interaction of an organized society, and its interactions with existing governance solutions, including corporate, government, and nongovernment organizations (NGOs). We refer the readers to [\[Bevir, 2012\]](#) for a review of existing governance solutions, including various forms of social coordination and patterns of rules.

- *Category 6: System design.* We include literature that answers questions related to designing blockchain as an advancement of existing computer systems. We refer the readers to Saltzer and Kaashoek [2009] for the design principles of computer systems.
- *Category 7: Cross-chain and Interoperability.* We include literature that answers questions related to communication, cooperation, and integration among blockchain systems, other computer systems, and human societies. We refer the readers to Wegner [1996] and Leal et al. [2019] for the importance and assessment of interoperability among information systems.

Table 6 lists the top 28 blockchain projects, excluding applications on the blockchain system and cross-chain solutions ranked by the market value of their native currency retrieved from Coinmarketcap, <https://coinmarketcap.com/>, on Dec. 27, 2022. We further collect the white papers that provide the technical foundations for the 28 projects. We then conduct a text analysis applying natural language processing (NLP) methods to produce a word cloud and bigram networks of the titles and abstracts of the SoKs and white papers. The results are presented in Table 4, Table 5, Table 7, Table 8, Table 9, Figure 1, Figure 8, Figure 3, Figure 7, Figure 6, Figure 4, Figure 5, and Figure 9, Figure 8. The word cloud distinguishes the word frequency in these documents through font size, and the bigram represents the coappearance of two words in sequential order ranking by counts in the tables and in the network figures. We also further research the emerging documents of blockchain standard development and papers discussing blockchain standards by working groups and institutions globally.

**Data and Code Availability:** We open source the data and code for replication and future research on the GitHub: <https://github.com/sunshineluyao/design-principle-blockchain>.

We find that the current blockchain design principles, in both research and practice, are more centered around the first category of privacy and security and the fourth category of applicability. Future scholars, practitioners, and policy-makers have vast opportunities in the other much less exploited categories and the synthesis at the interface of multiple categories.

## 4 THE FUTURE

What are the gaps between the current design of blockchain and the design principle of a trust engine for a truly intelligent world? In this section, we do not intend to provide a comprehensive answer. Instead, we question the possibility of developing a plausible solution of singularity to the gaps without crossing the current boundaries of domain expertise by providing counterexamples.

### Case Study 1:

#### How can we elaborate on the design principle of privacy and security for a better society?

The scientific community of distributed systems and cryptography has made great milestones in blockchain development by achieving the anonymity of private information and the audibility of public transactions. However, privacy and security are the means but not necessarily the ends for a better society of human prosperity. Through history, critiques [DeCew, 2018] have addressed privacy as the source of criminal activities, economic inefficiency, and the abuse of minorities. Cong et al. [2022b] identify that wash trading accounts for approximately 70% of the total cryptocurrency trading volumes. Cong et al. [2022a] further provide a taxonomy of crimes enabled by the anonymity feature on blockchain. Abundant literature in behavioral science [Dawson, 2018] establishes a connection between anonymity and abusive behavior. However, none of those negative effects on human behavior are considered in the original design principles of blockchain. How can we redesign privacy and security to cultivate human cooperation better and minimize abusive behavior? Behavior scientists have the expertise to contribute to this discussion.

### Case Study 2:

#### How can we elaborate on the design principle of decentralization for a better society?

Most top-ranked blockchain projects aim to create a permissionless system that is more inclusive, democratic, and decentralized than those that have been presented previously. However, what is required to satisfy the permission for the permissionless blockchains? You must have access to the internet, afford the computer system requirements to run a replica node, and master the engineering skills needed to participate in the network. Unfortunately, according to World in Data, <https://ourworldindata.org/internet>, in most parts of our world, less than half of the population has access to the internet, let alone the higher requirements of computer system and engineering skills. Moreover, Ao et al. [2022] and the references therein evidence most of the crypto transactions are executed via centralized exchanges but not in the decentralized form of on-chain peer-to-peer transactions. Cong et al. [2022c] further address the inclusion issues of the current Web3 economy due to technology barriers and lack of inclusion consideration in the original design principle of blockchain. The famous Irish playwright Bernard Shaw said, "Revolutions have never lightened the burden of tyranny. They have only shifted it to another shoulder" [Tiliouine and Estes, 2016]. To direct blockchain development to avoid the fate stated by Bernard Shaw and serve a more decentralized society—of the people, by the people, and for the people—anthropologists, social scientists, and economists are able to contribute to designing a society of democracy, diversity, and inclusion.

### Case Study 3:

#### How can we elaborate on the design principle of efficiency for a better society?

The current solutions for efficiency or scalability on blockchain focus on improving transaction throughput and automating business processes. However, the pursuit of efficiency in an isolated system of short-sighted consideration might lead to inefficiency for the society as a whole with regard to long-term sustainability. For example, the current scalability solutions in general consider the blockchain system only in isolation but ignore the negative externality of the high-energy consumption design to the outside world [Truby, 2018]. Moreover, Grimmelmann [2019] notes that although smart contracts automate business processes, the current design ignores the ambiguity in the semantics of the programming language. Thus, a temporary convenience of the smart contract operation might lead to costly disputes in unforeseen scenarios when developers and users disagree. Policy-makers and lawyers can contribute to reconsidering the blockchain design to improve the efficiency of negotiations among different stakeholders and our society as a whole.

### A Call for Collaboration

Kranzberg [1986] stated the following in his 1985 address as president of the Society for the History of Technology (SHOT): "Technology is neither good nor bad, nor is it neutral." blockchain is a powerful technology that brings about many new possibilities. How can we redesign blockchain for a truly intelligent world? To address this questions, we call for a joint endeavor from all disciplines.

### REFERENCES

- Yousif Abuidris, Rajesh Kumar, and Wang Wenyong. 2019. A survey of blockchain based on e-voting systems. In *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications*. 99–104.
- Kareem Adel, Ahmed Elhakeem, and Mohamed Marzouk. 2022. Decentralizing construction AI applications using blockchain technology. *Expert Systems with Applications* 194 (2022), 116548.
- Anwaar Ali, Mohamed Rahouti, Siddique Latif, Salil Kanhere, Jatinder Singh, Umar Janjua, Adnan Noor Mian, Junaid Qadir, Jon Crowcroft, et al. 2019. Blockchain and the future of the internet: A comprehensive review. *arXiv preprint arXiv:1904.00733* (2019).
- Ghada Almashaqbeh and Ravital Solomon. 2022. SoK: privacy-preserving computing in the blockchain era. In *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*. IEEE, 124–139.

