frontiers in Blockchain

PERSPECTIVE
published: 11 September 2020
doi: 10.3389/fbloc.2020.522600

Convergence of Blockchain, IoT, and AI

Philipp Sandner*, Jonas Gross and Robert Richter

Frankfurt School Blockchain Center, Frankfurt School of Finance & Management, Frankfurt, Germany

Blockchain, IoT, and AI are key technologies driving the next wave of the digital transformation. We argue that these technologies will converge and will allow for new business models: Autonomous agents (i.e., sensors, cars, machines, trucks, cameras, and other IoT devices) will in the future act as own profit centers that (1) have a digital twin leveraging IoT, (2) send and receive money leveraging blockchain technology on their own, and (3) autonomously make decisions as independent economic agents leveraging AI and data analytics. We further argue that this convergence will drive the development of such autonomous business models and, with it, the digital transformation of industrial corporations.

Keywords: blockchain, internet of things (IoT), artificial intelligence (AI), crypto assets, payments, digital Euro, tokenization

OPEN ACCESS

Edited by:
Olinga Taeed,
Centre for Citizenship, Enterprise and Governance, United Kingdom

Reviewed by:
Erika Beerbower,
Independent Researcher, Denver, United States
Natalie Pankova,
Metadvice Ltd, United Kingdom

****Correspondence:***
Philipp Sandner
philipp.sandner@fs-blockchain.de

Specialty section:
This article was submitted to Blockchain for Science, a section of the journal Frontiers in Blockchain

Received: *23 December 2019*
Accepted: *21 August 2020*
Published: *11 September 2020*

Citation:
Sandner P, Gross J and Richter R (2020) Convergence of Blockchain, IoT, and AI. Front. Blockchain 3:522600. doi: 10.3389/fbloc.2020.522600

INTRODUCTION

Today, blockchain technology, internet of things (IoT), and artificial intelligence (AI) are recognized as innovations that have the potential to improve current business processes, create new business models, and disrupt whole industries. Blockchain, for example, can increase trust, transparency, security, and privacy of business processes by providing a shared and decentralized distributed ledger. A blockchain, or generally a distributed ledger, can store all kinds of assets similar to a register (Diedrich, 2016). Primarily, these data can be related to money and identities. IoT drives the automatization of industries and user-friendliness of business processes that is essential for the German and the European industry. Finally, AI improves processes by detecting patterns and optimizing outcomes of these business processes (Salah et al., 2019).

Up to this point, the interconnection between these three innovations is often neglected, and blockchain, IoT, and AI are typically used separately. However, these innovations can and should be applied jointly and will converge in the future. One possible connection between these technologies could be that IoT collects and provides data, blockchain provides the infrastructure and sets up the rules of engagement, while AI optimizes processes and rules (Salah et al., 2019; Zheng et al., 2020). By design, these three innovations are complementary and can exploit their full potential if combined. The convergence of these technologies can be particularly promising for data management and the automatization of business processes that we analyze and discuss in the following.

THE INTERCONNECTION BETWEEN BLOCKCHAIN, IoT, AND AI

Until a few years ago, blockchain technology was only discussed in the context of payments, i.e., in the context of Bitcoin (Nakamoto, 2008) and Ether. In the last years, more and more non-financial use cases for blockchain technology emerged (Treleaven et al., 2017), such as supply chain management and digital identities (Roeck et al., 2020). The more recent literature identifies the value of combining blockchain technology with other innovations such as IoT and AI. For example, Huh et al. (2017) discuss the use of blockchain technology to improve the system infrastructure of various IoT devices. Dorri et al. (2017) outline how the architecture of blockchains can be modified such that the resulting infrastructure is better equipped to serve IoT devices, especially with respect to the speed of transactions. Besides focusing on blockchain in connection with IoT, some studies also focus on the combination of blockchain and AI (Salah et al., 2019). To date, the focus is primarily on connecting blockchain with one other innovative technology, such as IoT and AI, and not applying all three innovations simultaneously. However, the true potential of these new, emerging technologies will only be unlocked if these innovations are combined. Kumar Singh et al. (2020) design a blockchain-based infrastructure that supports IoT and AI. Contrary to Kumar Singh et al. (2020), this paper provides a non-technical overview of the benefits of each innovation and how they complement each other. The potential combination of blockchain technology, IoT and AI is illustrated by a concrete use case.

