Magdalena Konopacka, Maciej Replin

BLOCKCHAIN TECHNOLOGY AND SMART CONTRACTS – MERGING TECHNOLOGY WITH THE LAW

Abstract: Blockchain's application is transformative, especially when combined with other emerging technologies such as the Internet of Things (IoT). The Authors underline blockchains' core aspects: decentralisation and trust based on enhanced security provided by underlying cryptographic technology. This trust is crucial when considering real-world applications like transferring money, assets, or even verifying the authenticity of products. Smart contracts are digital protocols executed within the Ethereum environment that introduce enhanced logic for streamlining transactions. These contracts stipulate specific criteria that must be met for the successful completion of a transaction. Functioning as an autonomous program on a distributed ledger (blockchain), smart contracts ensure transactional integrity and security by automatically verifying the fulfillment of transaction conditions, thereby facilitating predetermined outcomes without necessitating trust between transactional parties.
The 2016 Ethereum case study presents the pitfalls of overoptimism and the need for cautious approach to technology. The Authors welcome the European Law Institute efforts to propose pioneer European codification of principles enhancing consumer protection in the blockchain and smart contracts era.

1. INTRODUCTION – THE METHOD

The blockchain represents an organised, logical structure, serving as a decentralised transaction platform for at least two users. The platform's decentralisation is based on peer-to-peer (P2P) communication between users, meaning that no user occupies a central (dominant, privileged) position relative to others[1].

[1] P2P is a computer network communication model wherein all hosts (users, "peers") possess equal rights, contrasting with the client-server architecture. Consequently, the P2P communication model enables each user to operate as a client and server.

Each user stores the same amount of data, ensuring that there is no information asymmetry between users in a model approach. For effective implementation, blockchain utilises several information technologies. Beyond the mentioned P2P transmission technology, dedicated consensus mechanisms and encryption algorithms are crucial[2]. Each blockchain party (user) has access to the entire database and its complete history. None of the parties independently control the data and information. Every party can directly verify its counterpart's previous transaction record (the historical progression) without any intermediary's involvement.

Communication within the blockchain occurs directly, without the involvement of a central institution. Every network node (user) stores and sends information to all other nodes. Each transaction and its assigned value are visible to anyone with system access. Every node (user) has an alphanumeric address identifying it within the network. Once a transaction is added to the database following its verification (proof of work), the record cannot be changed, as it is linked (using a hash function) with the preceding transaction record. Various algorithms and cryptographic solutions ensure that the database record remains unchanged, chronologically ordered, and accessible to all on the network.

2. BLOCKCHAIN, TRANSACTION SAFETY AND TRANSACTION COSTS

A globally distributed database operating on millions of devices in the network enables the recording of anything of value to a user. Money, property rights, bonds, and other assets, licenses, certificates, and contracts can be transferred and securely stored between network users thanks to P2P protocols almost in real-time, without the mediation of verifying entities (regulators, intermediaries, "third-party authorities"). Trust in central institutions (banks, public authority entities, clearing institutions) is not required at all – it is replaced by so-called network consensus, verified code, and the computational effort of network users willing to offer their processing power[3]. Moreover, any network user can join the "settlement" (transaction) system by merely providing their computer's computational capacity.

---

[2] Y. Guo, Ch. Liang, Blockchain application and outlook in the banking industry, [in:] Financial Innovation, [online], 2016, https://jfin-swufe.springeropen.com/articles/10.1186/s40854-016-0034-9 [Accessed 5 May 2023]. Also: A. Tapscott, D. Tapscott, How Blockchain Is Changing Finance, "Harvard Business Review", Financial Markets, 1 March 2017, https://hbr.org/2017/03/how-blockchain-is-changing-finance [Accessed: 10 May 2023].

[3] The so-called "network consensus" involves the periodic agreement on the state of the main ledger after each alteration of its status. This agreement is based on finding a cryptographic solution that meets specified conditions – the solution can be verified (checked) by all network users.

