RS Global Journals

Scholarly Publisher
RS Global Sp. z O.O.
ISNI: 0000 0004 8495 2390

Dolna 17, Warsaw, Poland 00-773
Tel: +48 226 0 227 03
Email: editorial_office@rsglobal.pl

JOURNAL	International Journal of Innovative Technologies in Economy
p-ISSN	2412-8368
e-ISSN	2414-1305
PUBLISHER	RS Global Sp. z O.O., Poland

ARTICLE TITLE	ARTIFICIAL INTELLIGENCE IN BLOCKCHAIN-PROVIDE DIGITAL TECHNOLOGY
AUTHOR(S)	Dziatkovskii Anton.
ARTICLE INFO	Dziatkovskii Anton. (2022) Artificial Intelligence in Blockchain-Provide Digital Technology. *International Journal of Innovative Technologies in Economy*. 4(40). doi: 10.31435/rsglobal_ijite/30122022/7931
DOI	https://doi.org/10.31435/rsglobal_ijite/30122022/7931
RECEIVED	07 December 2022
ACCEPTED	29 December 2022
PUBLISHED	30 December 2022
LICENSE	This work is licensed under a **Creative Commons Attribution 4.0 International License.**

ARTIFICIAL INTELLIGENCE IN BLOCKCHAIN-PROVIDE DIGITAL TECHNOLOGY

Dziatkovskii Anton
Blockchain Technology and Data Science specialist, Platinum Software Development Company, Australia

DOI: https://doi.org/10.31435/rsglobal_ijite/30122022/7931

ARTICLE INFO

Received 07 December 2022
Accepted 29 December 2022
Published 30 December 2022

KEYWORDS

Artificial Intelligence, AI, Blockchain, Technology, Digital.

ABSTRACT

Artificial intelligence technologies, today, are rapidly developing and are an important branch of Computer Science. Artificial intelligence is at the heart of research and development of theory, methods, technologies, and applications for modeling and expanding human intelligence.

Artificial intelligence technology has three key aspects, namely data, algorithm, and computing power, in the sense that training an algorithm to produce a classification model requires significant data, and the learning process requires improved computing capabilities. In the age of big data, information can come from a variety of sources (such as sensor systems, Internet of Things (IoT) devices and systems, as well as social media platforms) and/or belong to different stakeholders. This mostly leads to a number of problems.

One of the key problems is isolated data Islands, where data from a single source/stakeholder is not available to other parties or training an artificial intelligence model, or it is financially difficult or impractical to collect a large amount of distributed data for Centralized Processing and training. There is also a risk of becoming a single point of failure in centralized architectures, which can lead to data intrusion.

In addition, data from different sources may be unstructured and differ in quality, and it may also be difficult to determine the source and validity of the data. There is also a risk of invalid or malicious data. All these restrictions may affect the accuracy of the forecast.

In practice, artificial intelligence models are created, trained, and used by various subjects. The learning process is not transparent to users, and users may not fully trust the model they are using. In addition, as artificial intelligence algorithms become more complex, it is difficult for people to understand how the result of training is obtained. So, recently there has been a tendency to move away from centralized approaches to artificial intelligence to decentralized ones.

Citation: Dziatkovskii Anton. (2022) Artificial Intelligence in Blockchain-Provide Digital Technology. *International Journal of Innovative Technologies in Economy.* 4(40). doi: 10.31435/rsglobal_ijite/30122022/7931

Introduction.

Compared to artificial intelligence, blockchain is a relatively young technology, which was first offered in 2008 (Abbassi, 2021). Blockchain, a peer-to-peer distributed system that provides reliable protection with a basic hashing algorithm and timestamping technology. The confidentiality of the data stored in the blockchain is guaranteed by the use of certain cryptographic algorithms. The use of smart contracts allows the program to run automatically to ensure the reliability of the execution results. Thanks to the consensus mechanism and distributed registration technology, all nodes can participate in financial transactions and verify transactions.

The architecture of the blockchain consists of a certain set of levels, each of which has blocks in its composition.

The data layer is mainly focused on the data structure, including a hash function, digital signature, Merkla Tree 1, asymmetric encryption and other technologies. The most important structure of each data layer is a block. A block consists of both a block head and a body. The block title contains the Merkle root, the timestamp, and the hash values of the current and previous blocks.

Every day, an energy company can receive a huge amount of data about its energy production and consumption by users. With qualitative analysis, these data can point companies to both problem areas and development vectors.

With serious production volumes and millions of consumers, such analysis is difficult to conduct without the involvement of artificial intelligence. Well-designed software based on it helps you collect and analyze data, track trends, and find problems.

Artificial intelligence can also help optimize production, reduce waste, and make services more cost-effective. This is a tool that can make both energy production and consumption efficient.

If we talk about the connection between artificial intelligence and blockchain in the context of cryptocurrency trading, then AI has also found application here. Probably, many of you have heard about trading bots that can make deals instead of users according to the specified settings. This technology, of course, significantly saves the Trader time and allows you to trade simultaneously on several exchanges (Salman, 2019).

What are the advantages and potential opportunities of the tandem of artificial intelligence and blockchain?

- AI transparency. If artificial intelligence components such as data and algorithms are placed on the blockchain in the public domain, this will indicate the transparency and integrity of AI, thereby increasing trust in it. In addition, if all the “thought processes” of artificial intelligence are registered in data chains, they will be easier to track and understand logic.
- Data protection.
- Data trading.
- Sale of computing power.
- Optimization of the blockchain operation.
- A combination of privacy and personalization.

Materials and methods.

A smart contract is a kind of computer protocol that can be independently executed, self-applied, self-tested, and self-restricted in the execution of its instructions. This allows transactions between untrusted or anonymous parties without the need to involve a trusted third party. These operations are traceable and irreversible. A smart contract consists of cost, address, function, and status. The transaction is accepted as input, the corresponding code is executed, and the output event is triggered; the status then changes according to the function logic (Abenugba, 2019).