Note that the concepts introduced in this paper apply to both public and private blockchains. The primary difference between the two types of blockchains is that in a public blockchain every participant can access data stored on the blockchain. In contrast, in private blockchains, access to data is restricted to selected entities. For the purpose of this paper, it is secondary whether the access is public or private as the use cases could be implemented on both blockchain infrastructures. Furthermore, it should be noted that blockchains, in line with any other database, are impacted by poor data quality. Since this topic is not solely related to blockchain-based data, it will not be discussed further in this paper.

Data Management

Improving Standardization, Privacy, Security, and Scalability of Data

IoT devices, such as smart home devices, smart buildings, sensors, machines, cars, or smart grids, typically collect a large amount of data. This data is often stored on a centralized server, where the data format is not standardized. Companies use different legacy systems that make it difficult to extract and interpret data cross-platform. Blockchain technology could help with the standardization of data by setting up a harmonized digital platform for IoT data accessible for multiple parties. Data would then be stored in one data format. Due to the use of hash functions, data on blockchain systems is typically stored in one data format. Consequently, data management could be optimized by increased interoperability of stored data (Karafiloski and Mishev, 2017).

There exist two general storage options for blockchain-based data, namely on-chain and off-chain storage. On-chain storage has the advantage that data is always available on-chain and can be restored from any node at any time. However, storage requirements are significant, which can lead to “blockchain bloating” were a large amount of on-chain-stored data hamper blockchains throughput and scalability. Off-chain storage offers an alternative that stores the actual data off-chain and only keeps aggregated metadata on-chain. This alternative has the benefit of being considerably more scalable than the on-chain solution but decreases data transparency.

Another feature of blockchain platforms is the high degree of data privacy that can be implemented by the underlying cryptography (Zyskind et al., 2015). On blockchains, transactions are mainly conducted using pseudonyms or are – in some blockchain systems such as Monero or Zcash – conducted completely anonymously. The architecture of blockchain systems also allows for full encryption of stored and transmitted data such that only the device itself can read and write its own data through private/public key infrastructure (Es-Samaali et al., 2017). In IoT, machines and devices store a large amount of sensitive data. It is essential to ensure privacy and security of this data. Today, IoT data is often sent directly from the machine to the respective database (often a cloud), where the data is collected. However, this data is not encrypted and does, therefore, not ensure privacy. Blockchain technology can provide tremendous benefits in this respect as blockchain technology can easily ensure privacy of the collected data. Blockchain technology has been developed with the following approach: Security by design.

Further, a blockchain is operationally resilient and has a low risk of hacks. This high level of security arises from the combination of cryptography and the consensus mechanisms used. Thus, using blockchain technology can increase data security (Steger, 2017). However, there is a trade-off between a high level of privacy and control for illicit activities. In case a blockchain platform is set up completely anonymously, it is not possible to associate a transaction with a particular party. This anonymity opens the door for illicit activities, such as money laundering or terrorist financing. AI can help increasing security and detecting illicit activities. Yin et al. (2019) propose to use AI leveraging data analytics to reduce the risk of illicit activities on the blockchain resulting from the anonymity of transactions. AI technologies benefit from the high amount of provided IoT data since AI algorithms learn from the data – the more data is used to train the AI algorithm, the better the performance of the algorithm.

Today, it is one of the main limitations of IoT to store and manage a large amount of data. The management of data could be made more scalable by a convergence of technologies using blockchain technology and AI jointly. Opponents of blockchain technology criticize that blockchain systems lack scalability due to the use of energy-consuming consensus mechanisms to validate transactions, e.g., proof-of-work consensus (Li et al., 2019). However, there are various more energy-efficient consensus mechanisms, such as proof-of-stake or proof-or-authority that can increase scalability (Narayanan et al., 2016). In fact, the high energy consumption will soon be an artifact of the Bitcoin network. Alongside blockchain, AI can support a further increase in scalability. Liu et al. (2019) propose a performance optimization framework for blockchain-enabled IoT systems. This system could be grounded on deep reinforcement learning (DRL), one form of machine learning, to reach a higher degree of throughput. The authors suggest a "DRL-based algorithm to dynamically select/adjust the block producers, consensus algorithm, block size, and block interval to improve the performance."

