BLOCKCHAINS: PRACTICAL APPROACHES

Irina Radeva

Institute of Information and Communication Technologies,
Bulgarian Academy of Sciences,
Acad. Georgy Bonchev Str., Bl. 2, 1113 Sofia,
e-mail: irina.radeva@iict.bas.bg

Abstract. Originally proposed for Bitcoin, Ethereum and other digital currencies, blockchain technology is now the most innovative framework for decentralized data management. This technology has not yet revealed its full potential to transform all economic and social processes. Its characteristics, interpreted and implemented in practice, are about to have their revolutionary impact on the possibilities for safe, fair and objective digitalization of the physical environment. The purpose of this paper is to present some general and specific aspects in research on applications of blockchain technology in intelligent agriculture. The main elements of the technology, popular definitions, focus areas in risk management concepts and the implications for internal audit and control procedures in companies that adopting blockchain in intelligent agriculture are briefly discussed. In summary, an algorithm for selecting of blockchain platforms and an algorithm for text mining in the domain of plant genetic resources are presented. A blockchain-based approach to modelling a supply chain in smart crop production is proposed, which is illustrated with a conceptual example of blockchain architecture and smart contract functions design. The future development of this study will focus on detailed analysis of existing blockchain standards, improving descriptions of functional levels in the supply chain network model and blockchain architecture design.

Keywords: blockchain, blockchain based supply chain modelling, smart contracts, smart crop production, NISTIR 8202, ISO 22739, FG DLT D1.1.

1. INTRODUCTION

Originally proposed for Bitcoin, Ethereum and other digital currencies, blockchain technology is now the most innovative framework for decentralized data management. The technology is becoming a key infrastructure component that integrates the digital, biological and physical elements of the economy. In the recent past, the Internet allowed users to share documents and

DOI: 10.7546/EngSci.LIX.22.01.01

information. Today, blockchain is a reasonably enough reliable network for exchange of digital assets and associated with them exchangeable value. Beyond the finance sector, blockchain technology attracts interest in applications in various industrial sectors ranging from entertainment, insurance, voting systems, logistics and transportation, supply chains, healthcare, information management, retail, power supply, etc.

However, despite the high expectations, there are currently few ideas about where and how blockchains could be effectively applicable and provide noticeable societal effects. So far, the many studies on applications are still scarce, fragmented, and focused on limited topics (e.g., payment systems) [1]. The hopes and expectations on this technology are undeniable. The ideas, suggestions, promises and attempts at possible proposals are growing exponentially, both by researchers and developers. At the same time, practitioners continue to present arguments on security and reliability issues, concerning development and application of any new technology with "unlimited powers".

Blockchain technology has seven basic principles that could facilitate many industries [2]: (i) A network integrity, which is encoded and distributed throughout the blockchain network; (ii) A distributed power through a peer-to-peer network with no any control point. If a central authority succeeds in withdrawing/cutting off an individual or group, the system survives; (iii) A value as an incentive of all stakeholders; (iv) The software rewards those who work on it and belongs to those who hold it; (v) A security that is built into the network ensures confidentiality and authenticity of all activities by cryptography; (vi) A confidentiality of users who have the right to decide what, when, how, and how much identity to share; (vii) An inclusion in a mutual cooperation with equal rights, access and perspectives for all participants by means of cyber-physical environment that facilitates financial, physical, digital and information resources exchange through transparent and traceable mathematical mechanisms.

At this stage, which could be called as mainly dedicated to analysis and research of variety possible areas based on blockchain applications and solutions, the smart agriculture is also in the focus. Here, the technology could solve many tasks and challenges in supply-chains monitoring and tracing, logistics and financial management, data provision or retail and etc. Data generated by Internet of Things (IoT) (sensors) is able to provide continuous information about soil temperature, moisture, pH level, etc. These data could be analysed by data mining algorithms, machine learning technics, artificial intelligence, then results uploaded in a blockchain and used in decision-making process about crop growing, watering, fertilizing, harvesting or trading.

The purpose of this paper is to present some general and specific aspects in research on applications of blockchain technology in intelligent agriculture. The main elements of the technology, popular definitions, focus areas in risk management concepts and the implications for internal audit and control procedures in companies that adopt blockchain in intelligent agriculture are briefly discussed. In summary, an algorithm for selecting of blockchain platforms and an algorithm for text mining in the domain of plant genetic resources are presented. A blockchain-based approach to modelling a supply chain in smart crop production is proposed, which is illustrated with a conceptual example of blockchain architecture and smart contract functions design.

2. BRIEF INTRODUCTION OF BLOCKCHAIN DEFINITIONS

A great variety of blockchain definitions could be found in scientific and popular recourses. Usually, the definitions link Distributed Ledger Technology (DLT) and blockchain. A blockchain (a chain of blocks) is a type of DLT. From technical perspective, a DLT is simply a decentralized database managed by various participants. A Blockchain is a DLT with a specific set of features. Here, examples are presented with the proviso that clear and consistent definitions remain subject to further clarification.

– "Blockchains are distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules" – NISTIR 8202 [3].
– "Distributed ledger (3.22) with confirmed blocks (3.9) organized in an append-only, sequential chain using cryptographic links (3.16). Note 1 to entry: Blockchains are designed to be tamper resistant and to create final, definitive and immutable (3.40) ledger records (3.44)" – ISO 22739 (updated 2020) [4].
– "A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision" – Technical Specification FG DLT D1.1 (August 2019) [5].
– "A blockchain is a secured, shared and distributed ledger that facilitates the process of recording and tracking resources without the need of a centralized trusted authority" [6].