Furthermore, it is worth noting that through a globally distributed database, information asymmetry is eliminated – no central entity becomes "privileged" by gathering information about other system users, or in other words, every user possesses equal rights concerning access to information (provided they have been granted such rights at all).

As more comprehensive implementations appear on the market, several distinguishing features emerge low transaction costs, high privacy (despite each transaction being visible in the system), and independent circulation (free from any central institution), which characterise the technology's advantages. On the flip side, a high degree of volatility, frequent cases of private key theft, and the attractiveness (primarily of cryptocurrencies) for committing international-scale crimes are considered undesirable phenomena accompanying the technology's use[4].

Blockchain, as a technology ensuring security and transactional certainty, presents a potential solution to many challenges facing the Internet of Things in its current development stage. Primarily, blockchains guarantee that devices can settle ("enter" into agreements with one another based on a predefined scheme) due to an initiating event (often termed a triggering event). For instance, a coffee machine will "order" coffee supplies – using a crewless vehicle (e.g., drone) – when its coffee level drops below 10%. The initiating event for the order would be the drop in coffee levels – payment will be made once it is confirmed that the goods have been delivered. Simultaneously, both "parties" would be contractually bound from the beginning since the funds, which the machine "manages", would be blocked in a specialised escrow account from the moment the order is placed and only released for payment upon the "confirmation" by the machine that the coffee level has been replenished as per the order.

3. SMART CONTRACTS AND CRYPTO COMMERCE – THE EXAMPLE OF ETHEREUM

Given the presented example, the concept of so-called smart contracts, mainly developed in the Ethereum environment, is worth discussing. Ethereum is designed to allow every user to create their digital symbol (token, coin) when needed. In the Ethereum environment, a token can represent any tradable good: money, loyalty points, gold acquisition certificates, debt acknowledgements[5] or

[4] N. Swartz, "Bursting the Bitcoin Bubble: The Case To Regulate Digital Currency as a Security or Commodity, Tulane Journal of Technology Intellectual Property, 2014, Vol. 17, s. 319–335.

[5] IOUs, plural of: "I owe you".

game items[6]. Given that all tokens have some basic functions implemented in a standard way, a user-designed token will instantly be compatible with the Ethereum wallet and any other client or contract using the same standards.

Vitalik Buterin, Ethereum's co-founder, identifies three possible types of Ethereum applications[7]. The first category includes financial applications, providing users stronger forms of agreement and money management. This category contains "internal" currencies (sub-currencies), financial derivatives, hedging contracts, savings wallets, wills, as well as some types of "full-fledged" work contracts. The second category involves semi-financial applications, where money is involved, but there is also a solid non-monetary side to what is being done. Perfect examples are self-executing rewards for computational problem solutions. Finally, completely non-financial applications, such as online voting or decentralised governance models, are possible.

Buterin's White Paper focuses on some possible applications, starting with tokens. Digital token systems can represent assets ranging from a currency issued by a state to a company's shares, individual signs representing smart property, secure non-counterfeitable payment coupons, and even systems unrelated to conventional value, used solely as incentive point systems. As Buterin indicates, token systems are straightforward to implement in Ethereum. The critical point is understanding that all currencies, as well as token systems, are essentially a database with one operation: subtract X units from A and add X units to B, provided that (i) A has at least X units before the transaction and (ii) the transaction is approved by A. All that needs to be done is to implement a token system to deploy this logic into a contract.

Furthermore, the White Paper addresses the most common application of a smart contract, i.e., a smart contract as a derivative instrument. According to Buterin, the main challenge in implementing financial contracts is that most require reference to an external price ticker. For instance, a desired application is a smart contract that hedges against ether's volatility (or another cryptocurrency) concerning the U.S. dollar exchange rate. However, executing this task requires the contract to "know" the current ETH/USD rate. The simplest way to achieve this is a data feed contract, operated by a particular entity (e.g., NASDAQ), designed so that the entity can update the contract if such an update is needed and provides an interface that allows other contracts to send messages to it and receive a price (rate of that currency pair) in response. With this critical component, a hedging contract might look as follows:

---

6 V. Buterin describes the Ethereum environment as the "Lego of cryptofinance" see N. Schneider, "Code your utopia: Meet Ethereum, bitcoin's most ambitious successor" http://america.aljazeera.com/articles/2014/4/7/code-your-own utopiameetethereumbitcoinasmostambitious-successor.html, [Accessed 20 June 2023].