- Nasser Alsalam and Bingsheng Zhang. 2019. SoK: A systematic study of anonymity in cryptocurrencies. In *2019 IEEE Conference on Dependable and Secure Computing (DSC)*. IEEE, 1–9.
- Roger T Ames and Henry Rosemont Jr. 2010. *The analects of Confucius: A philosophical translation*. Ballantine books.
- Ralph Ankele, Kai Nahrgang, Branka Stojanovic, and Atta Badii. 2020. SoK: Cyber-Attack Taxonomy of Distributed Ledger-and Legacy Systems-based Financial Infrastructures. *Cryptology ePrint Archive* (2020).
- Ziqiao Ao, Gergely Horvath, and Luyao Zhang. 2022. Are decentralized finance really decentralized? A social network analysis of the Aave protocol on the Ethereum blockchain. *arXiv preprint arXiv:2206.08401* (2022).
- Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. 2017. A survey of attacks on ethereum smart contracts (sok). In *International conference on principles of security and trust*. Springer, 164–186.
- Sarah Azouvi and Alexander Hicks. 2019. Sok: Tools for game theoretic models of security for cryptocurrencies. *arXiv preprint arXiv:1905.08595* (2019).
- Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch Lafuente. 2021. SoK: lending pools in decentralized finance. In *International Conference on Financial Cryptography and Data Security*. Springer, 553–578.
- Carsten Baum, James Hsin-yu Chiang, Bernardo David, Tore Kasper Frederiksen, and Lorenzo Gentile. 2021. Sok: Mitigation of front-running in decentralized finance. *Cryptology ePrint Archive* (2021).
- Dave Bayer, Stuart Haber, and W Scott Stornetta. 1993. Improving the efficiency and reliability of digital time-stamping. In *Sequences II*. Springer, 329–334.
- Rafael Belchior, Luke Riley, Thomas Hardjono, André Vasconcelos, and Miguel Correia. 2022. Do You Need a Distributed Ledger Technology Interoperability Solution? *Distrib. Ledger Technol.* (sep 2022). <https://doi.org/10.1145/3564532> Just Accepted.
- Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. 2021. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. *ACM Comput. Surv.* 54, 8, Article 168 (oct 2021), 41 pages. <https://doi.org/10.1145/3471140>
- Badr Bellaj, Aafaf Ouaddah, Emmanuel Bertin, Noel Crespi, and Abdellatif Mezrioui. 2022. SOK: a comprehensive survey on distributed ledger technologies. In *ICBC 2022: IEEE International Conference on Blockchain and Cryptocurrency*. IEEE, 1–16.
- Mark Bevir. 2012. *Governance: A very short introduction*. OUP Oxford.
- Steven Bird, Ewan Klein, and Edward Loper. 2009. *Natural language processing with Python: analyzing text with the natural language toolkit*. " O'Reilly Media, Inc.".
- Matt Bishop. 2003. What is computer security? *IEEE Security & Privacy* 1, 1 (2003), 67–69.
- Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A Kroll, and Edward W Felten. 2015. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. In *2015 IEEE symposium on security and privacy*. IEEE, 104–121.
- Silvia Bonomi, Antonella Del Pozzo, Álvaro García-Pérez, and Sara Tucci-Piergiovanni. 2021. SoK: Achieving State Machine Replication in Blockchains based on Repeated Consensus. *arXiv preprint arXiv:2105.13732* (2021).
- Eric B Budish. 2022. The economic limits of Bitcoin and anonymous, decentralized trust on the blockchain. *University of Chicago, Becker Friedman Institute for Economics Working Paper* 83 (2022).
- Fran Casino, Claudia Pina, Pablo López-Aguilar, Edgar Batista, Agustí Solanas, and Constantinos Patsakis. 2022. SoK: Cross-border Criminal Investigations and Digital Evidence. *arXiv preprint arXiv:2205.12911* (2022).
- Panagiotis Chatzigiannis, Foteini Baldimtsi, and Konstantinos Chalkias. 2021. SoK: auditability and accountability in distributed payment systems. In *International Conference on Applied Cryptography and Network Security*. Springer, 311–337.
- Panagiotis Chatzigiannis, Foteini Baldimtsi, and Konstantinos Chalkias. 2022. Sok: Blockchain light clients. In *International Conference on Financial Cryptography and Data Security*. Springer, 615–641.
- Anamika Chauhan, Om Prakash Malviya, Madhav Verma, and Tejinder Singh Mor. 2018. Blockchain and scalability. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. IEEE, 122–128.
- Huashan Chen, Marcus Pendleton, Laurent Njilla, and Shouhuai Xu. 2020. A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Computing Surveys (CSUR)* 53, 3 (2020), 1–43.
- Yan Chen and Cristiano Bellavitis. 2020. Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights* 13 (2020), e00151.
- Jeremy Clark, Didem Demirag, and Mahsa Moosavi. 2019. SoK: demystifying stablecoins. *Communications of the ACM, Forthcoming* (2019).
- Lin William Cong, Campbell R Harvey, Daniel Rabetti, and Zong-Yu Wu. 2022a. An anatomy of crypto-enabled cybercrimes. Available at SSRN 4188661 (2022).
- Lin William Cong, Xi Li, Ke Tang, and Yang Yang. 2022b. *Crypto wash trading*. Technical Report. National Bureau of Economic Research.
- Lin William Cong, Ke Tang, Yanxin Wang, and Xi Zhao. 2022c. Inclusion and democratization through web3 and defi? initial evidence from the ethereum ecosystem. *Initial Evidence from the Ethereum Ecosystem (July 29, 2022)* (2022).
- Simon Coussaert, Jiahua Xu, and Toshiko Matsui. 2022. Sok: Yield aggregators in defi. In *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 1–14.

- Mark Csikszentmihalyi. 2020. Confucius. In *The Stanford Encyclopedia of Philosophy* (Summer 2020 ed.), Edward N. Zalta (Ed.). Metaphysics Research Lab, Stanford University.
- Thomas K Dasaklis, Fran Casino, and Constantinos Patsakis. 2021. Sok: Blockchain solutions for forensics. In *Technology Development for Security Practitioners*. Springer, 21–40.
- Joe Dawson. 2018. Who is that? The study of anonymity and behavior. *APS Observer* 31 (2018).
- Judith DeCew. 2018. Privacy. In *The Stanford Encyclopedia of Philosophy* (Spring 2018 ed.), Edward N. Zalta (Ed.). Metaphysics Research Lab, Stanford University.
- Dominic Deuber, Viktoria Ronge, and Christian Rückert. 2022. SoK: Assumptions Underlying Cryptocurrency Deanonymizations. *Proceedings on Privacy Enhancing Technologies* 3 (2022), 670–691.
- Monika Di Angelo, Christian Sack, and Gernot Salzer. 2020. SoK: Development of secure smart contracts—lessons from a graduate course. In *International Conference on Financial Cryptography and Data Security*. Springer, 91–105.
- Maya Dotan, Yvonne-Anne Pignolet, Stefan Schmid, Saar Tochner, and Aviv Zohar. 2020. SoK: cryptocurrency networking context, state-of-the-art, challenges. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*. 1–13.
- Shayan Eskandari, Seyedehmahsa Moosavi, and Jeremy Clark. 2020. Sok: Transparent dishonesty: front-running attacks on blockchain. In *International Conference on Financial Cryptography and Data Security*. Springer, 170–189.
- Shayan Eskandari, Mehdi Salehi, Wanlyn Catherine Gu, and Jeremy Clark. 2021. Sok: Oracles from the ground truth to market manipulation. In *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*. 127–141.
- Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, and Neeraj Kumar. 2019. A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications* 126 (2019), 45–58.
- Federico Franzoni and Vanesa Daza. 2022. SoK: Network-Level Attacks on the Bitcoin P2P Network. *IEEE Access* 10 (2022), 94924–94962.
- Thippa Reddy Gadekallu, Thien Huynh-The, Weizheng Wang, Gokul Yenduri, Pasika Ranaweera, Quoc-Viet Pham, Daniel Benevides da Costa, and Madhusanka Liyanage. 2022. Blockchain for the Metaverse: A Review. *arXiv preprint arXiv:2203.09738* (2022).
- QingQiu Gan, Raymond Yiu Keung Lau, and Jin Hong. 2021. A critical review of blockchain applications to banking and finance: a qualitative thematic analysis approach. *Technology Analysis & Strategic Management* (2021), 1–17.
- Juan Garay and Aggelos Kiayias. 2020. Sok: A consensus taxonomy in the blockchain era. In *Cryptographers' track at the RSA conference*. Springer, 284–318.
- Simin Ghemmati, Walid Fdhila, and Edgar Weippl. 2021. SoK: How private is Bitcoin? Classification and Evaluation of Bitcoin Mixing Techniques. *Cryptography ePrint Archive* (2021).
- James Grimmelmann. 2019. All smart contracts are ambiguous. *JL & Innovation* 2 (2019), 1.
- Lewis Gudgeon, Pedro Moreno-Sánchez, Stefanie Roos, Patrick McCorry, and Arthur Gervais. 2020. Sok: Layer-two blockchain protocols. In *International Conference on Financial Cryptography and Data Security*. Springer, 201–226.
- Stuart Haber and W Scott Stornetta. 1990. How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography*. Springer, 437–455.
- Justin D Harris and Bo Waggoner. 2019. Decentralized and collaborative AI on blockchain. In *2019 IEEE international conference on blockchain (Blockchain)*. IEEE, 368–375.
- Campbell R Harvey, Ashwin Ramachandran, and Joey Santoro. 2021. *DeFi and the Future of Finance*. John Wiley & Sons.
- Lioba Heimbach and Roger Wattenhofer. 2022. SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance. *arXiv preprint arXiv:2203.11520* (2022).
- Frank Hofmann, Simone Wurster, Eyal Ron, and Moritz Böhmecke-Schwafert. 2017. The immutability concept of blockchains and benefits of early standardization. In *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*. IEEE, 1–8.
- Adedoyin A Hussain and Fadi Al-Turjman. 2021. Artificial intelligence and blockchain: A review. *Transactions on emerging telecommunications technologies* 32, 9 (2021), e4268.
- Md Rafiqul Islam, Muhammad Mahbubur Rahman, Md Mahmud, Mohammed Ataur Rahman, Muslim Har Sani Mohamad, et al. 2021. A Review on Blockchain Security Issues and Challenges. In *2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC)*. IEEE, 227–232.
- Alon Jacovi, Ana Marasović, Tim Miller, and Yoav Goldberg. 2021. Formalizing trust in artificial intelligence: Prerequisites, causes and goals of human trust in ai. In *Proceedings of the 2021 ACM conference on fairness, accountability, and transparency*. 624–635.
- Steve TK Jan, Vatche Ishakian, and Vinod Muthusamy. 2020. AI trust in business processes: the need for process-aware explanations. In *Proceedings of the AAAI Conference on Artificial Intelligence*, Vol. 34. 13403–13404.
- Prasad Jagalekar and Murray Woodside. 2000. Evaluating the scalability of distributed systems. *IEEE Transactions on parallel and distributed systems* 11, 6 (2000), 589–603.
- Maxim Jourenko, Kanta Kurazumi, Mario Larangeira, and Keisuke Tanaka. 2019. SoK: A taxonomy for layer-2 scalability related protocols for cryptocurrencies. *Cryptography ePrint Archive* (2019).