All parties negotiate in advance the details of the smart contract, including the scenarios that trigger the execution of the contract, the rules for the transition of status and liability for violation of the contract. The smart contract is then provided in the form of code in the blockchain. As soon as the requirements are met, the smart contract is started and executed automatically (Battineni, 2020).

Ethereum is the most popular platform for the development of smart contracts. The Ethereum Smart Contract Code is written in the stack-based bytecode language and is executed on the Ethereum Virtual Machine. Chain code is usually developed using Go or Java.

The consensus mechanism works on a blockchain basis to coordinate all nodes and blocks. If there is no communication between each node on the blockchain, it is necessary to coordinate each independent node to exchange information on such a network. The network system therefore decides who will be the next payer by using the appropriate protocols to achieve equilibrium via the consensus mechanism (Cao, 2018).

Blockchain and AI can have many common ground for joint application in different areas, and some projects have already seriously taken up the implementation of this idea.

Bext360. the project decided to implement blockchain and artificial intelligence technologies in coffee supply chains. AI adapts the process of growing coffee beans to weather conditions and determines their quality. Data obtained at each stage of the supply chain is stored on the blockchain, where it cannot be changed or hacked. This way, the entire coffee path is tracked and properly controlled (Wirth, 2018).

BurstIQ. The company has released the Service “Health Wallet", focused on the healthcare sector. it is used as a network for exchanging data on the health of users and their treatment. Patients can provide access to this data to medical professionals to study certain diseases and treatment methods.

Blackbird.AI the project uses a combination of two technologies to combat fake news and hate speech. The AI verifies the veracity of information and sorts it into categories, and the already verified content is stored on the blockchain.

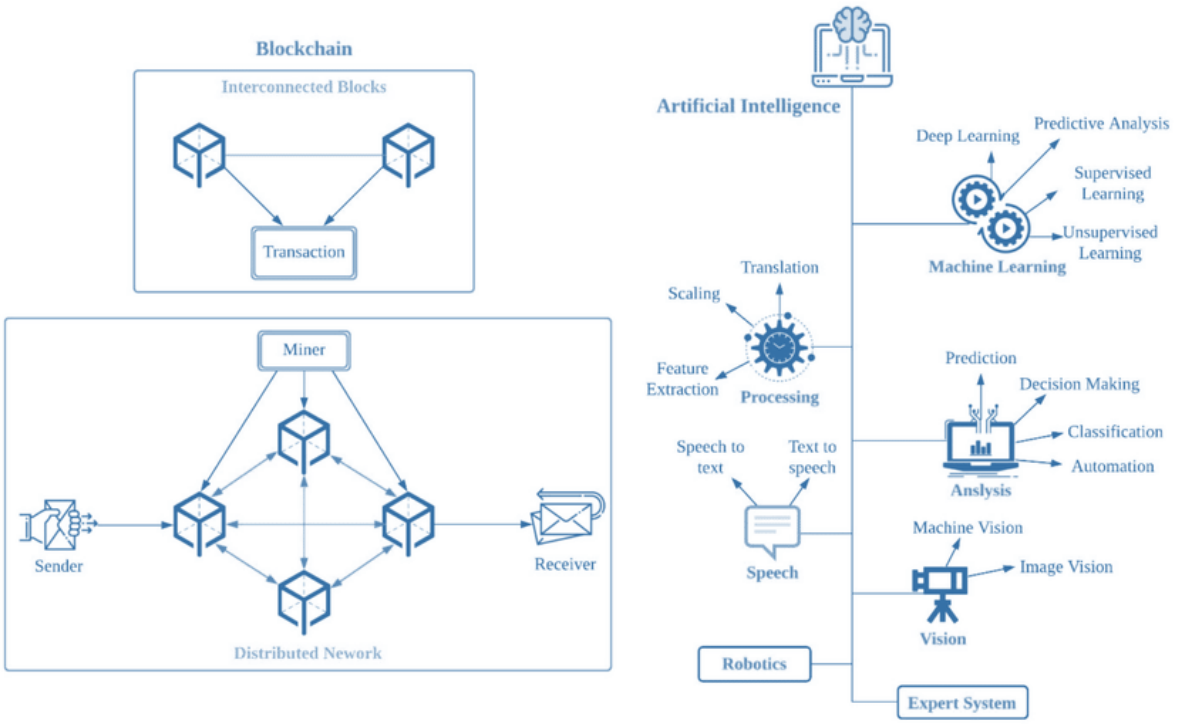

Fig. 1. Artificial intelligence structure in blockchain
Source: author’s own research

In general, the blockchain can be divided into three types, depending on the access level of the blockchain data: public blockchain, private blockchain and consortium blockchain (Yang, 2021).

Public Blockchain. All records stored in a public blockchain are open and transparent to everyone, and all nodes can freely join and leave the blockchain network. Anyone can check the transaction and fight for accounting rights. Bitcoin and Ethereum are public blockchains.

Artificial intelligence is one of the most promising areas of computer science that studies methods for solving problems for which there are no solutions. Artificial intelligence systems have capabilities like human intelligence in planning, learning, solving logical tasks, as well as social skills and creativity. There are developments for cars without drivers, robots-couriers, but at the same time there is a growing concern (Meng, 2018).

With the use of blockchain, artificial intelligence could reach a new level of innovation scale, and all artificial intelligence solutions will become more transparent, understandable and trustworthy.

Artificial intelligence is developing thanks to huge amounts of data that are potentially available to researchers, developers, and merchants. Data is the value of the digital economy, but there is no access to it through barriers of trust.