7 V. Buterin, White Paper, A Next-Generation Smart Contract and Decentralised Application Platform, https://github.com/ethereum/wiki/wiki/White-Paper [Accessed 15 March 2023].

wait for Party A to transfer 1000 ether,

wait for Party B to transfer 1000 ether,

record the USD value of 1000 ether, calculated by "querying" the data feed contract; marking this, for example, as $x, after 30 days, allow A or B to "reactivate" the contract to transfer ether worth $x (calculated by re- "querying" the data feed type contract to get a new price) to A, and send the rest back to B.

As Buterin points out, the described contract would have significant potential in crypto-commerce. It would address one of the main problems of cryptocurrencies: their volatility. Although many users and traders may want the security and convenience of using digital assets, they may want to avoid facing the prospect of losing 23% of their funds' value in one day. Buterin elaborates that the most commonly proposed solution currently is issuer-backed assets. The idea is based on the issuer creating an internal currency (sub-currency), which they have the right to issue and write off. The issuer provides a currency unit to anyone who delivers them (offline), a unit of a specific underlying asset (e.g., gold or a state currency). The issuer promises to deliver a unit of the underlying asset to anyone who returns (sends back) a unit of the crypto-asset. Such a mechanism allows non-cryptographic assets to be "elevated" to cryptographic assets, assuming the issuer is trustworthy. In practice, however, issuers are only sometimes trustworthy, and in some cases, the banking infrastructure needs to be more robust or more beneficial for such services to exist. Derivatives, therefore, provide an alternative solution. In this case, instead of a single issuer providing funds to back a given asset, a decentralised market of speculators plays the role, betting that the price of the cryptographic reference asset will rise, for example.

Unlike issuers, speculators cannot default on their transactional obligations, as the hedging contract keeps their funds in an escrow account[8]. Buterin notes that this approach is not entirely decentralised since a trusted source is still required to provide the price ticker. Despite this, the solution significantly improves fraud mitigation[9]. It greatly reduces infrastructure requirements – unlike being an issuer, providing price information does not require licensing and can be regarded as an exercise of free speech.

The White Paper addresses at least one significant issue worth noting here: the concept of decentralised autonomous organisations (DAO). As the author

8 For an early risk analysis from before the cryptocurrency era, compare United Nations Office on Drugs and Crime, Risk of Money Laundering through Financial Instruments 2nd Edition, English version 2 Bogota, D.C. 2013, pp. 159–160.

9 On recent developments, especially on the challenge of more sophisticated ransomware see: The Conversation, International ransomware gangs are evolving their techniques. The next generation of hackers will target weaknesses in cryptocurrencies, 28 August 2023 [Accessed 30 August 2023]. With respect to potential art-bubble, namely NFT market, see also: The Conversation, NFTs in the art world: A revolution or ripoff?, 11 December 2022 [Accessed: 30 August 2023].

suggests, this could be a virtual entity with a designated group of members or 'shareholders', wherein, for example, a majority of 67% has the authority to decide on the entity's fund expenditure or its code modification. Thus, members could collectively decide on resource allocation. This mirrors the governance manifestations of a traditional corporation or non-profit organisation but with blockchain enforcement.

Buterin emphasises the significant attention DAOs receive due to "capitalist" decentralised autonomous corporation (DAC) solutions, with the potential for dividend receipt and transferable shares. An alternative, described as a "decentralised autonomous community", would mean all members have an equal stake in decision-making, and 67% of current members would be required to agree to add or remove a member. A mandate that one person can only hold one membership unit would have to be collectively introduced. Buterin highlights that more sophisticated structures could have built-in vote delegation – user A transfers their vote to B, and B transfers to C; C decides with the vote originally belonging to A. According to the author, such a design facilitates the organic growth of a DAO as a decentralised organisation, allowing people to delegate tasks through "filtering" to specialists. Unlike the "current system", specialists can quickly come and go as individual community members change their views. However, the reality has tested Vitalik Buterin's plans concerning the DAO development. The DAO was established in April 2016 as a venture capital type in the Ethereum environment, with the mission of providing a new business model for commercial and non-profit ventures.