– "Blockchain is an append-only ledger, a sequential database maintained by a decentralized network of users responsible for agreeing upon additions to the chain and secured through cryptography. A blockchain is a secure, transparent, irreversible digital ledger shared across participants. It is important to note that many different types of blockchains exist; there is no singular the blockchain" [7].
– "Blockchain is a distributed ledger – a continuously growing list of records that are hardened against tampering and revision. Fundamentally, it can be seen as a peer-to-peer infrastructure where nodes in the network coordinate to play a vital role in processing transactions" [8].
– "Blockchain technology refers to a fully distributed system for cryptographically capturing and storing a consistent, immutable, linear event log of transactions between networked actors. This is functionally similar to a distributed ledger that is consensually kept, updated, and validated by the parties involved in all the transactions within a network" [1].

Basically, a Blockchain is a publicly available ledger where participants enter data and certify their acceptance of the transaction via an Elliptic Curve Digital Signature Algorithm (ECDSA), i.e., for public-key cryptography. An elliptic curve is an equation such as $y^2 = x^3 + ax + b$. In Bitcoin and most other implementations, $a = 0$ and $b = 7$, so this is simply $y^2 = x^3 + 7$. Elliptic curves have numerous interesting properties, such as the fact that a nonvertical line intersecting two nontangent points will always intersect a third point on the curve [9]. The ECDSA is specified in ANS X9.62. FIPS 186-4 approves the use of ECDSA and specifies additional requirements [10]. In particular, Bitcoin, Ethereum or EOSIO use secp256k1 algorithm. The EOSIO supports secp256r1 also known as Prime-256 NIST Standard.

Blockchains element can be simplified by its components, Fig. 1. The detailed description can be found in [11]. Here, the element is presented breathily.

The block consists of the block header and its data. The header contains metadata for this block. The block data is a list of validated and authentic transactions that have been submitted to the blockchain network. Validity and authenticity are ensured by verifying that each transaction is properly formatted and that the providers of the digital asset have a cryptographic signature in each transaction (listed in the transaction "input" values).

The cryptographic hash function is an algorithm. It uses an arbitrary amount of data and creates an encrypted text output with a fixed amount, called a hash value or simply "hash". A cryptographic nonce is an arbitrary number that is used only once. It can be combined with data in order to produce different hash digests per nonce.

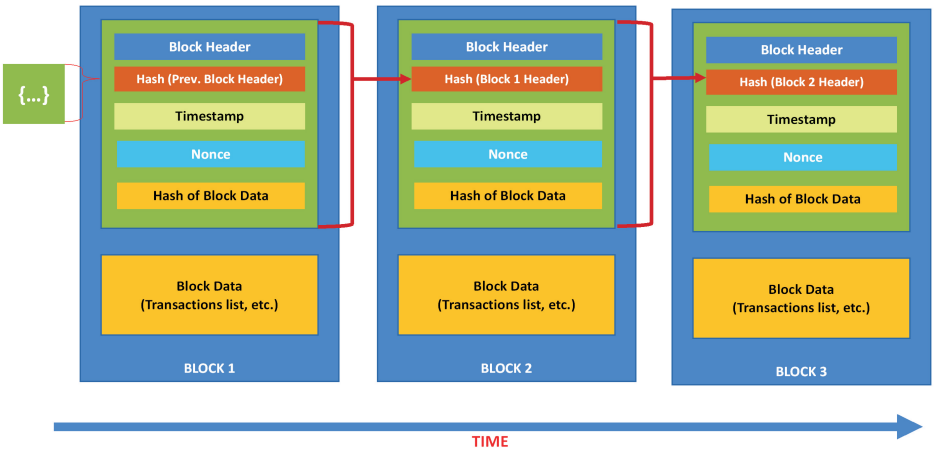

Fig. 1. Generic Chain of Blocks (Source: [3])

Transactions represent an interaction between parties. A transaction could be a way of recording activities occurring on digital or physical assets. Each block in a blockchain can contain zero or more transactions.

Blockchain technology uses asymmetric-key cryptography (also referred as public key cryptography). It uses a pair of keys: a public key and a private key that are mathematically related to each other.

There are two general types of blockchains – permissionless and permissioned. In a permissionless blockchain anyone can read and write to the blockchain without authorization. Permissionless access often is used in public blockchain networks (exchange of cryptocurrencies). Permissioned blockchain limits participation to specific users/organizations and allows finer-grained controls. Permissioned access is more commonly associated with private blockchain networks. Most enterprise blockchains (for non-crypto purposes) are private permissioned blockchains. The blockchain can also use a combined approach – consortium where only pre-selected participants are accepted. The consortium is not open to everyone, but is semi-private. A consortium blockchain is usually much more performant than a public blockchain, but is also less decentralized.

Some blockchains use an address (short, alphanumeric string of characters) derived from the blockchain user's public key by a cryptographic hash function, along with some additional data (e.g., version number, checksums). On unauthorized blockchains, users must store and manage securely their own private keys via software (wallet). The wallet stores private, public keys and

related addresses. The security and storage of private keys are a crucially important in blockchain technology.

The blockchain technology is associated with application of smart contracts. A smart contract is a computer program that is deployed using cryptographically signed transactions on the distributed ledger network. The smart contract is executed by nodes within the distributed ledger system. The results of the execution are validated by consensus and recorded on the distributed ledger. Smart contract automation reduces costs, lowers risks of errors, mitigates risks of fraud and potentially streamlines many business processes [5].

The blockchain, as a specific application, is closely related to the blockchain platform. The blockchain platform allows users and developers to create its own application in the existing blockchain infrastructure. The selection of blockchain platforms and their main characteristics (governance, platform description, mode of operation, consensus algorithm, cryptocurrency and smart contracts) and components should be assessed in advance, before undertaking the development of a blockchain application.

3. RELATED WORKS

In this section papers related to the tasks in the National Research Program "Smart crop production", approved by Decision of the Ministry Council No866/26.11.2020 and the Scientific Research Fund "BG PLANTNET establishment of national information network genebank – plant genetic resources", project KP-06-N36 are presented. The conducted researches explore aspects of risk management issues, impacts on internal audit procedures and control in companies adopting blockchain, the approach to blockchain software selection, the text mining in the domain of Plant Genetic Resources.