Machine learning can usually be divided into learning with a teacher, learning with reinforcement, and learning without a teacher. Learning with the teacher uses the specified data to train the model that will be used for the prediction. The nearest neighbor, the decision tree, the neural network and the SVM are learning algorithms with the teacher. Lessons without a teacher uses a set of learning data without a label. The key to learning without a teacher is to analyze the hidden data structure and find out if there is a separation theorem. Training reinforcement combines teacher-to-

teacher learning and teacher-to-teacher teaching by using a lot of named data and large amounts of data for learning and classification.

Machine learning requires a large amount of sensitive data, and data confidentiality is a very important issue. At the same time, the data is distributed among different organizations. These decentralized data are generally heterogeneous and unbalanced, so it is difficult to combine them. Google first offered model learning, which combines machine learning with distributed computing, in 2016.

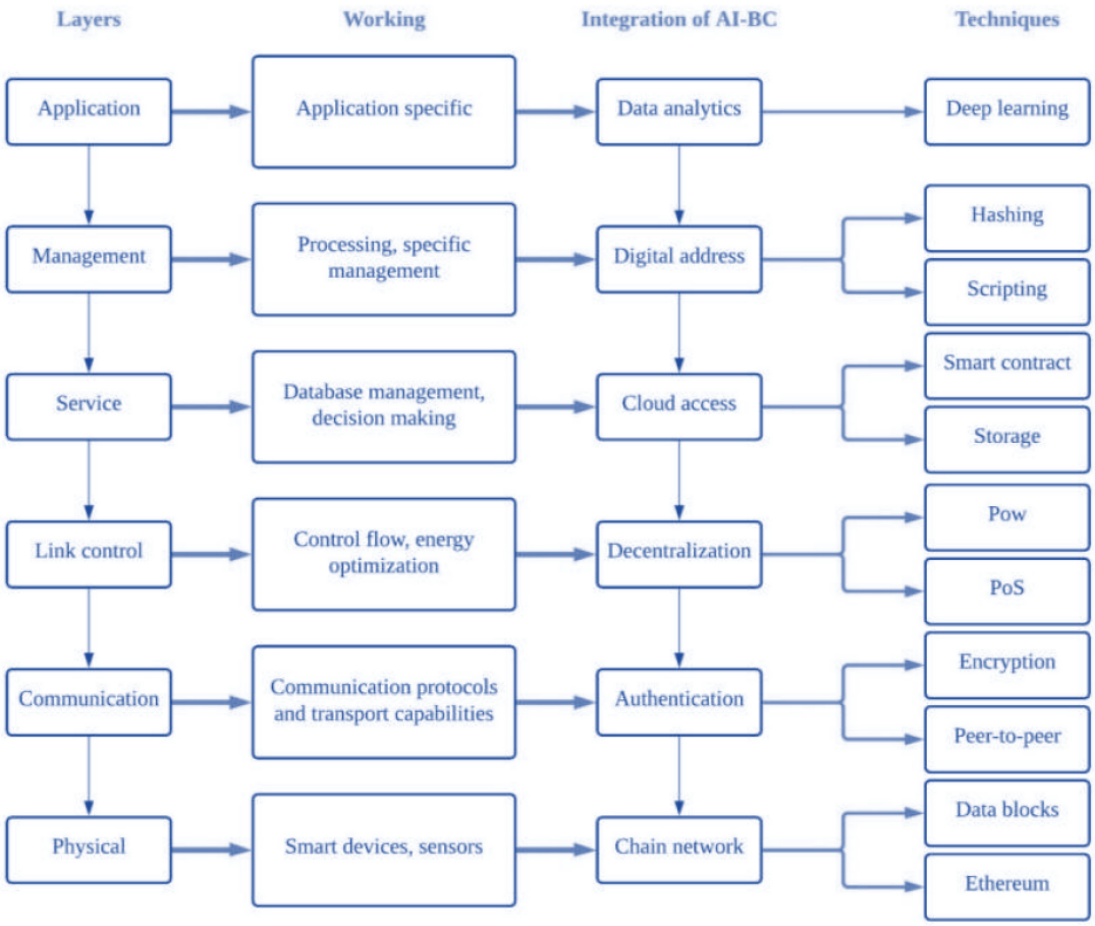

Fig. 2. Integration AI to blockchain
Source: IBM research 2021 of blockchain, ibm.com

They will then upload the updated parameters to the coordinator, which merges the local submodel into the combined Model. In model training, participants only need to share their own parameters of the training model, and they do not need to send source data, which can protect data privacy to some extent (Namasudra, 2020).

It can be concluded that blockchain, first of all, is a tool for solving issues of security, reliability and transparency of transactions, so its use in various areas of business activity is gaining momentum. Given the challenges of developing blockchain applications, it is necessary to continue developing the technology in the direction of standardization, application security and integration of blockchain systems with other modern technologies.

Standardization of blockchain technology is an important step towards a single conceptual framework, interoperability, scaling, auditing, and possible further regulation of the technology. That is why in 2016 the International Organization for Standardization (ISO – International Organization for Standardization) formed a committee to develop a standard for blockchain technology and began working on the international standard ISO/TC 307 – Blockchain and distributed ledger technologies (blockchain and distributed ledger technologies).

It is also necessary to take a systematic approach to the security of blockchain applications. Serious research is needed in this direction. Today, there is not much practical experience in using

blockchain systems. The only network that works for a long time without significant failures is the Bitcoin blockchain. The problems associated with the Bitcoin network were due to the hacking of services built on top of the blockchain. Also, an attack was successfully performed on the Ethereum Network (Salman, 2019).