The organisation's code was transparent – everything was readable and auditable[10]. The DAO was designed as a hub that disperses funds to projects. Investors received voting rights by purchasing tokens – they voted on specific projects reviewed by contractors, and a group of volunteers, called curators, verified the identity of proposal submitters and ensured their proposals were legal before being safe-listed[11]. To raise initial capital for the fund during a 28-day crowd sale, they collected ether valued at over USD 150 million, setting a record for ICOs at that time.

Yet, the complexity of the codebase and its rapid market entry meant that the intended behaviour deviated from reality. This became evident, especially after the attack on 17 July 2016, during which attackers "extracted" ether worth

10 M. E. Peck, Ethereum's $150-Million Blockchain-Powered Fund Opens Just as Researchers Call For a Halt, https://spectrum.ieee.org/tech-talk/computing/networks/ethereums-150-million-dollar-dao-opens-for-business-just-as-researchers-call-for-a-moratorium [Accessed 7 May 2023].

11 R. Waters, Automated company raises equivalent of $120M in digital currency, "Financial Times", 17.05.2016, online, https://www.cnbc.com/2016/05/17/automated-company-raises-equivalent-of-120-million-in-digital-currency.html [Accessed 1 May 2023].

approximately USD 50 million[12]. The attack exploited specific vulnerabilities in the fund's operational code. A technically "legal" transaction locked the funds in a separate account, so they were not entirely lost. This sparked a debate among investors and the Ethereum community on addressing the situation. Notably, 14% of ether was in The DAO at that time. Ultimately, part of the community advocated for a "manual" rollback of the blockchain to a state as if the funds had not been extracted from The DAO. Another faction believed that if the overriding value is the mathematical "independence" of the system, other ways to recover the funds should be sought, possibly by developers executing a reverse transaction. Following the attack, the DAO project concluded with the fund's closure, which also profoundly impacted the future development of the Ethereum blockchain itself. Ethereum split into two separate chains – due to the implementation of a hard fork, the blockchain was restored as if the attack never occurred (now called Ethereum (ETH)); however, the existence of the original blockchain could not be eradicated and persists as Ethereum Classic (ETC). This instance underscores the controversies surrounding the immutability of transactions once introduced to the blockchain.

The Ethereum blockchain is akin to the Bitcoin blockchain, but with notable distinctions[13]. The primary difference lies in its structure; blocks in the Ethereum chain contain copies of both the transaction list and their most recent state, unlike Bitcoin. Furthermore, each block also stores two other values: the block number and the difficulty level. Ethereum's verification model currently operates on a proof of work system; however, there are plans to transition to a more efficient proof of stake model. Much like Bitcoin, Ethereum requires dynamic difficulty adjustments. On average, blocks on the Ethereum network are produced every 15 seconds. This interval is crucial for the system's state synchronisation, ensuring that chain branching (or forks) and transaction history alterations are impossible unless an attacker possesses more than half of the network's computational power. In essence, the mathematical assumptions of Ethereum do not diverge from those of Bitcoin.