- Aljosha Judmayer, Nicholas Stifter, Alexei Zamyatin, Itay Tsabary, Ittay Eyal, Peter Gaži, Sarah Meiklejohn, and Edgar Weippl. 2021. Sok: Algorithmic incentive manipulation attacks on permissionless pow cryptocurrencies. In *International Conference on Financial Cryptography and Data Security*. Springer, 507–532.
- Dimitris Karakostas, Aggelos Kiayias, and Christina Ovezik. 2022. SoK: A Stratified Approach to Blockchain Decentralization. *arXiv preprint arXiv:2211.01291* (2022).
- Kostis Karantias. 2020. Sok: A taxonomy of cryptocurrency wallets. *Cryptology ePrint Archive* (2020).
- Aggelos Kiayias and Philip Lazos. 2022. SoK: Blockchain Governance. *arXiv preprint arXiv:2201.07188* (2022).
- Kartick Kolachala, Ecem Simsek, Mohammed Ababneh, and Roopa Vishwanathan. 2021. SoK: Money Laundering in Cryptocurrencies. In *The 16th International Conference on Availability, Reliability and Security*. 1–10.
- M Kranzberg. 1986. Technology and History: Kranzberg’s Laws, Technology and Culture. (1986).
- Richard Kraut. 2022. Plato. In *The Stanford Encyclopedia of Philosophy* (Spring 2022 ed.), Edward N. Zalta (Ed.). Metaphysics Research Lab, Stanford University.
- Stefano Lande and Roberto Zunino. 2018. SoK: unravelling Bitcoin smart contracts. *Principles of Security and Trust LNCS 10804* (2018), 217.
- Gabriel da Silva Serapião Leal, Wided Guédria, and Hervé Panetto. 2019. Interoperability assessment: A systematic literature review. *Computers in Industry* 106 (2019), 111–132.
- Sung-Shine Lee, Alexandr Murashkin, Martin Derka, and Jan Gorzny. 2022. SoK: Not Quite Water Under the Bridge: Review of Cross-Chain Bridge Hacks. *arXiv preprint arXiv:2210.16209* (2022).
- Rujia Li, Qin Wang, Qi Wang, David Galindo, and Mark Ryan. 2022. SoK: TEE-assisted Confidential Smart Contract. *arXiv preprint arXiv:2203.08548* (2022).
- Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. 2020. A survey on the security of blockchain systems. *Future Generation Computer Systems* 107 (2020), 841–853.
- Iuon-Chang Lin and Tzu-Chun Liao. 2017. A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.* 19, 5 (2017), 653–659.
- Michael L Littman, Ifeoma Ajunwa, Guy Berger, Craig Boutilier, Morgan Currie, Finale Doshi-Velez, Gillian Hadfield, Michael C Horowitz, Charles Isbell, Hiroaki Kitano, et al. 2022. Gathering strength, gathering storms: The one hundred year study on artificial intelligence (AI100) 2021 study panel report. *arXiv preprint arXiv:2210.15767* (2022).
- Patrick McCorry, Chris Buckland, Bennet Yee, and Dawn Song. 2021. Sok: Validating bridges as a scaling solution for blockchains. *Cryptology ePrint Archive* (2021).
- Amani Moin, Kevin Sekniqi, and Emin Gun Sirer. 2020. SoK: A classification framework for stablecoin designs. In *International Conference on Financial Cryptography and Data Security*. Springer, 174–197.
- Ahmed Afif Monrat, Olov Schelén, and Karl Andersson. 2019. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access* 7 (2019), 117134–117151.
- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. 2016. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.
- c Plato. 2005. From the republic. In *Readings in the economics of the division of labor: The classical tradition*. World Scientific, 43–49.
- Eugenia Politou, Fran Casino, Eftimios Alepis, and Constantinos Patsakis. 2019. Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing* 9, 4 (2019), 1972–1986.
- Deepak Puthal, Nisha Malik, Saraju P Mohanty, Elias Kougianos, and Chi Yang. 2018. The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine* 7, 2 (2018), 18–21.
- Mayank Raikwar and Danilo Gligoroski. 2022. SoK: Decentralized Randomness Beacon Protocols. *arXiv preprint arXiv:2205.13333* (2022).
- Mayank Raikwar, Danilo Gligoroski, and Katina Kralevska. 2019. SoK of used cryptography in blockchain. *IEEE Access* 7 (2019), 148550–148575.
- Roy Rinberg and Nilaksh Agarwal. 2022. Privacy when Everyone is Watching: An SOK on Anonymity on the Blockchain. *Cryptology ePrint Archive* (2022).
- Ashish Rajendra Sai, Jim Buckley, Brian Fitzgerald, and Andrew Le Gear. 2021. Taxonomy of centralization in public blockchain systems: A systematic literature review. *Information Processing & Management* 58, 4 (2021), 102584.
- Jerome Saltzer and M Frans Kaashoek. 2009. *Principles of computer system design: an introduction*. Morgan Kaufmann.
- Alan T Sherman, Farid Javani, Haibin Zhang, and Enis Golaszewski. 2019. On the origins and variations of blockchain technologies. *IEEE Security & Privacy* 17, 1 (2019), 72–77.
- Zeshun Shi, Cees de Laat, Paola Grossi, and Zhiming Zhao. 2021. When Blockchain Meets Auction Models: A Survey, Some Applications, and Challenges. *arXiv preprint arXiv:2110.12534* (2021).
- Peter Stone, Rodney Brooks, Erik Brynjolfsson, Ryan Calo, Oren Etzioni, Greg Hager, Julia Hirschberg, Shivaram Kalyanakrishnan, Ece Kamar, Sarit Kraus, et al. 2022. Artificial intelligence and life in 2030: the one hundred year study on artificial intelligence. *arXiv preprint arXiv:2211.06318* (2022).