The blockchain keeps records of values in real time. Soon, billions of "smart" things will interact with each other, so the Internet of Things (IoT) needs blockchain technology. Nowadays, there is a growing need to perform operations with large data flows. Blockchain technology allows you to identify and organize bigdata databases that relate to various business areas. At the same time, the process of drawing up schedules, systematizing information, and recording resource movements in the course of the company's activities is simplified.

Companies that use blockchain solutions can be sure of the security and safety of all data, its compliance with legal requirements. Such solutions allow you to store information and records with data in the form of blockchains, making a timestamp. At this stage, projects are considered (for example, Woroom.network) for building a network that combines blockchain, artificial intelligence, big data, and IoT technologies.

AI with blockchain technology in justice.

Blockchain technology is an information system that provides data storage with protection from falsification and loss, as well as data transfer and transformation within the system while maintaining their reliability. Data protection is achieved by: writing it to a chain of cryptographic interconnected blocks, decentralized storage of copies of chains, and synchronization of chains using an algorithm. That is, the blockchain is also called the block chain itself. By its design, the blockchain can serve as an open distributed system that records transactions between two parties in a controlled and permanent way.

While performing various operations, a new code is generated in the system of interconnected blocks, which is embedded in the existing chain.

This means that in the case of, for example, a hacker attack or unauthorized access to electronic materials of a court case, the chain is not destroyed, but simply rejects this element. This" rejection " indicates that this block is incorrect and contains attempts to hack the system, which indicates a very high level of system security and reliability of the entered information.

Advances in technology can be used to improve, refine, and optimize our traditional ways of working in courts. Most judges and lawyers, when they think about technology, think about routine, repetitive and often outdated methods of performing tasks in courts and imagine that thanks to modern information technologies, it is possible to increase efficiency and make life easier (van Klompenburg, 2020). So, since 2018, Internet courts in Beijing and Guangzhou have been online filing documents, presenting evidence (using blockchain to confirm the authenticity of evidence), judicial proceedings and making decisions (van Klompenburg, 2020).

Over the past five years, Chinese courts have become world leaders in their efforts to implement automated court analysis and monitoring, standardize decision-making, and monitor trends in society (Wang, 2019).

In this regard, the people's Republic of China is actively introducing innovative information and telecommunications technologies in the dispute resolution process. Thus, in China, the judicial system has adopted the thinking of a technology company and is rapidly promoting the use of electronic technologies in court proceedings.

Chinese courts across the country have begun working with giant tech companies to create their own blockchain platforms, including the "judicial blockchain" in Hangzhou (September 2018), the "balance Chain" in Beijing (March 2019), and the "Internet Legal Chain" in Guangzhou (April 2019). In November 2019, it announced its own blockchain platform for storing electronic files, the "unified platform of the judicial blockchain of the people's Court", which is aimed at covering jurisdictions throughout the country (Yazdinejad, 2020).

All judicial blockchain platforms in China are united by a blockchain, where objects can become members (nodes) of the network only after prior approval of their host, as opposed to a fully decentralized public blockchain system (for example, the Bitcoin blockchain and the Ethereum blockchain), which is open to all. Blockchain technologies currently has 27 participants, including 21 representative courts from different regions at all levels (from local courts to city-level courts, regional

courts) and other legal entities, such as notary offices and forensic centers. Each of these members contains an electronic copy of the blockchain and is equipped with high-speed servers, storage devices, and a dedicated internal LAN. All participants apply the same rules for entering, storing, and retrieving electronic evidence to preserve only reliable and fixed data. The collaborative technology company provides mission-critical technologies such as electronic signatures, location and time tags, and data encryption and decryption. End-user portals, such as smartphone apps and websites, allow anyone to host electronic files (Yazdinejad, 2020).