Ethereum's management emphasises collaboration with the developer community. Notably, Ethereum boasts its high-level programming language called Solidity, reminiscent of JavaScript in syntax. Efforts are being made to enhance its accessibility and widespread use, evident in the project's guiding principles: simplicity, universality, modularity, non-discrimination, and agility. The ethos of simplicity dictates that the Ethereum protocol should be as straightforward

---

12 K. Finley, $50 Million Hack Just Showed That the DAO Was All Too Human, 18.06.2016, online, https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/ [Accessed: 20 May 2023]

13 A. M. Antonopoulos, G. Wood., Ethereum dla zaawansowanych. Tworzenie inteligentnych kontraktów i aplikacji zdecentralizowanych (Mastering Ethereum: Building Smart Contracts and Dapps), translation T. Walczak, Helion, Gliwice 2019, p. 37.

as possible, even if it comes at the cost of efficiency concerning disk space or time. The creators highlight that an average developer should fully grasp and implement the solution, and optimisations that unduly complicate the code should only be made if they offer significant benefits. Universality suggests that while Ethereum inherently lacks built-in features, it facilitates constructing any contract or transaction mathematically definable. Modularity means components of the Ethereum protocols should be constructed as modules, enabling them to be detached and repurposed. Non-discrimination implies that a protocol should not actively limit or prevent certain types of use; regulatory mechanisms should directly address harm rather than opposing specific undesirable applications. Finally, agility indicates that Ethereum's protocol specifics are not set in stone.

Although the founders approach changes cautiously, especially those complicating the language, they remain open to modifications improving the language considering scalability or security. The Ethereum Foundation, a non-profit entity, oversees the platform's operations. Its mission encompasses promoting Ethereum, researching the underlying technology, fostering development, and educating to provide tools and incentives for next-gen decentralised app (dapps) developers, aiming for a more globally accessible, free, and trustworthy internet. Ethereum's founders are among the first to recognise the significance of a unified programming environment for the holistic development of the blockchain market. The project's maintenance as open-source and the rising popularity of cryptocurrencies, chiefly Bitcoin, have amplified efforts towards advanced contracts, including those pertaining to the 'smart property' market segment.

4. ASSET CONTROL WITH SMART CONTRACTS

'Smart property' refers to assets controlled by smart contracts, meaning through a blockchain application. Examples of smart property on the blockchain could be a physical item (vehicle, house) or a property right like a company share. A vehicle exemplifies how a smart contract operates in practice, turning the vehicle 'smart'. The vehicle's onboard computer requires authentication via an ownership key, typically a cryptographic key (e.g., a Bitcoin ECDSA-256 key). The vehicle is manufactured, and the public part of the ownership key is created with a small cryptocurrency amount deposited on this key.

Moreover, the vehicle possesses a digital certificate from its manufacturer and an identification key, with the public part enclosed in the certificate. This allows interested parties to verify the vehicle's existence and details like its age or mileage. When sold, the buyer generates a nonce (random number) and requests the vehicle data from the seller. The seller inputs the nonce into the vehicle, which then produces authentication data, encompassing the nonce, certificate, vehicle data, the current owner's public key, the transaction, and the last ownership transfer's Merkle tree[14]. This assures the buyer about the exact vehicle they are purchasing and that they are transacting with the actual owner.

The seller chooses a key (k1) and sets a sale price (P). The buyer then creates a new ownership key (k2) and constructs a transaction with two inputs and outputs. The first input records P funds, and the second connects to the output containing T funds as the property address. The first output sends P funds to k1, while the second sends T funds to k2. This transaction still needs to be validated since only the first input can be signed. The partially complete transaction is handed to the seller, who signs the second input with the current vehicle ownership key before transmitting it. They then await several network confirmations. The buyer then 'presents' the vehicle with the transaction (plus the Merkle tree linked to the block header containing this transaction) and several subsequent block headers in the chain, ensuring the irreversible property transfer transaction. The vehicle updates ownership details. Furthermore, the vehicle needs to retain only part of the blockchain record or block headers, only enough data to link future block headers to what was presented. Despite the apparent complexity, this process could seamlessly happen using standard phones equipped with NFC; tapping a dashboard with a phone containing the ownership key would trigger the smart property trading app in the appropriate mode.