To summarize, blockchain technology can improve data management of IoT devices due to its transparency, trust, truthfulness, immutability, security, and privacy features. Combined with AI, it can address current limitations of IoT data.

Authentication via a Blockchain-Based Identity

Moreover, blockchain technology can be applied to authenticate IoT network participants and can increase trust by managing the identity of IoT devices. Note that identity management can refer to individuals and companies but – in the context of IoT – also to IoT devices and machines. Blockchain-based identities ensure that transaction parties receive a digital identity on the blockchain, based on their physical identity (e.g., identity card for individuals, commercial register entry for companies). Based on such an identity, transactions between an individual and a company (example: car sharing) but also between an individual and a machine (example: passenger transport of an autonomous car) or between two machines (example: autonomous car pays for parking) can be processed efficiently – i.e., with fast transaction speed and low transaction costs (Zhu and Badr, 2018).

In the future, money will be transferred between individuals, companies, devices, and machines. According to estimates by IoT Analytics, more than 20 billion devices will be connected to the internet by 2025 (IoT Analytics, 2020). These devices will partly also participate in payment processes. Therefore, a completely new, possibly decentralized, payment infrastructure will be required. Individuals, companies, and machines must be registered with their digital identities on blockchain systems. Consequently, identity management on a blockchain will play a key role.

Of course, these identities have to be issued and managed in compliance with data protection laws. However, the critique that blockchains cannot sufficiently account for data protection by design is not appropriate. This is due to the fact that blockchain technology, with its integrated access systems and encryption processes, is even better than non-blockchain-based systems able to firstly protect data by design, secondly organize the ownership of data and, thirdly enable the monetization of data (Suliman et al., 2018).

Another advantage of blockchain technology is that the immutable record of the digital identity is difficult to forge. In the context of independently interacting machines and devices, it is crucial to be able to rely on the identity of things that can be reached by the help of blockchain technology.

Automatization via Smart Contracts

Aside from data and identity management purposes, the convergence of the three innovations by applying blockchain, IoT, and AI jointly can be very promising for the automatization of business processes. One crucial component of connecting these three innovations is the use of smart contracts.

Smart contracts specify a set of promises, digitally, in a protocol that automatically executes the terms of the contract (Szabo, 1996). In programming terms, smart contracts are comparable to "if-then" functions that define specific actions if a particular event takes place. For example, one can think of a situation if in the case the delivery of a good has been successful ("if"), a payment is made automatically ("then"). In other words, smart contracts are the main connector of the three building blocks IoT, AI, and blockchain technology.

Despite its enormous potential, smart contracts are currently not used in the context of industrial companies. The main issue behind classical smart contracts is that they require crypto assets such as Ether or EOS and, therefore, transfer amounts of these crypto assets. However, companies are hesitant to use crypto assets, mainly due to regulatory and economic reasons. One main limitation is the high price volatility of crypto assets. If a smart contract is conducted in Ether, then the receiving party is exposed to a high exchange rate risk. Sometimes, the price of crypto assets increases or decreases by more than ten percent within one day. Even if stablecoins can potentially provide a solution to the high volatility of "classical" crypto assets, they will not be heavily used by industrial companies or in B2B contexts for the following reasons: Firstly, stablecoins are currently unregulated. Therefore, risk-averse companies do not seek to use such unregulated instruments. Secondly, companies' accounting and IT systems are denominated in and working with fiat currencies like the Euro. Consequently, it is an operational burden for companies to convert the stablecoin in their "system-based" currency. This conversion costs both personnel (i.e., working time) and financial resources (i.e., transaction costs, hedging for price fluctuations).