Four of the components that an organization should focus when implementing a blockchain are presented in [12] and include, Fig. 2: human and organizational resources, risk identification, blockchain control procedures and risk management and risk mitigation. The presented scheme is actually applicable to the blockchains auditing as well.

Human and organizational resources include training/recruitment of personnel with technical skills (including programming, cybersecurity), analysis of automated business processes, blockchain skills.

Risk identification includes five main subcategories: customer information security, model and network complexity, smart contracts and oracles, blockchain coding, and cybersecurity. Particular attention is needed to the initial stages of design and operation of blockchains.

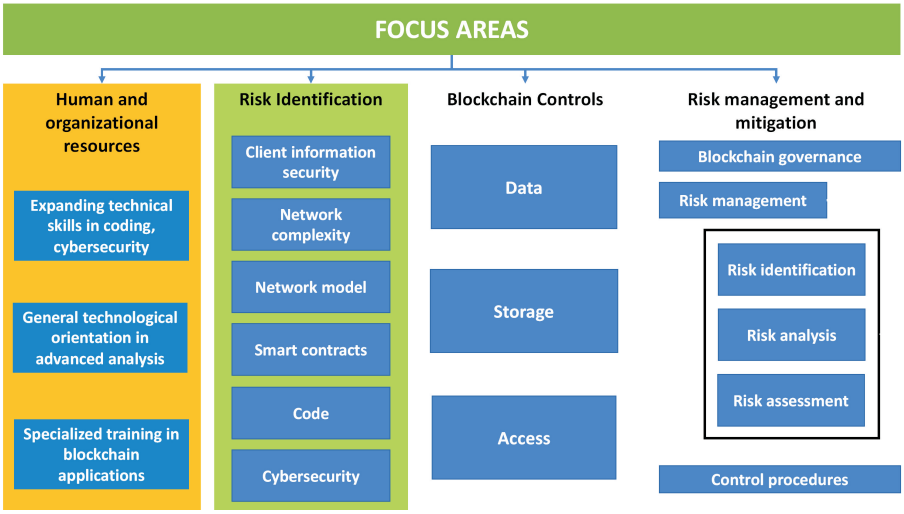

Fig. 2. Focus areas in blockchain adoption

Blockchain controls are related to data (throughput, network latency, consensus algorithm control), storage (amount of data in blocks, in nodes, or in the cloud), and access (data confidentiality and integrity).

Risk management and mitigation is a separate huge area for blockchains, despite the large number of internally set automatic mechanisms. In (13) this topic is presented in various aspects and applications. The main subcomponents are three: blockchain governance, blockchain management (storage and protection of private keys, adding/removing nodes, digital signatures) and control procedures (control of network access, execution of transactions, maintenance of current versions of blocks, contents of the block, etc.).

In its variety of application, the blockchains are of particular challenge for Internal Audit (IA) in organizations. IA functions need to be adapted and updated to the new interactions, logic and complexity that accompany the implementation and use of this technology. In [2] a framework for stages, procedures and elements for an IA execution plan in organizations that implement blockchains in smart crop production is proposed, Fig. 4. In many cases, it is a standardized process, with a clear protocol and responsibilities. If the IA execution plan should be presented only through the additions concerning blockchain adoption, it would have the following contents.

– Step 1. Initial phase – compiling a list of general and specific (blockchains) legislative base, regulating requirements, rules and standards.
– Step 2. Risk register (related to the "Risk management and mitigation"

component, Fig. 3, – risks and processes (future and current) under audit – assessment of impact, probabilities and control level of inherent blockchain risks: pseudo-anonymity, accountability issues blockchains, incompetence, unethical feats, negative reaction (employees/clients/advisors/ supervisors, loss of control by management).

– Step 3. Process (blockchain-based) on focus, for instance supply chain. When implementing the audit plan, this is reflected in step 2 also.
– Step 4. Risk assessment. In [14–16] the Enterprise Global Risk Management framework is proposed, which is related to the implementation of blockchain technology also.
– Step 5. Initial meeting with the auditee.

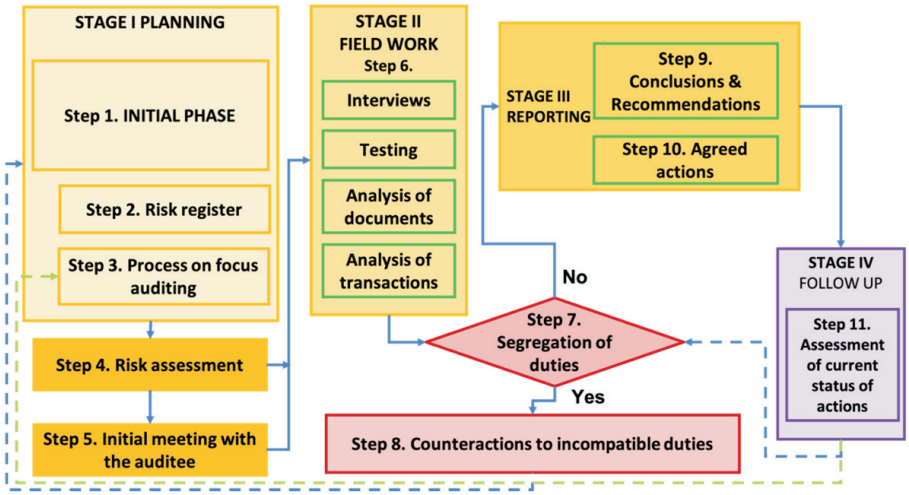

Fig. 3. Internal audit execution plan block-diagram

– Step 6. Interviews, testing, documents and transactions analysis – new requirements, rules, standards, etc. compliance, job description, qualification, training.
– Step 7. Checking for segregation of duties. The implementation of blockchains can significantly worsen the assessments for segregation of duties and impose significant changes at different levels in the organization. The solutions can be determined by the results and actions set out in steps 2, 3 and 8.
– Step 8. Counteractions to incompatible duties. Here, it is required going back to one or through all steps 1 to 5.
– Step 9. Audit report. Conclusions and recommendations regarding blockchain adoption could be in many directions, such as: segregation of duties/respon-

sibilities, procedures, policies for the operation of the blockchain, regulatory, legislation and rules alignment, personnel qualification and teams' management, control and response to errors identification, specific block circuits protocols, blockchain nodes operation and etc.