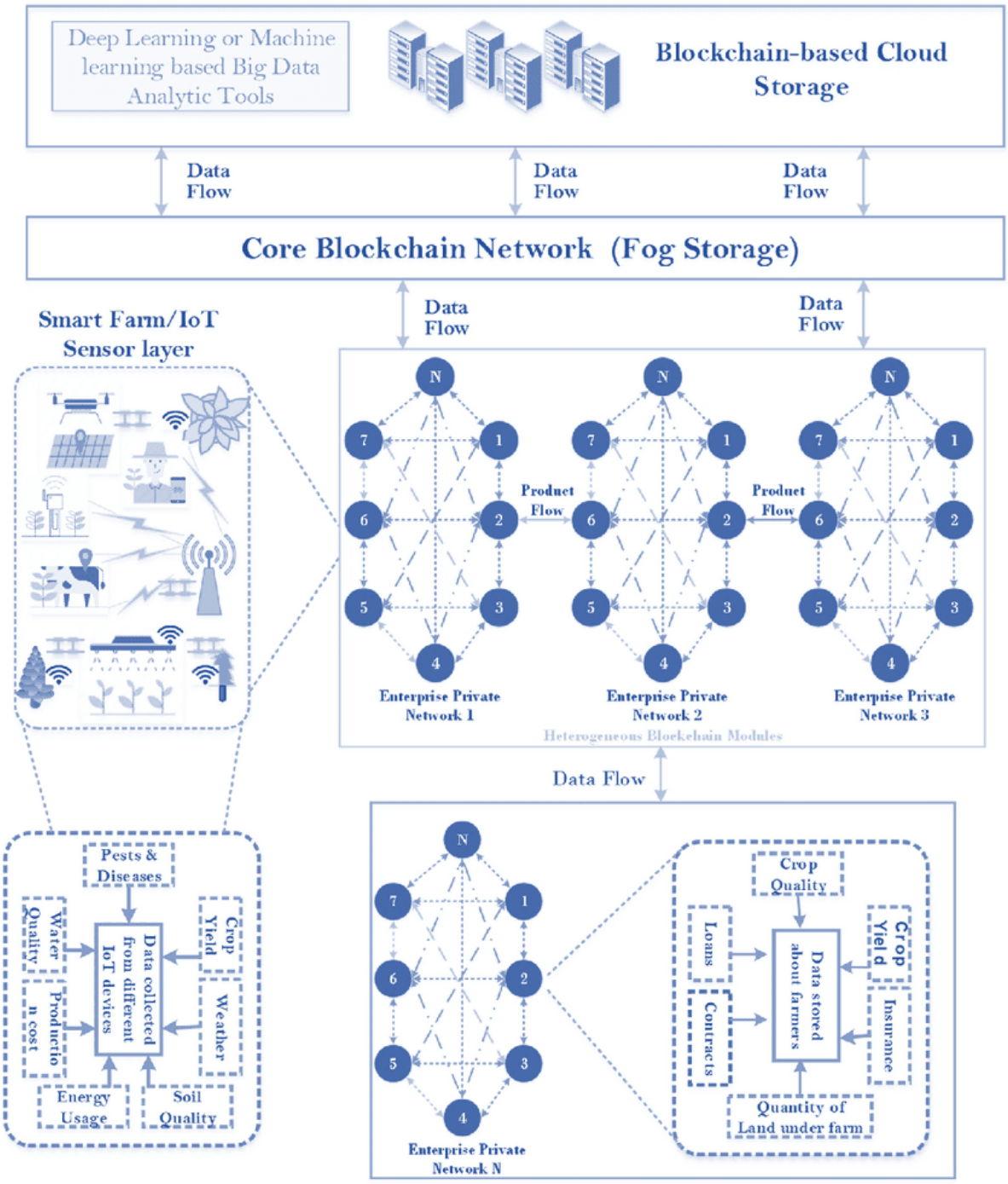

Fig. 3. Blockchain AI cloud in justice
Source: Justchain.us

Thus, the example of China highlights the relationship between the centralization of power and the growing state interest in solving court cases of minor complexity using artificial intelligence

algorithms that are considered reliable and impartial. And blockchain technology allows China's judicial system to be protected.

The development of digital information technologies has a sufficient impact on the civil process in Estonia. This is how the Unified Judicial Information and communication system operates in the courts today.

Claims and other applications, complaints and other procedural documents provided for by law, submitted to the court and may be the subject of judicial proceedings, in the order of their receipt, are subject to mandatory registration in the Unified Judicial Information and communication system on the day of receipt of the documents.

The Unified Judicial Information and communication system, in accordance with the law, provides the exchange of documents (sending and receiving documents) in electronic form between courts, between the court and participants in the trial, between participants in the trial, as well as recording the trial and participation of participants in the trial in the court session via videoconference (Zhang, 2019).

In accordance with the existing requirements, an application to the court for protection of their violated, unrecognized or disputed rights, freedoms or legitimate interests can be in the form of a submitted electronic document signed with a Qualified Electronic Signature through the electronic cabinet of the "electronic court" subsystem.

After consideration of the court case, the court decision is entered in the Unified State Register of court decisions in the form of an electronic document, which is signed by the judge (judges, if the judicial act was adopted by the court collectively) also with a Qualified Electronic Signature. The process of conducting electronic court records management, processing incoming documents, sending electronic court summonses to participants in the case is a complex system that includes a set of heterogeneous data processed using information systems, where at different stages of their processing there is a human factor that significantly affects the reliability, legality and irreversibility of actions.

With the help of blockchain technology, the parties and other participants in the process can see in their personal electronic cabinet of the electronic court not only all the procedural documents that the court registers – both on the part of the plaintiff and on the part of the defendant – the opposite party, but also all the procedural documents of the court – these are both rulings and court decisions, especially when the court announced only the introductory and operative part of the decision, and the full text was announced later, and when someone was not present at the court session or did not wait for its proclamation, for example, due to a break in court or the next day in the morning.

A set of different data sources and electronic documents and the participation of various parties in the processes place high demands on the quality of information. That is why the proposed approach to the use of blockchain technology will allow creating a secure information judicial system.

An important advantage of data storage when using blockchain technology is high reliability, which eliminates the possibility of loss or destruction. And the use of modern certified cryptographic protection algorithms will give legal significance to the electronic data of the civil process.

It is obvious that many more intellectual, material, financial, and time costs are needed before innovative proposals are implemented in the practical activities of the Estonian judicial system. However, it is quite clear that the Estonian judicial process in general, and the civil process, must meet modern realities, and the implementation of the latest information and communication technologies in its activities is a vital necessity.

Blockchain in telemedicine.

With the growing popularity of blockchain, more and more scientists and developers are researching and offering their own solutions in various spheres of life, as well as analyzing the feasibility of implementing such projects and how this will affect people's perception of such systems (Ensor, 2019).

Such materials confirm that blockchain technology has both advantages, including decentralization, transparency of operations, independence, but at the same time it has its drawbacks - such as trust in product developers, problems with ensuring anonymity and easy access for all users in the real world. And, since telemedicine as such, there are many problems that have plagued it since the very beginning of the industry - such as increased reception time due to long communication, the

possibility of data loss due to unreliable transmission channels and storage locations, and other data problems.

Many of the problems that the telemedicine industry faces are solved using blockchain technology, so there are enough medical projects in the medical field, so it makes sense to consider some of them to determine their advantages to determine how they were achieved in projects, and disadvantages to assess the possibilities of avoiding them in our project.

MedRec.

MedRec is a simple distributed system for personal control of the identification and distribution of personal information (Faroukhi, 2020). The project was implemented in the context of a Distributed Health Information System, where patients retain control over who has access to their data. MedRec creates a network of reliable data warehouses, access to which is determined by a set of smart contracts. These contracts are stored in the distributed ledger of those who generate the data.