The only way the potential of smart contracts can be fully exploited is by using a blockchain-based fiat currency that "flows through" the smart contract. Only a blockchain-based digital Euro would enable Euro-denominated smart contracts, such that machines, cars or sensors can directly offer services on their own like pay-per-use, leasing, and factoring. Due to a digital blockchain-based Euro, such new business models could come into existence: fully automized devices making decisions on their own leveraging AI and "economically surviving" on their own leveraging blockchain for financial transactions while implementing a profit center logic on the device-level.

The benefits of such a DLT-based digital Euro are manifold. First, with such blockchain-based digital currency, micropayments for IoT devices could be transacted with low transaction fees that are essential for the further evolution of IoT. Secondly, every transaction denominated in this blockchain-based digital Euro would be included in internal Enterprise

Resource Planning (ERP) systems and would, therefore, be directly accessible for invoicing and accounting purposes. Thirdly, in comparison to crypto assets and stablecoins, conversion in fiat currencies would become redundant, thereby saving valuable resources. Fourthly, such a digital fiat currency would comply with current regulations. There are first startups that have developed blockchain-based fiat currencies and use e-money licenses for the tokenization of fiat currencies (CashOnLedger, 2020; Monerium, 2020). Therefore, industrial companies demanding such blockchain-based Euro solutions do not have to fear regulatory uncertainty since existing e-money regimes are used (Sandner et al., 2020b).

The blockchain-based Euro can be issued either by banks, e-money institutes, as indicated above, unregulated institutions, or central banks (Sandner et al., 2020b). According to a study by the Bank for International Settlements (Barontini and Holden, 2019), more than 70 central banks worldwide currently analyze the issuance of an own central bank digital currency (CBDC). However, no central bank has yet introduced such a currency, even if the Swedish central bank and the Chinese central bank are pioneering and might potentially launch a first central bank digital currency soon. The Chinese CBDC project DC/EP is currently being tested in various Chinese cities, also in Chinese subsidiaries of international companies, such as McDonald's or Starbucks. To date, the European Central Bank (ECB) has not yet announced the issuance of a CBDC. Nevertheless, a European blockchain-based CBDC would be required for the use of a central bank-backed Euro for smart contracts in the European industry.

One might ask: Why is a central bank-issued Euro necessary if e-money providers have already introduced a blockchain-based Euro? The answer lies in detail: The money issued by e-money providers counts as e-money/commercial bank money, while the money provided by the central bank is central bank money. Even if both forms of money represent the Euro, in the case of bankruptcy, commercial bank money could default, whereas central bank money is a claim to the central bank, that can, by definition, not go bankrupt. Even if this difference seems non-essential in times of economic and financial stability, it gets highly relevant in times of crisis.

Use Case: The Joint Potential of Blockchain, IoT, and AI

Based on the previous discussion it is evident that the combination of blockchain technology with IoT devices and AI can unlock new business models for the monetization of IoT devices. One such use case is outlined below.

One can think of a lamp (e.g., a street light), that has its own blockchain-based identity (see section "Data Management") and operates with a blockchain-based Euro (see section "Automatization Via Smart Contracts"). Therefore, the lamp gets the status of an autonomous entity operating "on its own." By using smart contracts, micropayments can be made directly to the lamp, triggering the lamp to turn on. The lamp will shine once somebody pays for it, e.g., an individual, a company, or even the public administration. In this context, pay-per-use payment schemes could be implemented. Since the lamp owns a digital wallet, it can act as its own profit center.

Since all lamps are connected to a blockchain, they will store data, e.g., about their usage, performance, and downtime. Artificial intelligence could leverage this data and optimize the network's maintenance. For example, it could suggest a more regular maintenance of lamps that are used frequently as well as immediately dispatch the maintenance crew in case of a fault. Additionally, AI can smooth the maintenance process by improving the ordering process of replacement parts for the network or by helping to anticipate the number of replacement parts required more precisely. This support would ultimately result in less down-time of the network.