– Step 10. Agreed actions plan and deadlines.

– Step 11. Assessment of current status of actions implementation. This step loops the audit process and makes the execution of IA plan continuous or at least cyclical over time.

The introduction of blockchains can facilitate and automate execution of IA plan, but it cannot replace the functions and content.

Another issue in the application of blockchains is the selection of the blockchain platform. In [16] a framework for Blockchain Software selection is proposed as a Fuzzy Multi-Criteria Problem. The flowchart of the framework is presented in Fig. 4. In the paper several tasks are solved concerning blockchain and its implementation with focus on agriculture: (i) comparison of the most widely used blockchain platforms; (ii) exploration of the impact of blockchain software on agricultural companies; (iii) proposition of a conceptual framework for multi-criteria selection of an appropriate blockchain software; and (iv) verification of the proposed framework through an illustrative example.

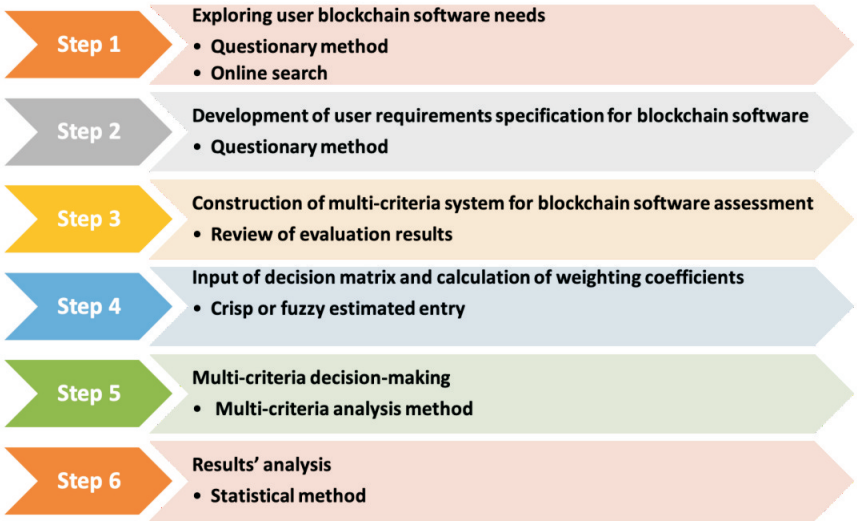

Fig. 4. The flowchart of the proposed framework for blockchain software selection

The results of the study disclosed some problems in blockchain implementations: (i) blockchain requires significant resources (financial, technological,

human and material); (ii) specific laws and regulations restrict access to distributed computing infrastructure; (iii) blockchain poses some potential risks (e.g., fraud, price manipulation, misuse of personal data). Most of these problems can be avoided by increasing the awareness of the principles and features of blockchain technology. The process of determining the best suitable blockchain software in organizations depends on many factors, for example, peculiarities of work processes and surrounding ecosystem. It is, in fact, a multi-criteria decision-making problem.

One of the areas that is developing in connection with blockchain technology applications is the convergence with Artificial Intelligence (AI), Machine Learning (ML), the Internet-of-Things and est. The Artificial intelligence reveals possibilities for the design and improvement of virtual platforms for intelligent agriculture. Via AI help, the systems can be constructed to perform various tasks in particular when the access to information from everywhere and at any time is very easy. The agricultural practices are enhanced by biotechnologies and new digital technologies such as distant observation cloud computing and the IoT, leading to the term "intelligent agriculture" – an ecosystem which integrates biological, chemical, physical, ecological, economic and social sciences in full-scale way for the development of new practices which do not harm the environment. For better coping with the challenges of the intelligent agriculture, agricultural ecosystems should be better analysed and understood. The technologies add to this understanding by continuously observing and measuring various aspects of the physical environment, producing huge quantities of data. This assumes the necessity of a large-scale collecting, storage, preliminary processing modelling and analysis of huge quantities of data, from different and heterogeneous sources.

In [17] a multistep algorithm for automatic analysis of documents from the area of plant genetic resources is proposed. Determination of the significant words in the document and the type of its content is carried out based on the object-oriented ontologies in the field. The documents are processed by software instruments for classification, testing and evaluation into related and not related to the studied subject area – agriculture and plant genetic resources of Bulgaria. The algorithm block-scheme is shown in Fig. 5.

In Step 1 the significance of the words in the document is determined. Certain words are significant for its content, and the sentences which transfer the most important information in the document are those that contain the most such significant words close to each other. In order to discover the significant words for the document, the frequency of appearance of the words is searched by using the software Wordclouds.com (free online cloud).

Fig. 5. The multistep algorithm for analysis and prognosis of the documents block-scheme

In Step 2 the degree of proximity is determined. It is carried out a search for every word of the so obtained set of words and phrases (Dataset) in the glossary of terms related to the ontology of the field subject and the least obtained value is taken.

In Step 3 a classifier is created. Through the analysis of the documents in the previous two steps a new set of data is created with the extracted central words and their degree of proximity to the terms of the field. The classifier is created if two thirds of these data are an object of classification algorithms for learning. The target attribute reflects whether the document is related to the field or not. The aim is to create a classifier for a new document to the classes {not related to the field = 0, related to the field = 1}.