- Ege Tekiner, Abbas Acar, A Selcuk Uluagac, Engin Kirda, and Ali Aydin Selcuk. 2021. SoK: cryptojacking malware. In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 120–139.
- Habib Tiliouine and Richard J Estes. 2016. The state of social progress of Islamic societies. *Op. cit* 222 (2016).
- Jon Truby. 2018. Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies. *Energy research & social science* 44 (2018), 399–410.
- Fei-Yue Wang. 2010. The emergence of intelligent enterprises: From CPS to CPSS. *IEEE Intelligent Systems* 25, 4 (2010), 85–88.
- Gang Wang. 2021. SoK: Understanding BFT Consensus in the Age of Blockchains. *Cryptography ePrint Archive* (2021).
- Gang Wang, Zhijie Jerry Shi, Mark Nixon, and Song Han. 2019b. Sok: Sharding on blockchain. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*. 41–61.
- Qin Wang, Jiangshan Yu, Shiping Chen, and Yang Xiang. 2020. SoK: Diving into DAG-based blockchain systems. *arXiv preprint arXiv:2012.06128* (2020).
- Shuai Wang, Liwei Ouyang, Yong Yuan, Xiaochun Ni, Xuan Han, and Fei-Yue Wang. 2019a. Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 49, 11 (2019), 2266–2277.
- Peter Wegner. 1996. Interoperability. *ACM Computing Surveys (CSUR)* 28, 1 (1996), 285–287.
- Sam M Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J Knottenbelt. 2021. Sok: Decentralized finance (defi). *arXiv preprint arXiv:2101.08778* (2021).
- Jiahua Xu, Krzysztof Paruch, Simon Cousaert, and Yebo Feng. 2021. Sok: Decentralized exchanges (dex) with automated market maker (AMM) protocols. *arXiv preprint arXiv:2103.12732* (2021).
- Sen Yang, Fan Zhang, Ken Huang, Xi Chen, Youwei Yang, and Feng Zhu. 2022. SoK: MEV Countermeasures: Theory and Practice. *arXiv preprint arXiv:2212.05111* (2022).
- Jingfan Yu, Mengqian Zhang, Xi Chen, and Zhixuan Fang. 2022. SoK: Play-to-Earn Projects. *arXiv preprint arXiv:2211.01000* (2022).
- Alexei Zamyatin, Mustafa Al-Bassam, Dionysis Zindros, Eleftherios Kokoris-Kogias, Pedro Moreno-Sanchez, Aggelos Kiayias, and William J Knottenbelt. 2021. Sok: Communication across distributed ledgers. In *International Conference on Financial Cryptography and Data Security*. Springer, 3–36.
- Dirk A Zetzsche, Douglas W Arner, and Ross P Buckley. 2020. Decentralized finance. *Journal of Financial Regulation* 6, 2 (2020), 172–203.
- Luyao Zhang, Xinshi Ma, and Yulin Liu. 2022. SoK: Blockchain Decentralization. *arXiv preprint arXiv:2205.04256* (2022).
- Luyao Zhang and Xinyu Tian. 2022. On Blockchain We Cooperate: An Evolutionary Game Perspective. *arXiv preprint arXiv:2212.05357* (2022).
- Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)* 52, 3 (2019), 1–34.
- Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. 2022. SoK: Decentralized Finance (DeFi) Incidents. *arXiv preprint arXiv:2208.13035* (2022).
- Qiheng Zhou, Huawei Huang, Zibin Zheng, and Jing Bian. 2020. Solutions to scalability of blockchain: A survey. *Ieee Access* 8 (2020), 16440–16455.

Citation	Title
<b>Category 1: Privacy and Security</b>	
Almashaqbeh and Solomon [2022]	SoK: privacy-preserving computing in the blockchain era
Bonneau et al. [2015]	SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies
Wang [2021]	SoK: Understanding BFT Consensus in the Age of Blockchains
Eskandari et al. [2020]	Sok: Transparent dishonesty: front-running attacks on blockchain
Baum et al. [2021]	Sok: Mitigation of front-running in decentralized finance
Raikwar et al. [2019]	SoK of used cryptography in blockchain
Heimbach and Wattenhofer [2022]	SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance
Zhou et al. [2022]	SoK: Decentralized Finance (DeFi) Incidents
Li et al. [2022]	SoK: TEE-assisted Confidential Smart Contract
Ankele et al. [2020]	SoK: Cyber-Attack Taxonomy of Distributed Ledger-and Legacy Systems-based Financial Infrastructures
Yang et al. [2022]	SoK: MEV Countermeasures: Theory and Practice
Azouvi and Hicks [2019]	Sok: Tools for game theoretic models of security for cryptocurrencies
Atzei et al. [2017]	A survey of attacks on ethereum smart contracts (sok)
Judmayer et al. [2021]	Sok: Algorithmic incentive manipulation attacks on permissionless pow cryptocurrencies
Di Angelo et al. [2020]	SoK: Development of secure smart contracts–lessons from a graduate course
Chen et al. [2020]	A survey on ethereum systems security: Vulnerabilities, attacks, and defenses
Islam et al. [2021]	A Review on Blockchain Security Issues and Challenges
Li et al. [2020]	A survey on the security of blockchain systems
Garay and Kiayias [2020]	Sok: A consensus taxonomy in the blockchain era
Tekiner et al. [2021]	SoK: cryptojacking malware
Alsalam and Zhang [2019]	SoK: A systematic study of anonymity in cryptocurrencies
Deuber et al. [2022]	SoK: Assumptions Underlying Cryptocurrency Deanonymizations
Rinberg and Agarwal [2022]	Privacy when Everyone is Watching: An SOK on Anonymity on the Blockchain
Bonomi et al. [2021]	SoK: Achieving State Machine Replication in Blockchains based on Repeated Consensus
Ghesmati et al. [2021]	SoK: How private is Bitcoin? Classification and Evaluation of Bitcoin Mixing Techniques
Franzoni and Daza [2022]	SoK: Network-Level Attacks on the Bitcoin P2P Network
<b>Category 2: Scalability</b>	
Wang et al. [2019b]	SoK: Sharding on Blockchain
Gudgeon et al. [2020]	SoK: Layer-Two Blockchain Protocols
McCorry et al. [2021]	Sok: Validating bridges as a scaling solution for blockchains
Chatzigiannis et al. [2022]	SoK: Blockchain light clients
Zhou et al. [2020]	Solutions to scalability of blockchain: A survey
<b>Category 3: Decentralization</b>	
Zhang et al. [2022]	SoK: Blockchain Decentralization
Karakostas et al. [2022]	SoK: A Stratified Approach to Blockchain Decentralization
Raikwar and Gligoroski [2022]	SoK: Decentralized Randomness Beacon Protocols