The distributed nature of the system allows unified access from various sources to a single application without intermediaries. This increases patient control while maintaining the confidentiality of both the content of the data and its source. MedRec lends itself to extensions for decentralized messaging and information distribution to third-party applications of medical researchers, representatives, and other institutions. The system is based on a blockchain containing smart contracts that define users and the specifics of their distribution.

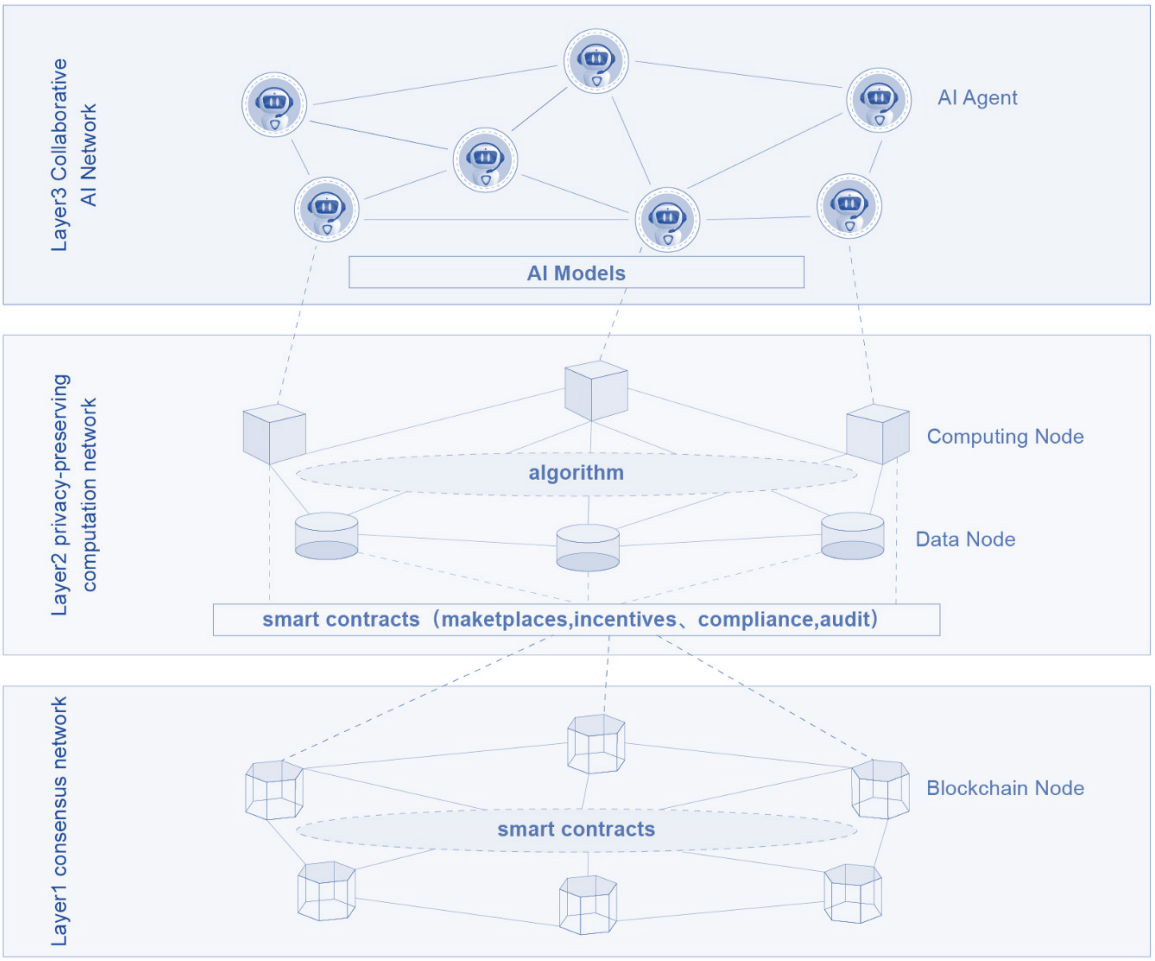

Fig. 4. AI network-models in blockchain
Source: Degruyter.com

The MedRec architecture is easy to understand by analogy with the World Wide Web. The web consists of three elements: an HTTP server that provides access to local data, HTML, the language used to define web elements, and a browser that forms the interface. Ideally, anyone can be a

server, and web browsers can render the interface from multiple servers at once to create a presentation. The World Wide Web is a network by design more than a client-server architecture, even though in practice the dominant component is servers. In MedRec, the analog of the HTML language is smart contracts that determine which entities or parties will have access to records. These contracts are managed using the blockchain, which is a component like a web server. Contracts are unnecessarily stored by every site that supports the blockchain. Unlike the web, MedRec servers, which provide access to data and provide data based on contracts, are interconnected, and support the blockchain protocol. These servers are also administrative members of the network. Each object in the system has a unique identifier that identifies each of them.

The system works by combining four components:

- A PC app that allows patients to access their data and determine who has the right to view it
- A daemon that interacts with the provider's databases and the underlying file system.
- Ethereum clients that connect to each other to form a MedRec network.
- Ethereum blockchain, which is used to manage access rights to medical records.

Basically, patients create access contracts that are stored on the blockchain. These contracts indicate to providers who can be given information about a particular medical record.

MedRec uses a proof-of-authority blockchain as part of the go-Ethereum client. Data stored on the blockchain can still be open for reading outside of the set of nodes that support the blockchain. Medical professionals become authorized if they have a specific set of nodes. Authorized employees can create blocks and add them to the blockchain. Since the identification signs are known for all providers, the regulation may be external, relative to the blockchain.

The penalty for abuse of their rights is provided in the form of withdrawal of rights to work with records in the chain. Since each transaction is public, each of the providers can verify the data. This is how providers are encouraged not to generate fraudulent data, because all such actions can be very easily detected by any of the participants. In addition, the type of attacks on the system by vendors ' services is limited, because their only responsibility is to confirm transactions. Vendors do not have the ability to pretend to be participants in the system, as they do not have their respective private keys.