In Step 4 the accuracy of the model is evaluated. After the learning, testing of the created models is carried out with the rest of the data and an evaluation of the precision of the work of every algorithm is made.

Finding keywords and phrases determines the thematic of one document. There are many applications based on subject ontologies, for example for searching in documents, indexing of large texts, automatic categorization of documents in given thematic category, automatic answering to questions and so on. The proposed multistage algorithm is dependent on the subject field because it can use specific characteristics of the field, set in the ontology. The considered field is strongly dynamic with the development of the artificial intelligence as well as many others connected to it sciences. The proposed algorithm can be integrated with the constantly appearing new technologies and applications.

4. BLOCKCHAIN-BASED SUPPLY CHAIN MODEL FOR SMART FARMING

In this section a blockchain-based supply chain model for smart farming is described. In general, the supply chain represents a network of participants involved in the production and distribution of a product to the end customer,

and includes various activities, entities, information and resources. The supply chain also includes the steps of the process from the initial moment of production to the point of the end user.

A blockchain-based supply chain can facilitate management by storing records about certification, quality, quantity, price, time, location and other relevant data. This information uploaded on the blockchain can increase the traceability of the products or materials, reduce losses by elimination of intermediaries, improve visibility, enhance trust, guarantee timely payments, and etc.

At this stage, the supply chain includes five supply chain channels suggested: (i) to facilitate the process of certification of new seed varieties, (ii) to support the control on technology for growing, yielding and selling the seeds; (iii) to monitor the subsequent certified seeds processing and/or selling; (iv) to facilitate interaction with state regulatory authorities; (v) to provide information on the origin of the seeds or their products to end-users. A blockchain-based supply chain (Fig. 6) has nine participants [18]:

– The GenBank of the Republic of Bulgaria (Gene Bank) stores germplasm through seeds under controlled conditions, observing FAO standards. It consists of many agricultural institutes that create new varieties of plants.
– Farmer-curators: authorized farmers in purchasing, propagation and selling the varieties of seeds from the Gene Bank to other farmers.
– Farmers: producers of unprocessed (raw materials) crop production.
– Producers: processors of raw materials into finished products.
– Store network: distribution and selling the final products to end customers.
– Logistics and transport companies.
– Financial and insurance bodies (banks, insurance companies, etc.).
– Distributors: wholesale and retail of products intermediaries.
– State regulators: supply-chains regulatory and controls bodies.

The supply chain considers five channels for value added products. They built a consortium blockchain with participants: Consortium GenBank Validator, GenBank Store, Seeds Exchange, Consortium Raw Materials and Consortium Products. The transactions in channels are governed by smart contracts. All attendees in the blockchain are registered as accounts and their sent/received requests are checked for formal and semantic correctness. All valid transactions are completed in a block and are recorded to the blockchain of the respective channel. After validation of the block, the distributed ledger is updated with the new data.

The GenBank Validator aims to verify and validate new plant variety. It is consisted of experts (members) from all agricultural institutes in the Republic

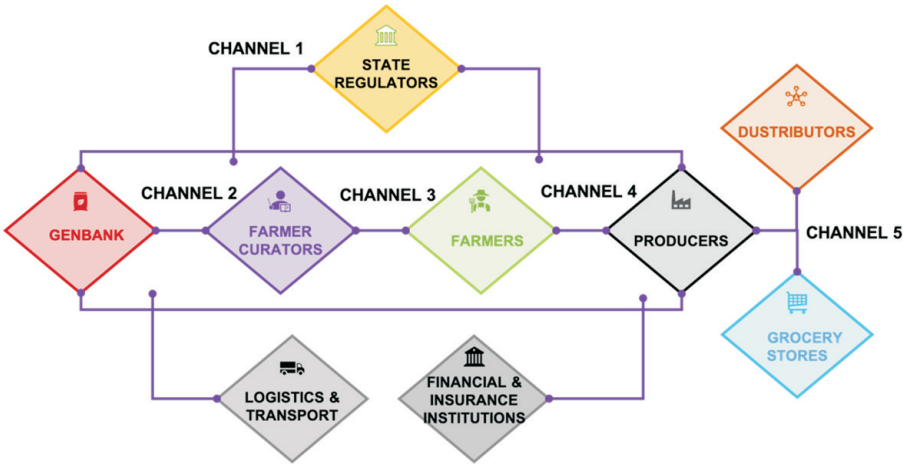

Fig. 6. A supply chain network

of Bulgaria, the Patent Office, and the Executive Agency of Variety Testing Field Inspection and Seed Control (EAVTFISC). Each member has an account and a public/private key pair for verification and signing of transactions.

A certificate is granted when the plant variety is new, different, homogeneous, and stable. The variety must also have a variety denomination, which is associated with its genetic designation and serves to identify it. The issuing a certificate for a new plant variety is approximately following. An authorized expert from a relevant institute generates a request and enters the new plant variety data into the system – creates an "asset". The same expert sends the request to a second expert from the same Institute through a transaction. If the two authorized experts sign the transaction, they agree to the existence of a new plant genetic variety. The "asset" is sent by transaction from the Institute to the Patent Office, along with all required documents. Within the statutory period, the Patent Office shall submit the application to the EAVTFISC for expertise. EAVTFISC performs the statutory inspections, samples for analysis, documents, etc., and returns its expert assessment to the Patent Office. The Patent Office signs (confirms the validation) the received transaction from the Institute. The new plant variety shall be entered in the state register of variety certificates of the Patent Office. The system issues a certificate for a new plant variety to the respective Institute after payment of respective fees.