Since lamps can be tokenized as assets, they can be made available to investors (International Institute for Sustainable Development, 2019). Consequently, investors could be willing to build and maintain these lamps on a full scale. In return, investors would receive their share on the lamps' profits. This application is a potential gamechanger. The tokenization of such assets could drive a new wave of investments since investors would directly be rewarded with a share of the return of the tokenized asset, in this case, of the lamp. The benefits of tokenization do not only hold for lamps but all IoT devices and, therefore, a wide range of industrial applications. For example, this could be sensors, cars, machines, cameras, trucks once these devices are connected to the internet and are connected to a blockchain network.

CONCLUSION

Blockchain, IoT, and AI are technologies that can be combined in multiple dimensions. We argue that a convergence of these innovations will take place since business models, products, and services will benefit from the combination of these technologies. Such business models could be widely applied to any autonomous agents such as sensors, cars, machines, trucks, cameras, and other IoT devices. These agents could send and receive money autonomously and leverage AI and data analytics to make decisions as independent economic agents.

Convergence will drive the development of such business models and the digital transformation of industrial corporations. Executives should deal with these technologies in order to realize tremendous efficiency gains. Blockchain technology, combined with IoT and AI, will pave the way to a new age of digitization.

Over the last decade, blockchain technology has improved considerably. Historically, for example, the main critiques about blockchain technology were its limited scalability and inefficiencies. These issues have now been addressed with initiatives such as EOS that can compete with a modern-day transaction system with respect to the conducted transactions per second. However, other challenges remain to be overcome. General Data Protection Regulation's (GDPR) right for data to be forgotten or the integration with legacy systems are examples of such issues. We argue that blockchain technology will again adapt, improve, and address these shortcomings, similar to efficiency and scalability issues.

AUTHOR CONTRIBUTIONS

JG: research about blockchain, IoT and AI and identification of fields of overlapping between these innovations (see sections "Introduction," "Improving Standardization, Privacy, Security, and Scalability of Data," "Automatization Via Smart Contracts," "Conclusion"). PS: discussion of blockchain-based identities, blockchain-based Euro, tokenization of assets (see sections "Authentication via a Blockchain-Based Identity," "Use Case: The Joint Potential of Blockchain, IoT, and AI," "Automatization Via Smart Contracts," "Conclusion"). RR: literature review (first 2 paragraphs of section "The Interconnection Between Blockchain, IoT, and AI"), enhancement of section "Improving Standardization, Privacy, Security, and Scalability of Data" (2nd and 3rd paragraph), use case, enhancement of section "Conclusion" (2nd and 3rd paragraph), and References. All authors contributed to the article and approved the submitted version.

FUNDING

This research and development project was funded by the German Federal Ministry of Education and Research (BMBF) within the funding number 02P17D020 and implemented by the Project Management Agency Karlsruhe (PTKA). The authors are responsible for the content of this publication.

REFERENCES

Barontini, C., and Holden, H. (2019). *Proceeding with Caution-A Survey on Central Bank Digital Currency*. Manek Bhawan: BIS.

CashOnLedger (2020). *CashOnLedger Website - The Payment Engine for the Machine Economy*. Available online at: https://cash-on-ledger.com/ (accessed August 5, 2020).

Diedrich, H. (2016). *Ethereum - Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*. Washington, DC: Wildfire Publishing.

Dorri, A., Kanhere, S., and Jurdak, R. (2017). "Towards an Optimized BlockChain for IoT," in *Proceedings of the IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation* (Piscataway, NJ: IEEE), 173–178.

Es-Samaali, H., Outchakoucht, A., and Leroy, J. P. (2017). A blockchain-based access control for big data. *Int. J. Comput. Netw. Commun. Secur.* 7, 137–147.

Huh, S., Cho, S., and Kim, S. (2017). "Managing IoT devices using blockchain platform," in *Proceedings of the 19th International Conference on Advanced Communication Technology* (Piscataway, NJ: IEEE), 464–467.

International Institute for Sustainable Development (2019). *Tokenization of Infrastructure - A Blockchain-Based Solution to Financing Sustainable Infrastructure*. Available online at: https://www.iisd.org/sites/default/files/publications/tokenization-infrastructure-blockchain-solution.pdf (accessed August 5, 2020).

IoT Analytics (2020). *Industrial AI Market Report 2020-2025*. Available online at: https://iot-analytics.com/product/industrial-ai-market-report-2020--2025/ (accessed July 30, 2020).