The blockchain requires all maintainers to store the entire blockchain chain and refer to its full version. This project implements restrictions on the so-called" small set": a set of administrative permissions and smart contracts that are needed to check agents and determine relationships.

Each patient must store a specific piece of data from the chain. They perform 9727-byte transactions to create a contract with the agent. Each interaction with the patient and provider then requires a 5007-byte transaction. Contract updates require 220 bytes. You can estimate how many bytes each node should store.

If we assume that the number of users will be 50 million, each of which has relationships with 5 different providers, then the size of the entire blockchain will not exceed a terabyte, and in the case of a smaller number of users, the size will be much smaller. If you compare the amount of data that is constantly transmitted between hospitals an excessive number of times, then the size of the MedRec blockchain is a small price to pay for the reliability of the system.

Even with a decentralized network, the blockchain also has a centralized part in the form of launch nodes. A startup Node is a network node that aims to connect a new user to a network of existing nodes in the network. They are similar in nature and purpose to DNS servers and BitTorrent trackers. These nodes are registered in advance in the MedRec client system. When the MedRec system is running, they must be installed by at least several well-known public health providers. only one of them must be harmless for a new user to be able to join the network.

Earlier research on Bitcoin and Ethereum analyzed the practicality of an attacker taking control of a node's connection to the rest of the network. Attacks of this type are called eclipse attacks. If the victim thinks that she is connected to the network, all peer connections from the victim's node go directly to the hacker who can manipulate interactions with the blockchain.

The use of a PoA-type blockchain adds another mechanism to prevent such attacks. One way is for all nodes to always maintain an open connection to at least one ISP node. The current set of provider nodes can be rigidly configured for each version of MedRec that uses startup nodes.

A side effect of using a single smart contract for a patient is that anyone can link real patient data to an Ethereum address and can identify all the healthcare providers that the patient has dealt with.

The case when this would be harmful is when, for example, the patient shares data with the employer for health insurance and other doctors, and in some cases the employer can use this to dismiss the employee to avoid insurance payments or other obligations to the employee.

The MedRec project solved this in two stages. The first step is to separate the patient and provider IDs. Each provider creates a new Ethereum account for each provider.

These accounts are called Patient-Centered delegate accounts. This method allows patients to have a relationship with the provider without the possibility of disclosing them. Even when the patient interacts with the provider through such a delegate account, the provider's primary account is still used to provide the patient with the ether needed for transactions.

Therefore, instead of meeting the patient's request directly, the provider asks the delegate account to meet the request, thus masking the patient's actual relationships.

The MedRec app is essentially a wallet containing their Ethereum private key. The app is designed to support multiple accounts, multiple users can use the same hardware without compromising the protection of other users. The patient has three pages that display their medical information. One displays information that may change over time, according to the contract. The other displays contract-specific information.

MedRec provides recovery of the user's private key using a standard that was first developed for Bitcoin, which is used in several blockchain wallets (such as Metamask and MyEtherWallet).

A private key view is created when an account is created. The private key will consist of 12 words, this key will be the only thing that the patient will need to access their medical information. However, this key must not be disclosed or lost, although if you lose the key, you can always create a new account. The project is written in the javascript programming language and the react library in combination with the electron framework, which allows you to create applications for desktop PCs, with which you can easily adapt the application for mobile devices (Feng, 2019).

When the patient logs in to the app, the data is retrieved and visualized in the interface. Then by polling through the RPC interface of the provider, each of which is digitally signed with the patient's Ethereum address. This signature is decrypted by the database manager and identifies the patient by their Ethereum address. The key / value data structure means that you don't need to store additional information about the patient, because their address is directly mapped to the ID in the database.

The block structure looks like a Merkle tree. The nodes on the leaves of this tree reflect the transactions of working with patient records and describe adding the resource to the official patient record. However, transactions do not include the document itself, which is added to the transaction. Instead, they link to the corresponding FHIR standard resource using a URL (Uniform Resource Locator - a unique link identifier). This allows institutions to maintain operational control over their data, but, importantly, keeps sensitive patient data out of the blockchain. FHIR was chosen as an exchange format not only because it is a new standard, but also because it contains allows for originality checks and audits, making it suitable for use as ledger entries, which can be useful for many health organizations. FHIR in combination with blockchain can serve as a guarantee of maintaining the integrity and context of transactions.

The transaction has the following structure:

- Hash: SHA256 hash from the transaction payload. Although the resource itself is not stored in the blockchain, its contents can be verified using this hash upon receipt.
- Participant signature: digital signature of the transaction initiator node.
- FHIR URL: link to the actual location of the FHIR resource
- FHIR profile: the URI of the FHIR profile that this resource corresponds to.
- Security Index: an encrypted index that allows you to search for information without opening the contents of the information itself.

Hashes of all transactions in a block become part of the Merkle hash, the block header. The block header contains the following information, which is used to validate the next block:

- Hash: hash of the SHA256 block. Assume that the block header has two children c0 and C1, and the previous block bn-1. then the hash of bn corresponds to the combined hash of all hashes bn-1, c0, and C1.
- Hash of the previous block: hash of the previous block for validation purposes.
- Participant signatures: each participant who has entered a block must have a digital signature. This block ensures its validity after it has been collected by miners.

- List of miners: each node that provided a transaction for the block must provide a random number encrypted with its private key.

In the proposed system, which is very similar to the Bitcoin system, each new block is added to the system at fixed intervals. For Bitcoin, this interval is determined by the complexity of the POW function. For the proposed network, the developers set a fixed time for creating a block, the so-called block period. During this block period, the network goes through four stages of activity. First, during the transaction distribution phase, which starts at time Ta, transactions are sent to the coordination or so-called mining node (Hassan, 2019).