The GenBank Store has three channels [19]: (i) a seed exchange channel for trading/swap seeds among Bulgarian institutes and agricultural institutes over

the world; (ii) a donation channel for granting seeds of Bulgarian institutes to botanical cities over the world; (iii) a sales channel for trading of genetic specimens of the Bulgarian Institutes to curatorial farmers. Here, the third channel is explained only, as it is included in the supply chain. The members in this channel are the GenBank, farmer-curators, and the state regulatory authorities. The catalogue of genetic specimens and seeds of the GenBank Store is available only to the channel members.

After the receiving a certificate for a new variety of plant (through the GenBank Validator) the institute preserves a certain quantity of seeds specimens for long-term storage. The rest quantity can be introduced to the sales system. The farmer-curators choose the variety for propagation and send a request (through a transaction) to the respective institute. The respective institute receives a transaction. A smart contract is concluded, through which the farmers-curators are agreed to grow the variety according to a specific procedure. The relevant logistics and payment (through the supply-chain) shall be completed. The exchange of seeds specimens and certificate of origin is simultaneous through respective logistics and payments. The institute sends a transaction signed by the respective private key and transfers ownership of the seeds to the respective farmer-curator. The farmer-curator receives the exact technology (recipe) for growing the seeds (fertilization time, minimum moisture values, maximum soil oxidation, etc.).

If the IoT infrastructure is in operation, the farmer-curator can collect different sensors data: temperature air, oxidation, soil moisture, etc. These data can be stored locally and used for further analysis in machine learning and artificial intelligence technics in smart crop production. A curator's internal sensor system and a blockchain are used as evidence of compliance with seed production technology. Sensory data is analysed and collected in the cloud. The results of analyses and records of critical data are stored in the blockchain.

In case of indications for violations in the growing technology of the respective variety, the system can automatically revoke the right of the farmer-curator. At the end of the life cycle of the variety, the farmer-curator notifies GenBank of the yield obtained from the cultivated variety and sends evidence of compliance with the cultivation technology. The respective institute confirms that the requirements of the farmer-curator are completed.

The members of the Consortium Seeds Exchange are farmer-curators, farmers, and state regulatory authorities. After harvesting, farmers-curators announce a quantity for sale and prices in the Seed Exchange channel, keeping the identification number of the seeds, received from the GenBank for the respective genetic material. The trade is carried out with contracts between

the parties, through smart contracts in the blockchain. All transactions for seeds transfer are completed in blocks, recorded in the blockchain. The performed logistics, payments, and insurances are controlled simultaneously on the supply chain level.

The purpose of the Consortium Raw Materials is to exchange raw materials between farmers and producers or between producers and producers. The members of the channel are farmers, producers, and state regulatory bodies. Farmers declare the harvest quantity for sale, using the same identification number of the variety received from the farmer-curators. However, they change the seed status to raw material or require the system to generate a new identification number in case they offer raw material on the market, flour for instance. A producer sends a transaction with a request for the respective raw material from a farmer or another producer via smart contract. It includes all the terms of the transaction. If a participant does not meet the required terms, the smart contract is not executed. The system will automatically deprive the rights of the incorrect party after two discrepancies have been identified. All logistics, transport, financial, and insurance relations that do not bring added value to the product will be processed from the supply chain level. All raw materials exchange transactions that add value to the products (value added transactions) are saved in the blockchain.

The members of the Consortium Products are producers, grocery stores, distributors, and state regulatory bodies. The raw materials that a manufacturer has procured through the Consortium Raw Materials channel could be used for production of products. In order to determine the product identification number, each producer adds the raw materials and quantity used in the production process. The system automatically generates identification number and creates a certificate of origin. The manufacturer sets the product price. The distributors/grocery stores can initiate smart contract request with a manufacturer/distributor. The supply chain level is used to organize financials and logistics exchange. The customer could receive information about a product by scanning the QR-code on the package.

5. CASE STUDY

The platform for design, deploying, and running the blockchain will be EOSIO (https://eos.io). This is an open-source platform, leveraging C++, EOSIO's development environment that can be configured and optimized for private and public networks. The blockchain is configured as a permissioned consortium blockchain. The number of nodes is minimum 3 distributed ter-

ritorially in different locations. The number of nodes is important for the decentralization and security of information in the blockchain.

Accounts are created for all users of the blockchain. An account is created for each channel, with a unique public/private key pair, with its own smart contract and corresponding functions (actions). Account names are maximum 12 lower-case Latin letters and numbers from 1 to 5.

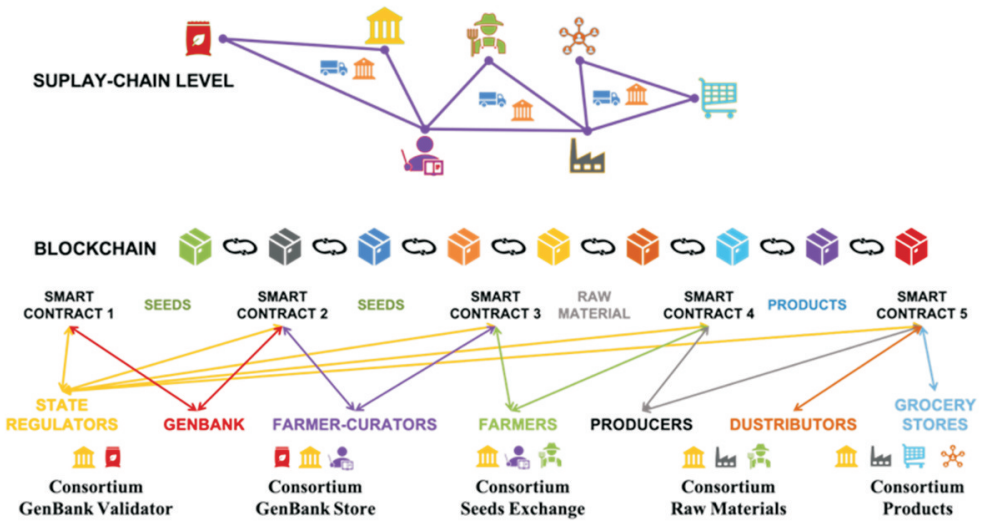

Fig. 7. Blockchain agriculture diagram

User accounts can be created with one or more (by type: farmers, farmer-curators, processors, etc.) public/private key pairs. Each account is allowed access to a relevant action (smart contracts) depending on their functions and characteristics.