Upon setting a price, the buyer and seller could close their phones together to finalise the transaction. An additional advantage of using the phone might be that it could also function as a means to start the engine. Having control over the "behaviour" of items in a physical sense allows for using this feature when granting simple secured loans based on these items. For example, a given smart contract could involve accumulating funds to finance a vehicle for an entrepreneur. If the entrepreneur fails to operate per the initial agreements they committed to, individual investors should be guaranteed the ability to withdraw from the investment by seizing the collateral or, at the very least, preventing the entrepreneur's further access to the vehicle funded by their investment. This can be achieved by adding an access key to the vehicle's ownership key. The access key granted to the entrepreneur would be valid within specific time frames aligned with the loan repayment period. Such a solution would ensure the entrepreneur's uninterrupted use of the vehicle while providing investors with the possibility of physical control over the vehicle (e.g., by removing the entrepreneur's ability to start the engine) in case of a loan default. Indeed, other systems also provide the described functionality, but – as rightly pointed out by Vinay Gupta – "not with the ele-

[14] R. Jabbar et al., Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review, https://hal.science/hal-03570962, pp. 7 et seq., [Accessed: 15 June 2023].

gance and simplicity of a smart contract"[15]. The development of intelligent contract environments and smart property is closely intertwined. However, it is important to note that currently, there are many formal limitations to further "integration". Creating new products and services by merging elements in the market is challenging when intricate legal and administrative regimes often govern these components[16]. This significantly hampers the efficiency of many economic sectors. Some endeavours are simply out of reach for an entity that lacks adequate economic resources (assets) and needs the necessary intellectual infrastructure.

5. THE VISION AND ITS CODIFICATION – A LEAP INTO THE UNKNOWN?

The European Law Institute has undertaken another of a series of ambitious comparative tasks of drafting model principles in the discussed field[17]. The Institute warns that Smart Contracts (ELI uses capital letters), through their technological complexity and integration within blockchains, offer transformative opportunities to streamline transactions but also present numerous legal challenges. A comprehensive approach is necessary, merging technological and legal perspectives. This entails examining them through the lens of private law or public regulation individually and holistically. Some national blockchain legislations have begun incorporating this integrated viewpoint[18]. However, this report predominantly explores the private law dimension to shed light on the legal ramifications of blockchain transactions and Smart Contracts. While Distributed Ledger Technology (DLT) and Smart Contracts can facilitate Government-related transactions (G2G, B2G, G2C), the ELI Principles address private law concerns, with view to protect consumers[19]. In this context, the European Commission has already introduced the Digital Finance Package (DFP), including the Regulation on Operational Digital Resili-

---

15 V. Gupta, Building The Hyperconnected Future on Blockchains, The Internet of Agreements, World Government Summit, Dubai 2017, http://internetofagreements.com/files/WorldGovernmentSummit-Dubai2017.pdf, p. 7 [Accessed: 15 May 2023].

16 Cf. M. Morena et al., Blockchain and real estate: Dopo di Noi project, Property Management Vol. 38 No. 2, Emerald Publishing Limited 2020, pp. 273–295.

17 ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection The European Law Institute, Vienna 2023 report is available at www.europeanlawinstitute.eu.

18 M. Lehmann, National Blockchain Laws as a Threat to Capital Markets Integration, Uniform Law Review, Vol. 26, March 2021, pp. 148 et seq.

19 O. Borgogno, Usefulness and Dangers of Smart Contracts in Consumer Transactions [in:] The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms (eds. L.A DiMatteo et al.), pp. 288–310.

ence in the Financial Sector (DORA)[20], which is set to be effective starting from 17 January 2025, and introduces significant measures in the EU's financial regulatory landscape.

On June 29, 2023, Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA) entered into force. The regulation defines in detail, among others: a crypto-asset, an Asset-Referenced Token ("ART"), and a token which is electronic money or e-money (Electronic Money Token – "EMT")[21]. MiCA becomes effective on June 30, 2024 (ART and EMT), while the remaining provisions are set to be in effect as from 30 December 2024.

MiCA is expected to foster innovation and fair competition, while improving the quality of operation and integrity of crypto-asset markets. It aims to support financial stability and ensure the proper functioning of payment systems, as well as counteract the threats to monetary policy that crypto-assets may pose[22]. The new regulation is linked to existing instruments such as MIFID[23] (markets in financial instruments directive) and MAR[24] (market abuse regulation), which set the early standard for investor protection.