Table 1. A Taxonomy of SoKs

Citation	Title
<b>Category 4: Applicability</b>	
Gudgeon et al. [2020]	SoK: Layer-Two Blockchain Protocols
Bartoletti et al. [2021]	SoK: lending pools in decentralized finance
Werner et al. [2021]	SoK: Decentralized Finance (DeFi)
Xu et al. [2021]	SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols
Shi et al. [2021]	When Blockchain Meets Auction Models: A Survey, Some Applications, and Challenges
Abuidris et al. [2019]	A survey of blockchain-based on e-voting systems
Gadekallu et al. [2022]	Blockchain for the Metaverse: A Review
Ali et al. [2019]	Blockchain and the future of the internet: A comprehensive review
Cousaert et al. [2022]	Sok: Yield aggregators in defi
Yu et al. [2022]	SoK: Play-to-Earn Projects
Dotan et al. [2020]	SOK: cryptocurrency networking context, state-of-the-art, challenges
Moin et al. [2020]	SoK: A classification framework for stablecoin designs
Gan et al. [2021]	A critical review of blockchain applications to banking and finance: a qualitative thematic analysis approach
Dasaklis et al. [2021]	Sok: Blockchain solutions for forensics
Wang [2021]	SoK: tokenization on blockchain
Karantias [2020]	Sok: A taxonomy of cryptocurrency wallets
Clark et al. [2019]	SoK: demystifying stablecoins
Jurenko et al. [2019]	SoK: A taxonomy for layer-2 scalability related protocols for cryptocurrencies
Lande and Zunino [2018]	SoK: unraveling Bitcoin smart contracts
Moin et al. [2020]	SoK: A Classification Framework for Stablecoin Designs
<b>Category 5: Governance and Regulations</b>	
Kiayias and Lazos [2022]	SoK: Blockchain Governance
Chatzigiannis et al. [2021]	SoK: Auditability and Accountability in Distributed Payment Systems
Kolachala et al. [2021]	SoK: Money Laundering in Cryptocurrencies
Casino et al. [2022]	SoK: Cross-border Criminal Investigations and Digital Evidence
Deuber et al. [2022]	SoK: Assumptions Underlying Cryptocurrency Deanonymizations -A Taxonomy for Scientific Experts and Legal Practitioners
<b>Category 6: System Design</b>	
Wang et al. [2020]	SoK: Diving into DAG-based blockchain systems
Bellaj et al. [2022]	SOK: a comprehensive survey on distributed ledger technologies
<b>Category 7: Cross-chain Interoperability</b>	
Zamyatin et al. [2021]	Sok: Communication across distributed ledgers
Wang [2021]	Sok: Exploring blockchains interoperability
Eskandari et al. [2021]	Sok: Oracles from the ground truth to market manipulation
Lee et al. [2022]	SoK: Not Quite Water Under the Bridge: Review of Cross-Chain Bridge Hacks
Belchior et al. [2021]	A Survey on Blockchain Interoperability: Past, Present, and Future Trends
Belchior et al. [2022]	Do You Need a Distributed Ledger Technology Interoperability Solution?

Table 2. The List of SoKs (continued)

Table 3. The Bigram of Blockchain Related SoK Titles (Top 25)

bigram	counts
(decentralized, finance)	5
(distributed, ledger)	3
(smart, contract)	3
(blockchain, system)	2
(stablecoin, design)	2
(classification, framework)	2
(ledger, technology)	2
(framework, stablecoin)	2
(blockchain, decentralization)	2
(finance, defi)	2
(finance, decentralized)	2
(blockchain, era)	2
(dag-based, blockchain)	1
(lending, pool)	1
(ledger, lending)	1
(across, distributed)	1
(communication, across)	1
(contract, communication)	1
(confidential, smart)	1
(tee-assisted, confidential)	1
(system, tee-assisted)	1
(solution, blockchains)	1
(diving, dag-based)	1
(client, diving)	1
(light, client)	1

Table 4. The Bigram of Blockchain Related SoK Abstracts (Top 1-45)

bigram	counts
(blockchain, technology)	25
(smart, contract)	25
(blockchain, system)	14
(future, research)	13
(systematization, knowledge)	12
(decentralized, finance)	11
(research, direction)	10
(lending, pool)	8
(consensus, protocol)	7
(finance, defi)	7
(automated, market)	6
(blockchain, metaverse)	6
(recent, year)	6
(market, maker)	6
(cryptographic, concept)	6
(security, privacy)	6
(layer-two, protocol)	6
(machine, replication)	6
(state, machine)	6
(maker, amm)	5
(blockchain, interoperability)	5
(digital, forensics)	5
(yield, farming)	5
(application, blockchain)	5
(distributed, system)	5
(open, research)	5
(research, challenge)	5
(distributed, ledger)	5
(blockchain, ecosystem)	5
(best, knowledge)	5
(blockchain, security)	4
(repeated, consensus)	4
(finance, sector)	4
(banking, finance)	4
(transfer, asset)	4
(use, case)	4
(privacy, issue)	4
(future, direction)	4
(decentralized, application)	4
(cross-chain, communication)	4
(body, research)	4
(solution, finally)	4
(off-chain, transaction)	4
(financial, system)	4
(open, challenge)	4

Table 5. The Bigram of Blockchain Related SoK Abstracts Continued (Top 46-90)

bigram	counts
(provide, systematization)	4
(payment, system)	4
(systematic, comprehensive)	4
(bft, consensus)	4
(protocol, along)	4
(first, present)	3
(security, guarantee)	3
(finally, discuss)	3
(general, design)	3
(payment, state)	3
(work, blockchain)	3
(layer-two, solution)	3
(state, channel)	3
(light, client)	3
(built, top)	3
(third, party)	3
(exchange, dexs)	3
(existing, protocol)	3
(system, security)	3
(integral, part)	3
(decentralized, exchange)	3
(ledger, technology)	3
(technology, dlt)	3
(auction, model)	3
(research, innovation)	3
(existing, solution)	3
(challenge, future)	3
(service, however)	3
(high, latency)	3
(cryptographic, primitive)	3
(existing, system)	3
(potential, research)	3
(solution, blockchain)	3
(two, major)	3
(property, system)	3
(provide, first)	3
(scattered, body)	3
(consensus, mechanism)	3
(important, role)	3
(application, domain)	3
(paper, conduct)	3
(conduct, systematic)	3
(research, gap)	3
(identify, future)	3
(based, finding)	3

Table 6. The Top 28 blockchain project and cross-chain solutions: ranked by market value retrieved from coinmarketcap on Dec. 27, 2022

Rank	name	symbol	Genesis	Type
1	Bitcoin	BTC	2009	Blockchain
2	Ethereum	ETH	2015	Blockchain
3	Binance smart chain	BNB	2017	Blockchain
4	XRP Ledger (Ripple)	XRP	2021	Blockchain
5	Cardano	ADA	2017	Blockchain
6	Polkadot	DOT	2022	Cross-chain
7	TRON	TRX	2017	Blockchain
8	Solana	SOL	2020	Blockchain
9	Avalanche	AVAX	2020	Blockchain
10	Chainlink	LINK	2017	Cross-chain
11	The Open Network (TON)	TON	2018	Blockchain
12	Cosmos	ATOM	2016	Cross-chain
13	Stellar	XLM	2015	Blockchain
14	Cronos Chain	CRO	2018	Blockchain
15	Quant Overledger	QNT	2018	Cross-chain
16	Agorand	ALGO	2019	Blockchain
17	NEAR Protocol	NEAR	2021	Blockchain
18	Filecoin	FIL	2017	Cross-chain
19	Hedera	HBAR	2019	Blockchain
20	Internet Computer	ICP	2021	Blockchain
21	EOS Network	EOS	2018	Blockchain
22	MultiversX (Elrond)	EGLD	2020	Blockchain
23	Flow	FLOW	2018	Blockchain
24	Theta Network	THETA	2019	Blockchain
25	Tezos	XTZ	2018	Blockchain
26	Zcash	ZEC	2016	Blockchain
27	Klaytn	KLAY	2019	Blockchain
28	Dash	DASH	2014	Blockchain

Table 7. The Bigram of Blockchain Projects and Cross-chain solutions Titles (Top 10)

bigram	counts
(smart, contract)	2
(public, blockchain)	2
(blockchain, platform)	2
(white, paper)	2
(public, hashgraph)	1
(ledger, stellar)	1
(distributed, ledger)	1
(network, distributed)	1
(whitepaper, network)	1
(cosmos, whitepaper)	1
(network, cosmos)	1
(open, network)	1
(network, open)	1
(oracle, network)	1
(decentralized, oracle)	1
(evolution, decentralized)	1
(step, evolution)	1
(next, step)	1
(chainlink, next)	1
(dynamic, chainlink)	1
(avax, dynamic)	1
(token, avax)	1
(native, token)	1
(avalanche, native)	1
(v0, avalanche)	1