This phase continues until the TD time when the mining node stops accepting new transactions to form a block. Then the miner node collects all new blocks received during this time and sends them for verification at the "block validation" stage. This allows all nodes that have made at least one transaction to a block to digitally sign this block, which will confirm its authenticity. The block is then returned to the mining node, in the "return signed block" stage. After that, the mining node adds a block to its local blockchain and distributes the new blockchain in the last stage of the "new blockchain distribution" algorithm.

Conclusions.

The paper reveals the principles of applying artificial intelligence and Internet of things technology in the blockchain system. Various characteristics of the blockchain that can be used to support data exchange, maintain confidentiality, and make trusted decisions of artificial and decentralized intelligence are described. As a decentralized platform, blockchain allows data owners and data users to share data peer-to-peer. Because blockchain is transparent and immutable, it can minimize the potential for cybercrime in distributed data exchange or transactions. In addition, the basic cryptographic algorithms (hashing algorithms, homomorphic encryption, threshold encryption, etc.) used to process data stored on the blockchain help ensure the confidentiality, integrity, and reliability of sensitive data. Using smart contracts to automate Model creation, training, data exchange, decision-making, and tracking on the blockchain helps ensure the reliability of decision-making results.

REFERENCES

1. Abbasi, M. A., Memon, Z. A., Durrani, N. M., Haider, W., Laeeq, K., and Mallah, G. A. (2021). A Multi-Layer Trust-Based Middleware Framework for Handling Interoperability Issues in Heterogeneous IOTs. Clust. Comput. 24, 2133–2160. doi:10.1007/s10586-021-03243-1
2. Adenugba, F., Misra, S., Misra, S., Maskeliūnas, R., Damaševičius, R., and Kazanavičius, E. (2019). Smart Irrigation System for Environmental Sustainability in Africa: An Internet of Everything (IoE) Approach. Math. Biosci. Eng. 16 (5), 5490–5503. doi:10.3934/mbe.2019273
3. Battineni, G., Sagaro, G. G., and Chinatalapudi, N. (2020). Applications of Machine Learning Predictive Models in the Chronic Disease Diagnosis. J. Pers. Med. 10, 21. doi:10.3390/jpm10020021
4. Cao, J., Zhang, Q., and Shi, W. (2018). Edge Computing: A Primer," in SpringerBriefs in Computer Science, Berlin/Heidelberg, Germany: Springer. doi:10.1007/978-3-030-02083-5_1
5. Ensor, A., Schefer-Wenzl, S., and Miladinovic, I. (2019). "Blockchains for IoT Payments: A Survey," in 2018 IEEE Globecom Work GC Wkshps (IEEE).
6. Faroukhi, A. Z., El Alaoui, I., Gahi, Y., and Amine, A. (2020). A Multi-Layer Big Data Value Chain Approach for Security Issues. Procedia Comput. Sci. 175, 737–744. doi:10.1016/j.procs.2020.07.109
7. Feng, Q., He, D., Zeadally, S., Khan, M. K., and Kumar, N. (2019). A Survey on Privacy Protection in Blockchain System. J. Netw. Comput. Appl. 126, 45–58. doi:10.1016/j.jnca.2018.10.020
8. Hassan, M. U., Rehmani, M. H., and Chen, J. (2019). Privacy Preservation in Blockchain Based IoT Systems: Integration Issues, Prospects, Challenges, and Future Research Directions. Future Gener. Comput. Syst. 97, 512–529. doi:10.1016/j.future.2019.02.060
9. Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., and Han, J. (2018). When Intrusion Detection Meets Blockchain Technology: A Review. IEEE Access 6, 10179–10188. doi:10.1109/access.2018.2799854
10. Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R., and Shanthini, A. (2020). Towards DNA Based Data Security in the Cloud Computing Environment. Comput. Commun. 151, 539–547. doi:10.1016/j.comcom.2019.12.041
11. Salman, T., Zolanvari, M., Erbad, A., Jain, R., and Samaka, M. (2019). Security Services Using Blockchains: A State of the Art Survey. IEEE Commun. Surv. Tutorials 21 (1), 858–880. doi:10.1109/comst.2018.2863956

12. van Klompenburg, T., Kassahun, A., and Catal, C. (2020). Crop Yield Prediction Using Machine Learning: A Systematic Literature Review. Comput. Electron. Agric. 177, 105709. doi:10.1016/j.compag.2020.105709
13. Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., and Wang, F-Y. (2019). Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. IEEE Trans. Syst. Man. Cybern. Syst. 49, 2266–2277. doi:10.1109/tsmc.2019.2895123
14. Wirth, C., and Kolain, M. (2018). "Privacy by BlockChain Design: A Blockchain-Enabled GDPR-Compliant Approach for Handling Personal Data," in ERCIM-Blockchain 2018: Blockchain Engineering - Challenges and Opportunities for Computer Science Research.
15. Yang, R., and Yu, Y. (2021). Artificial Convolutional Neural Network in Object Detection and Semantic Segmentation for Medical Imaging Analysis. Front. Oncol. 11, 1–9. doi:10.3389/fonc.2021.638182
16. Yazdinejad, A., Parizi, R. M., Dehghantanha, A., Srivastava, G., and Aledhari, M. (2020). Enabling Drones in the Internet of Things with Decentralized Blockchain-Based Security. IEEE Internet Things J. 8 (8), 6406.
17. Zhang, M., Li, L., Wang, H., Liu, Y., Qin, H., and Zhao, W. (2019). Optimized Compression for Implementing Convolutional Neural Networks on FPGA. Electronics 8, 295. doi:10.3390/electronics8030295