Beyond traditional legal frameworks, there is a push for innovative 'sandboxes', safe environments where blockchain functionalities and Smart Contracts can be tested without exposing developers to liability yet safeguarding platform users. One such initiative is the European Blockchain Partnership's European Blockchain Services Infrastructure (EBSI), a combined tech-regulatory sandbox[25]. Before taking the leap, humankind should take the new toys back to sandboxes and test the potential of merged legal and technological solutions.

BIBLIOGRAPHY

Antonopoulos: A. M. Antonopoulos, G. Wood., Ethereum dla zaawansowanych. Tworzenie inteligentnych kontraktów i aplikacji zdecentralizowanych (Mastering Ethereum: Building Smart Contracts and Dapps), transl. T. Walczak, Helion, Gliwice 2019;

Borgogno: O. Borgogno, Usefulness and Dangers of Smart Contracts in Consumer Transactions [in:] The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms (eds. L.A DiMatteo et al.);

Buterin: V. Buterin, White Paper, A Next-Generation Smart Contract and Decentralised Application Platform, https://github.com/ethereum/wiki/wiki/White-Paper [Accessed 15 March 2023];

[20] Regula2554,/2554, OJ L 333, 27.12.2022, pp. 1–79.
[21] See: KNF, Rozporządzenie MiCA – najważniejsze informacje, 18 October 2023.
[22] OJ L 150/40, 9 June 2023.
[23] Directive 2014/65/UE.
[24] Regulation 596/2014.
[25] ELI Principles on Blockchain Technology…, pp. 8–9.

Guo: Y. Guo, Ch. Liang, Blockchain application and outlook in the banking industry, [in:] Financial Innovation, [online], 2016, https://jfin-swufe.springeropen.com/articles/10.1186/s40854–016–0034–9 [Accessed 5 May 2023];

Gupta: V. Gupta, Building The Hyperconnected Future on Blockchains, The Internet of Agreements, World Government Summit, Dubai 2017, http://internetofagreements.com/files/WorldGovernmentSummit-Dubai2017.pdf, p. 7 [Accessed: 15 May 2023];

Jabbar: R. Jabbar et al., Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review, https://hal.science/hal-03570962, pp. 7 et seq., [Accessed: 15 June 2023];

Lehmann: M. Lehmann, National Blockchain Laws as a Threat to Capital Markets Integration, Uniform Law Review, Vol. 26, March 2021;

Morena: Cf. M. Morena et al., Blockchain and real estate: Dopo di Noi project, Property Management Vol. 38 No. 2, Emerald Publishing Limited 2020;

Peck: M. E. Peck, Ethereum's $150-Million Blockchain-Powered Fund Opens Just as Researchers Call For a Halt,https://spectrum.ieee.org/tech-talk/computing/networks/ethereums-150-million-dollar-dao-opens-for-business-just-as-researchers-call-for-a-moratorium [Accessed 7 May 2023];

Schneider: N. Schneider, Code your utopia: Meet Ethereum, bitcoin's most ambitious successor, http://america.aljazeera.com/articles/2014/4/7/code-your-own utopiameetethereumbitcoinasmostambitioussuccessor.html, [Accessed 20 June 2023];

Swartz: N. Swartz, "Bursting the Bitcoin Bubble: The Case To Regulate Digital Currency as a Security or Commodity, Tulane Journal of Technology & Intellectual Property, 2014, Vol. 17;

Tapscott: Also: A. Tapscott, D. Tapscott, How Blockchain Is Changing Finance, "Harvard Business Review", Financial Markets, 1 March 2017, https://hbr.org/2017/03/how-blockchain-is-changing-finance [Accessed: 10 May 2023];

Waters: R. Waters, Automated company raises equivalent of $120M in digital currency, "Financial Times", 17.05.2016, online, https://www.cnbc.com/2016/05/17/automated-company-raises-equivalent-of-120-million-in-digital-currency.html [Accessed 1 May 2023].