Table 8. The Bigram of Blockchain Projects and Cross-chain Solutions Abstracts (Top 1-45)

bigram	counts
(smart, contract)	27
(technical, paper)	8
(digital, asset)	6
(consensus, algorithm)	6
(blockchain, network)	6
(decentralized, application)	5
(virtual, machine)	5
(public, blockchain)	5
(cosmos, hub)	5
(byzantine, agreement)	4
(decentralised, application)	4
(blockchain, architecture)	4
(transaction, second)	4
(beacon, chain)	4
(native, token)	3
(development, platform)	3
(payment, scheme)	3
(storage, network)	3
(zone, cosmos)	3
(distributed, application)	3
(blockchain, application)	3
(end, user)	3
(proof, stake)	3
(new, blockchain)	3
(paper, proposes)	3
(blockchain, platform)	3
(programming, language)	3
(blockchain, technology)	3
(paper, also)	3
(introduces, new)	2
(tendermint, bft)	2
(ibc, protocol)	2
(communication, ibc)	2
(inter-blockchain, communication)	2
(hub, zone)	2
(zone, hub)	2
(well, suited)	2
(cosmos, network)	2
(address, problem)	2
(network, architecture)	2
(transaction, ledger)	2
(transaction, throughput)	2
(governance, mechanism)	2
(machine, evm)	2
(without, need)	2

Table 9. The Bigram of Blockchain Projects and Cross-chain Solutions Abstracts (Top 46-90)

bigram	counts
(ba, protocol)	2
(achieves, robustness)	2
(protocol, scp)	2
(application, built)	2
(set, transaction)	2
(next, set)	2
(secure, scalable)	2
(algorand, us)	2
(widespread, adoption)	2
(network, providing)	2
(application, across)	2
(broad, range)	2
(ledger, technology)	2
(distributed, ledger)	2
(trusted, secure)	2
(cronos, designed)	2
(transaction, fee)	2
(low, transaction)	2
(million, transaction)	2
(provides, useful)	2
(network, ton)	2
(used, encode)	2
(strong, focus)	2
(work, present)	2
(network, communicate)	2
(consensus, protocol)	2
(handling, million)	2
(high, speed)	2
(autonomous, organization)	2
(functional, programming)	2
(decentralized, autonomous)	2
(important, part)	2
(cpu, power)	2
(longest, chain)	2
(network, network)	2
(peer-to-peer, network)	2
(open, source)	2
(advanced, feature)	2
(open, network)	2
(consensus, mechanism)	2
(hybrid, smart)	2
(computing, resource)	2
(off-chain, computing)	2
(oracle, network)	2
(new, blockchains)	2