Karafiloski, E., and Mishev, A. (2017). "Blockchain solutions for big data challenges: a literature review," in *Proceedings of the IEEE EUROCON 2017 - 17th International Conference on Smart Technologies* (Piscataway, NJ: IEEE), 763–768.

Kumar Singh, S., Rathore, S., and Park, J. H. (2020). BlockIoTIntelligence: a blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Generation Comput. Syst.* 110, 721–743. doi: 10.1016/j.future.2019.09.002

Li, J., Li, N., Peng, J., Cui, H., and Wu, Z. (2019). Energy consumption of cryptocurrency mining: a study of electricity consumption in mining cryptocurrencies. *Energy* 168, 160–168. doi: 10.1016/j.energy.2018.11.046

Liu, M., Yu, R., Teng, Y., Leung, V., and Song, M. (2019). Performance optimization for blockchain-enabled industrial internet of things (IIoT) systems: a deep reinforcement learning approach. *IEEE Trans. Ind. Inform.* 15, 3559–3570. doi: 10.1109/TII.2019.2897805

Monerium (2020). *Monerium Website*. Available online at: https://monerium.com/ (accessed August 5, 2020).

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available online at: https://git.dhimmel.com/bitcoin-whitepaper/ (accessed August 3, 2020).

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies - A Comprehensive Introduction*. Princeton: Princeton University Press.

Roeck, D., Schöneseiffen, F., Greger, M., and Hofmann, E. (2020). "Analyzing the potential of DLT-based applications in smart factories," in *Blockchain and Distributed Ledger Technology Use Cases - Applications and Lessons Learned*, eds H. Treiblmaier and T. Clohessy (Cham: Springer), 245–266.

Salah, K., Rehman, M. H., Nizamuddin, N., and Al-Fuqaha, A. (2019). Blockchain for AI: review and open research challenges. *IEEE Access* 7, 10127–10149. doi: 10.1109/ACCESS.2018.2890507

Sandner, P., Gross, J., Schulden, P., and Grale, L. (2020a). *The Digital Programmable Euro, Libra and CBDC: Implications for European Banks*. Waltham, MA: SSRN.

Sandner, P., Klein, M., and Gross, J. (2020b). *How Will Blockchain Technology Transform the Current Monetary System? Medium, Online*. Available online at: https://medium.com/the-capital/how-will-blockchain-technology-transform-the-current-monetary-system-c729dfe8a82a (accessed August 5, 2020).

Steger, P. (2017). *Blockchain - Die revolutionäre Technologie erklärt. Das System, ihre Anwendungen und Gefahren*. Wrocław: Amazon Fulfillment.

Suliman, A., Husain, Z., Abououf, M., Alblooshi, M., and Salah, K. (2018). Monetization of IoT data using smart contracts. *IET Netw.* 8, 32–37. doi: 10.1049/iet-net.2018.5026

Szabo, N. (1996). Smart contracts: building blocks for digital markets. *EXTROPY J. Transhumanist Thought* 16:18.

Treleaven, P., Gendal Brown, R., and Yang, D. (2017). Blockchain technology in finance. *Computer* 50, 14–17. doi: 10.1109/MC.2017.3571047

Yin, H. H., Langenheldt, K., Harlev, M., Mukkamala, R. R., and Vatrapu, R. (2019). Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain. *J. Manag. Inform. Syst.* 36, 37–73. doi: 10.1080/07421222.2018.1550550

Zheng, P., Zheng, Z., Wu, J., and Dai, H. (2020). XBlock-ETH: extracting and exploring blockchain data from ethereum. *IEEE Open J. Comput. Soc.* 1, 95–106. doi: 10.1109/OJCS.2020.2990458

Zhu, X., and Badr, Y. (2018). Identity management systems for the internet of things: a survey towards blockchain solutions. *Sensors* 18:4215. doi: 10.3390/s18124215

Zyskind, G., Nathan, O., and Pentland, A. (2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. Available online at: https://ieeexplore.ieee.org/abstract/document/7163223 (accessed August 1, 2020).

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.