The basic architecture of accounts and smart contracts can be schematically described as follows, Fig. 7:

– State regulators are permissioned to use all Smart contracts: 1, 2, 3, 4 and 5;
– The GenBank is permissioned to use Smart contracts: 1 and 2;
– Farmer-curators are permissioned to use Smart contracts: 2 and 3;
– Farmers are permissioned to use Smart contracts: 3 and 4;
– Producers are permissioned to use Smart contracts: 4 and 5;
– Distributors are permissioned to use Smart contract: 5;
– Grocery stores are permissioned to use Smart contract: 5.

The smart contracting with Logistics and transport companies and Financial and insurance bodies (banks, insurance companies, etc.) is not designed at the current stage of development.

Smart contract 1: for “Consortium Genbank Validator” – “genbank” account and a smart contract with the following functionality:
– Internal request for certification of a new variety (confirmation by a second expert (multi-signature transaction);
– Application to the Patent Office for registration of a new variety;
– Application to the EAVTFISC for expertise;
– Registration (or refusal) of a new variety;
– Register of approved varieties;
– Register of paid fees;
– Register of submitted applications in the process of consideration;
– Register of consortium participants, roles.

Smart contract 2: for “Consortium GenBank Store” – “genbankstore” account and a smart contract with functionality:
– Request for purchase of a variety for propagation;
– Yield report on the cultivated variety;
– Register of consortium participants, roles;
– Register of genetic specimens and seeds;
– Register of stocks by varieties;
– Register of payments;
– Register (by farmers-curators) on the basis of built IoT data infrastructure from various sensors: air temperature, oxidation, soil moisture, etc.

Smart contract 3: for “Consortium Seeds Exchange” – “seedsexchange” account and a smart contract with functionality:
– Purchase request;
– Register of consortium participants, roles;
– Register of stocks by varieties;
– Register of payments.

Smart contract 4: for “Consortium Raw Materials” –“rawmaterials” account and a smart contract with functionality:
– Request for purchase of raw material;
– Request for added value in the processing of raw materials;
– Register of consortium participants, roles;
– Register of payments;
– Register of the quantity of the harvest for sale by identification number of the variety;
– Register of performed transports;
– Register of value-added raw materials.

Smart contract 5: for ”Consortium Products” – “product” account and a smart contract with functionality:

– Request for purchase of raw materials for product production;
– Request for purchase of products from a distributor/store;
– Register of consortium participants, roles;
– Register of manufactured products;
– Register of payments;
– Register of performed transports;
– Register of certificates of origin;
– Price register.

The described architecture is exemplary and is subject to further development, correction and detailing.

6. CONCLUSION

The implementation of a blockchain requires steps, such as: familiarization with the technology; studying the necessary prerequisites for safe implementation, management and control; selection of platforms or software, the specifics of application and software design. These steps do not cover all aspects and problems. The researches and preliminary results presented in this paper support the main stages of blockchain adoption and applications in the domain of smart crop production. However, following this approach, several conclusions can be drawn.

The presented variety of blockchain definitions indicates that developers, scientists and users describe the technology with various technical, logical and terminological means. A common and universal point of view has not yet been established. It is obvious that a lot of effort and research needs to be done to stabilize the understanding, description, capabilities and diversity in the applications of blockchain technology in a systematic interdisciplinary framework.

The application aspects of blockchain technology require expanding of the understanding in risk identification, management and mitigation. Any organization intending to upload some business processes or entire business on a blockchain must take into account variety of issues and rise an attention upon all affected levels of government. Audit and control procedures can be positively influenced by blockchains, but development of specific qualifications, capacity, resources and updates in approach to managing this process are required.

Implementation of a blockchain in an organization/consortium of organizations may proceed in two ways: by engaging internal resources or use ready-made and customised software that is designed for a specific field of appli-

cation (payments, supply chain, document flow, billing, etc.). Regardless of the approach chosen, the selection should be made according to criteria that correspond to the application. This is a classic multicriteria decision making problem, which could be formulated and solved with different algorithms and methods.

Blockchain technology manages data-driven processes. The result depends on the quality of data. A way to enhance the performance of the processes is application of date mining techniques for extracting context and structuring information. When embedded in a blockchain, they can facilitate the network operation and the decision-making. The convergence of data mining techniques, artificial intelligence, machine learning, internet-of thing and blockchain is the inevitable next step that will reveal the future levels of the blockchain applications.

The use of blockchain, no matter where, within one organization or in a group of organizations, is a concrete, interdisciplinary and software task and is no different than any other of automation one. However, the most encouraging features about this technology are imbibed integrity, distributed power, value as an incentive, security and confidentiality which benefit equally and mutually all participants in the new physical-digital ecosystem.

Agriculture is a promising area for implementation of blockchain technology. The main advantages of blockchain applications are: reliable and sustainable food supply chains; safe of quality and quantity of food supply; enhanced trust between producers and consumers; guarantee timely payments due to smart contracting; elimination of intermediaries [20].

The future development of this study will focus on detailed analysis of existing blockchain standards, improving descriptions of functional levels in the supply chain network model and blockchain architecture design.

ACKNOWLEDGEMENTS

This work was supported by the Bulgarian Ministry of Education and Science under the National Research Program "Smart crop production" approved by Decision of the Ministry Council No. 866/26.11.2020 and by the Scientific Research Fund "BG PLANTNET establishment of national information network genebank – plant genetic resources", project KP-06-N36.