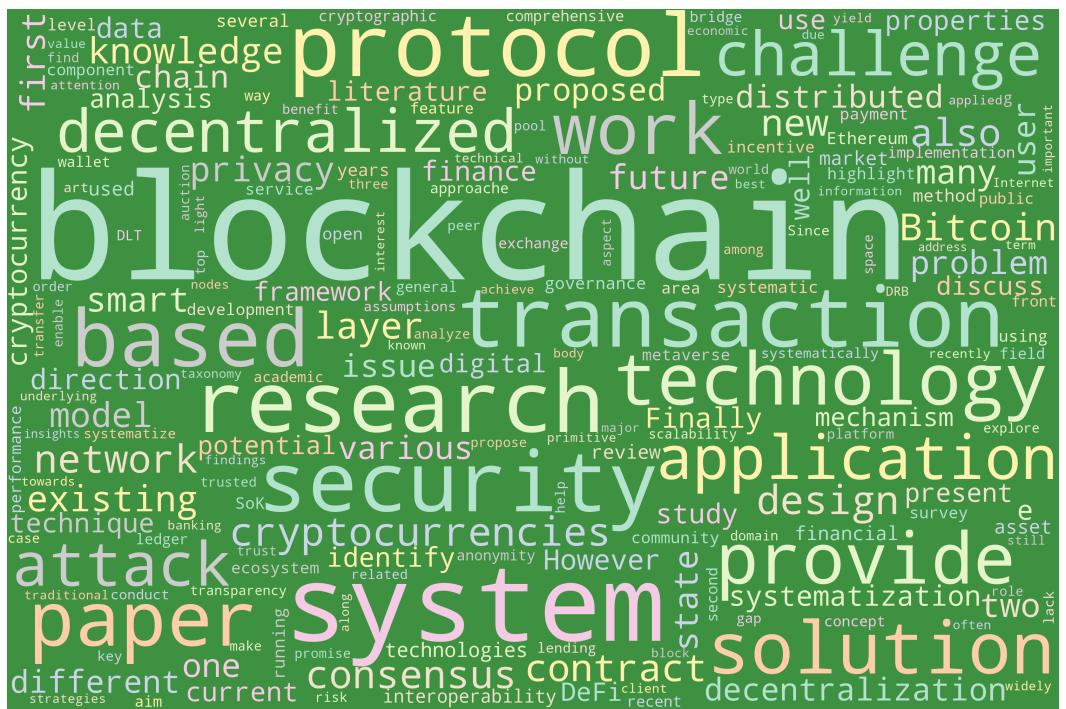


Fig. 3. The Word Cloud of blockchain Related SoK Abstract

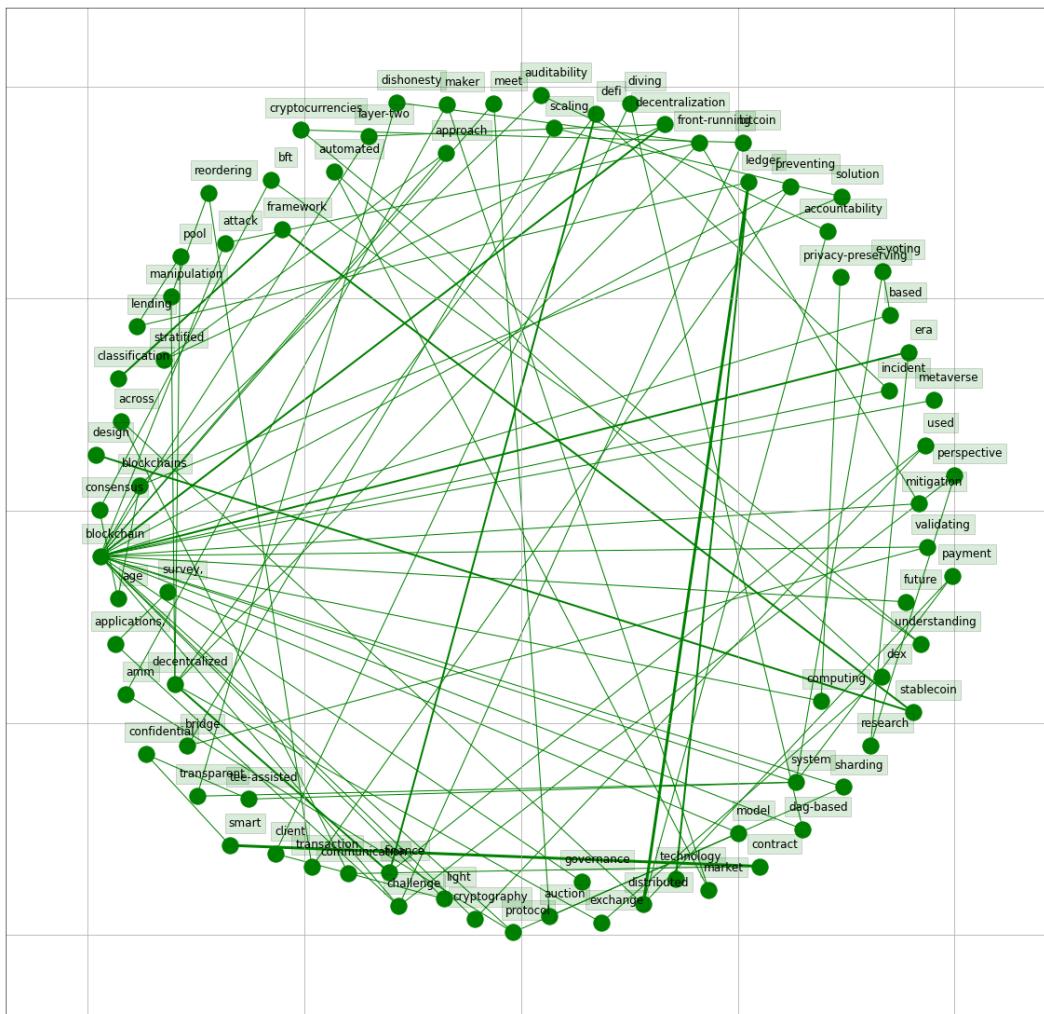


Fig. 4. The Bigram of blockchain Related SoK Title

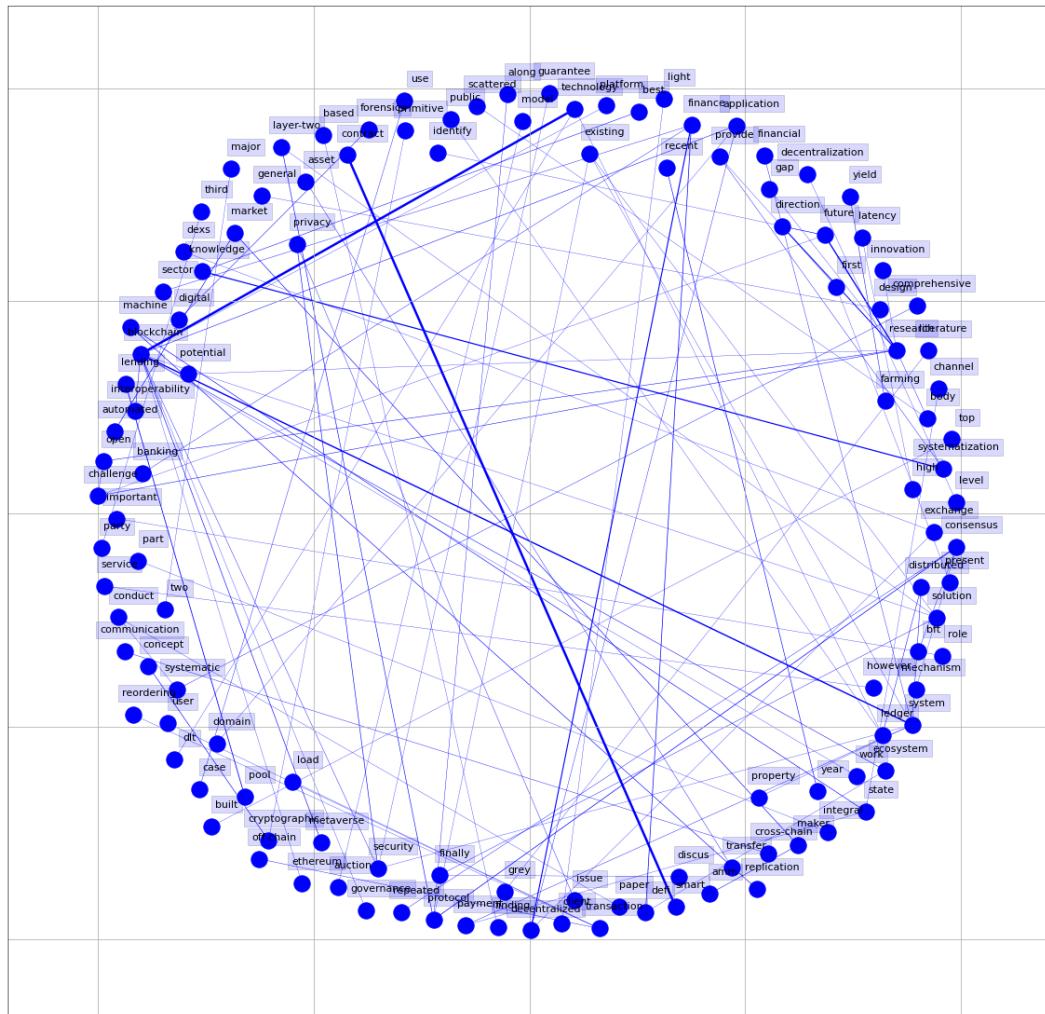


Fig. 5. The Bigram of blockchain Related SoK Abstract

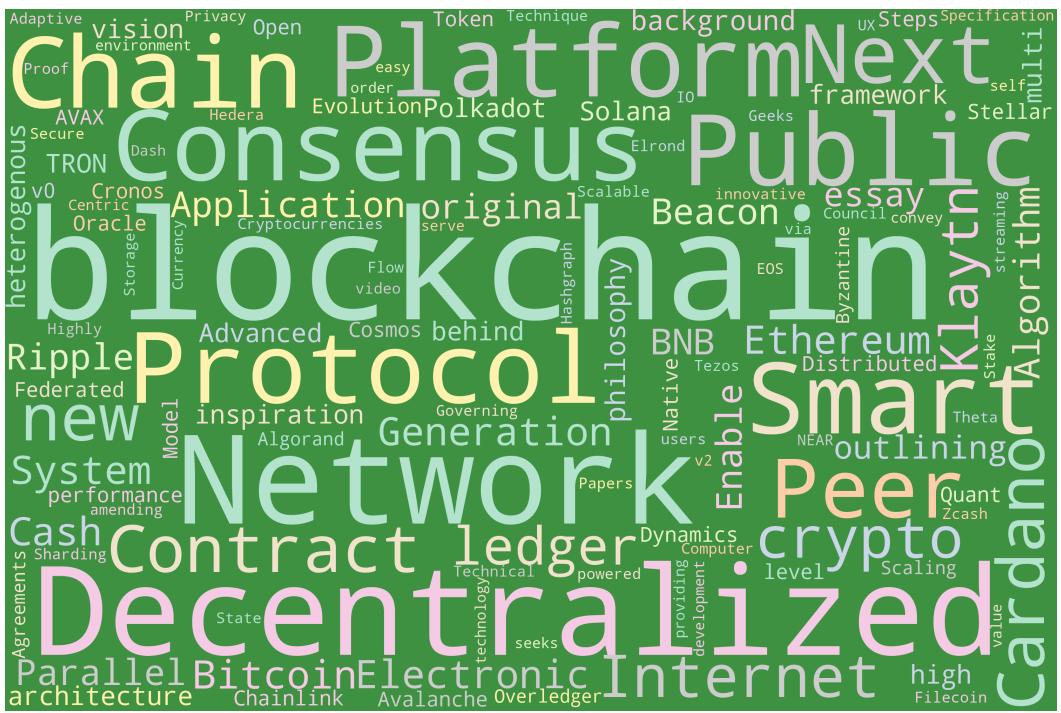


Fig. 6. The Word Cloud of blockchain Projects and Cross-chain Solutions Title

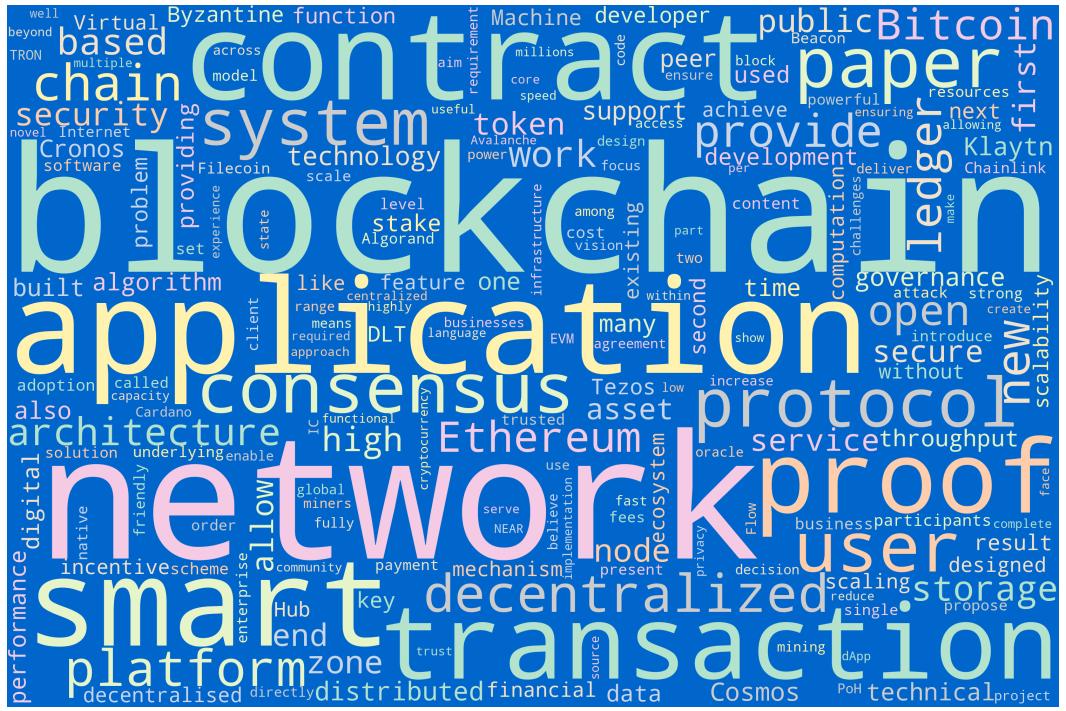


Fig. 7. The Word Cloud of blockchain Projects and Cross-chain Solution Abstract

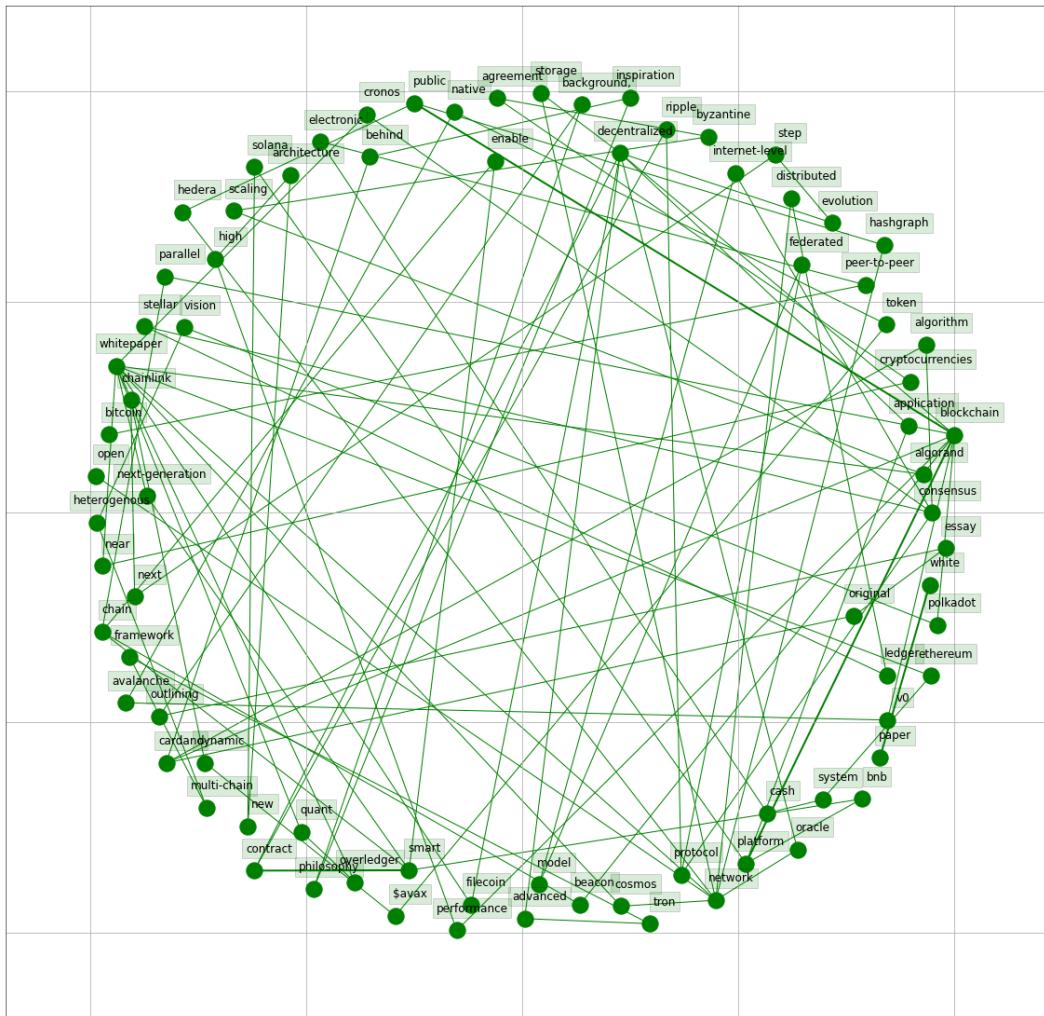


Fig. 8. The Bigram of blockchain Projects and Cross-chain Solution Title

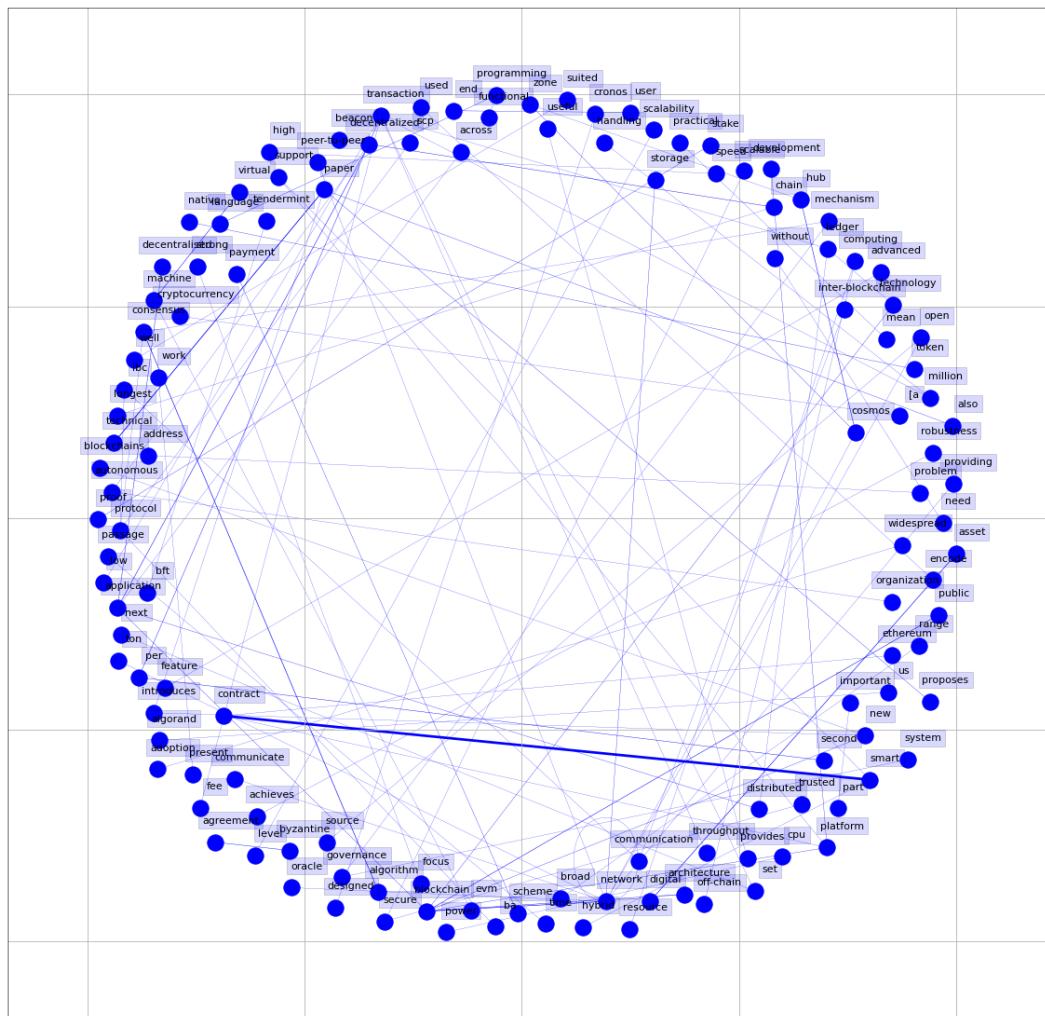


Fig. 9. The Bigram of blockchain Projets and Cross-chain Solution Abstract