REFERENCES

[1] Marten Risius and Kai Spohrer, A Blockchain Research Framework: What We (don't) Know, Where We Go from Here, and How We Will Get There, *Business & Information Systems Engineering* (2017) **59** 385–409, DOI: 10.1007/s12599-017-0506-0.

[2] I. Popchev, I. Radeva, and V. Velichkova, The Impact of Blockchain on Internal Audit, in: Proceedings of International IEEE Conference Big Data, Knowledge and Control Systems Engineering – BdKCSE'2021, Sofia, Bulgaria, October 28–29, 2021, IEEE Xplore, 2021, ISBN:978-1-6654-1042-7, DOI: 10.1109/BdKCSE53180.2021.9627276.

[3] NISTIR 8202 Blockchain Technology Overview, https://doi.org/10.6028/NIST.IR.8202 (last access 02.12.2021).

[4] ISO 22739:2020(En), Iso.Org, 2020, www.iso.org/obp/ui/#iso:std:iso:22739:ed-1:v1:en

[5] ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT), Technical Specification FG DLT D1.1. Distributed Ledger Technology Terms and Definitions (2019), https://www.itu.int/en/ITU-/focusgroups/dlt/Documents/d11.pdf

[6] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, Security Services Using Blockchains: A State of the Art Survey, *IEEE Communications Surveys Tutorials* (2019) **21** (1) 858–880.

[7] J. Burns, A. Steele, E. E. Cohen, and Dr. Sri Ramamoorti, Blockchain and Internal Control: The Coso Perspective, https://www.aicpa.org/content/dam/aicpa/interestareas/informationtechnology/downloadabledocuments/blockchain-and-internal-control-the-coso-perspective.pdf (last access 02.12.2021).

[8] P. O'Reilly, Beyond Cryptocurrency: How Blockchain Can Transform Business (2016), Siliconrepublic.com, https://www.siliconrepublic.com/companies/2016/04/19/Blockchain-business-disruption-bitcoin (Last access 02.12.2021).

[9] David Bailey, The Mathematics Behind Blockchain, August 11th, 2017, https://mathinvestor.org/2017/08/the-mathematics-behind-blockchain/

[10] FIPS PUB 186-4, Federal Information Processing Standards Publication, Digital Signature Standard, Category: Computer Security, Subcategory: Cryptography, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899-8900, Issued July 2013, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf (last access 02.12.2021).

[11] Bela Shrimali and Hiren B. Patel, Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities, *Journal of King Saud University – Computer and Information Sciences* (2021), ISSN: 1319-1578, https://doi.org/10.1016/j.jksuci.2021.08.005, (https://www.sciencedirect.com/science/article/pii/S131915782100207X)

[12] Blockchain and Internal Audit, A Joint Research Report by the Internal Audit Foundation and Crowe by Richard C. Kloch, Jr., CPA and Simon J. Little, CPA 2019, https://www.crowe.com/insights/asset/b/blockchain-internal-audit-2019

[13] I. Popchev, I. Radeva, and V. Velichkova, Blockchains in Enterprise Global Risk Management, in: Proceedings of International IEEE Conference Automatics and Informatics 2021 (ICAI'21), IEEE Xplore, 30 September–2 October, 2021, Varna, Bulgaria, IEEE Xplore, 2021, DOI:10.1109/ICAI52893.2021.9639500, 282-287.

[14] I. Popchev, I. Radeva, and I. Nikolova, Aspects of the Evolution from Risk Management to Enterprise Global Risk Management, *Engineering Sciences* (2021) **LVIII** (1) 16–30, ISSN: 1312-5702, e-ISSN: 2603-3542, DOI:10.7546/EngSci.LVIII.21.01.02, http://es.ims.bg/indexx.htm

[15] I. Popchev and I. Radeva, Risk Analysis – an Instrument for Technology Selection, *Engineering Sciences* (2019) **LVI** (4) 5–20, ISSN: 1312-5702, e-ISSN: 2603-3542, DOI: 10.7546/EngSci.LVI.19.04.01.

[16] G. Ilieva, T. Yankova, I. Radeva, and I. Popchev, Blockchain Software Selection as a Fuzzy Multi-Criteria Problem, *Computers* (2021) **10** (10) 1–24, MDPI, ST ALBAN-ANLAGE 66, BASEL, SWITZERLAND, CH-4052, ISSN: 2073-431X, DOI:10.3390/computers10100120, https://www.mdpi.com/2073-431X/10/10/120

[17] I. Popchev and D. Orozova, Text Mining in the Domain of Plant Genetic Resources, in: Proceedings of IEEE 10^{th} International Conference on Intelligent Systems – IS'20, Varna, Bulgaria, IEEE Xplore, 2020, pp. 596–600, ISBN: 978-1-7281-5456-5, ISSN: 1541-1672, DOI:10.1109/IS48319.2020.9200174.

[18] I. Krasteva, T. Glushkova, N. Moraliyska, and N. Velcheva, A Blockchain-Based Model of Genbank Store System, in: IEEE 10^{th} International Conference on Intelligent Systems (IS), Varna, Bulgaria, 2020, pp. 606–611, https://doi.org/10.1109/IS48319.2020.9200133.

[19] I. Krasteva, T. Glushkova, A. Stoyanova-Doycheva, N. Moraliyska, L. Doukovska, and I. Radeva, Blockchain Based Approach to Supply Chain Modelling in a Smart Farming System, in: Proceedings of the International Conference Big Data, Knowledge and Control Systems Engineering – BdKCSE'21, 28–29 October 2021, Sofia, Bulgaria, IEEE Xplore, 2021, ISBN:978-1-6654-1042-7, DOI:10.1109/BdKCSE53180.2021.9627309.

[20] https://medium.com/@blockchain_simplified/the-path-less-travelled-blockchain-in-agriculture-3deaec60008d (last access 13.12.2021).

Received December 14, 2021