International Journal on Consumer Law and Practice

Volume 7 Article 3

2019

BLOCKCHAIN 'WITNESS': A NEW EVIDENCE MODEL IN CONSUMER DISPUTES

Matej Michalko CEO and Founder
DECENT Group, Switzerland

BLOCKCHAIN 'WITNESS': A NEW EVIDENCE MODEL IN CONSUMER DISPUTES

—*Matej Michalko*[*]

Abstract *Concealing, falsifying, or altering court evidence is a significant issue on a global scale. An act like evidence tampering can serve as downright detrimental not only to criminal investigations and civil lawsuits but also the judicial system as a whole. In this article, Matej Michalko, CEO and Founder of one of the pioneering blockchain companies in the world, DECENT, explains how blockchain-supported evidence can be efficiently used to present legitimate proof in consumer disputes, demonstrating the benefits of using the secure, modern, and innovative technology inside the juridical sphere through authentic examples in which blockchain has served as a legitimate means for presenting evidence. As a leading figure in the blockchain scene, Michalko delves into various subject matters such as third-party evidence preservation platforms, judicial blockchain consortium, applying blockchain to trace online sales and protecting consumer rights, surging e-commerce consumer disputes and "off-radar" counterfeits, offering a global perspective on blockchain-based evidence preservation and its relevant developments in the judicial domain as well as exploring the technical*

[*] Matej Michalko is the CEO and Founder of DECENT Group, Switzerland. DECENT is a non-profit foundation that has developed an open-source blockchain platform, DCore which was founded in 2015. Cooperating closely with top investment funds and incubators, DECENT is dedicated to building the ecosystem upon its proprietary blockchain technology to help developers and businesses adapt to a decentralized future. DCore was launched in 2017 to provide user-friendly SDKs to empower dApp developers and businesses in the decentralized network. Digital Proof is a DCore-based evidence preservation platform that can provide proof for any type of files. Specializing in digital proof services targeted at individuals, businesses, intellectual property agencies, and notarial institutes, it allows users to upload files to the vault for a permanent registration record with blockchain timestamps. Digital Proof works closely with professionals and organizations in the global domain of intellectual property to provide a one-stop solution for intellectual property evidence preservation and protection. Author can be contacted at deja@decent.ch.

principles, demand, context, judicial environment, and social significance of the application of blockchain technology in consumer protection.

I. INTRODUCTION

On June 28, 2018, the Hangzhou Internet Court (HIC), China's first Internet court, recognized the validity of blockchain timestamped proof in a copyright dispute, the first time a court admits the legal value of blockchain-based evidence preservation through lawsuit results. In the dispute, the copyright holder, City Express, exclusively authorized Huatai Yimei, as the plaintiff, to file a copyright infringement suit on its behalf. The defendant, Daotong Technology Co., Ltd. was found to reprint City Express' articles and photos without permission, allegedly infringing on the plaintiff's right of dissemination through information networks. The defendant was then sued in the HIC, and demanded compensation for the plaintiff's financial loss.

Unlike ordinary copyright infringement cases, the plaintiff, in order to prove its claim, preserved evidence with blockchain technology: the plaintiff used a third-party blockchain evidence preservation platform to automatically fetch the web pages accused of copyright infringement, and identified their source codes. The web pages and source codes, together with the packages of call logs, were calculated to get a hash value to upload to the blockchain network to ensure the integrity of the evidence.

Taking the blockchain-supported data storage and legal standards for reviewing electronic evidence into full account, the court examined the effectiveness of blockchain-based evidence preservation. The court admitted the authenticity of the electronic data as the web page screenshots and source codes were fetched and identified with a credible platform; the above-mentioned electronic data was preserved using blockchain technology that meets relevant requirements, thus ensuring the data integrity; as the hash value was verified and consistent with other evidence, the court decided to base its judgment on the electronic data. In this connection, the HIC found that the electronic evidence of the blockchain submitted by the plaintiff had legal effect. In the end, Datong Technology was convicted of

copyright infringement and ordered to compensate the plaintiff for financial loss in the amount of RMB 4,000 yuan.[1]

The innovative practice of utilizing blockchain technology to store electronic data and ensure data integrity is a new way to integrate the Internet and electronic evidence preservation, which provides more possibilities for right holders to defend their rights and reflects a new trend of electronic evidence.

Globally, China has taken the lead in recognizing the legal effect of blockchain evidence, and thus blockchain evidence has been rapidly applied in various scenarios. Meanwhile, as China's growing share of online consumption brings about an increasing number of infringement disputes, consumer rights protection has already become a social focus. This paper will, by taking the development of blockchain evidence preservation in China as an example, explore the technical principles, demand, context, judicial environment, and social significance of the application of blockchain technology in consumer protection.

II. WHAT MAKES A BLOCKCHAIN 'WITNESS' CREDIBLE?

In this case, blockchain evidence preservation plays the role of a key 'witness'. So, what is the principle behind?

A. Blockchain Network: Tamper-free and Traceable Data

Blockchain is a form of distributed ledger technology that is maintained by multiple nodes on a blockchain network.

Distributed networks are completely different from traditional centralized networks. Distributed network theory proposes to establish an interface between each computer or network, and the connection does not require central control, but is directly connected through the interface between the networks. For distributed networks, the importance of a single node is greatly reduced. When one approach is not feasible, it is completely possible

[1] "Ten Typical Cases of the Hangzhou Internet Court" (Zhejiang Law Online, 3 September 2018) <http://www.zjfzol.com.cn/index.php/cms/item-view-id-70473.shtml> accessed 11 July 2019.

to take another one. And if a node has an error, it is not repaired through the central command, but by the node itself.

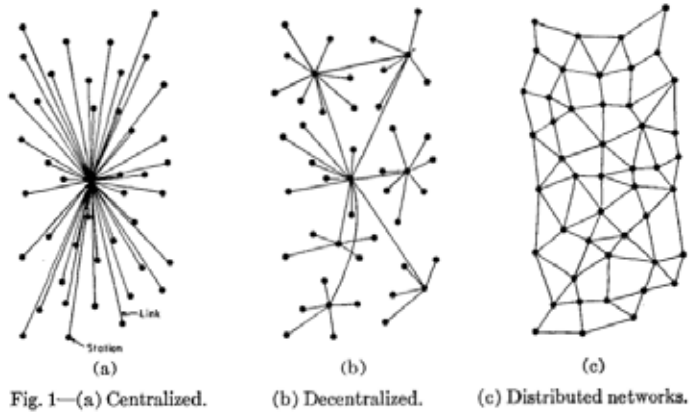

Figure: Centralized, Decentralized and Distributed Systems (Paul Baran, 1964)2

Additionally, in theory, the data transmitted in a distributed network has a specified length, and data exceeding this length is divided into a few blocks and transmitted again. Each block contains not only data itself, but also information about where it comes from and where it goes. These blocks are transferred between stations, with each station maintaining a record until it reaches its destination. If a block is not successfully delivered, it will be resent by the initial computer. If the delivery is successful, the computer that receives the data block will recombine all the blocks received, and then give a 'Data Received' message after confirming the data. In this way, the computer that originally sent the data will not send the data again.

In 1961, Dr L Kleinrock from the Massachusetts Institute of Technology (MIT) published the paper 'Information Flow in Large Communication Nets', the first time that the theory of distributed networks was discussed in detail. In the 1960s, Paul Baran, a Polish-American engineer, wrote several reports, which not only systematically expound the theory of distributed networks but also the core of network communication: packet switching. In 1965, with the support from the RAND Corporation, Baran officially proposed to the U.S. Air Force to establish a distributed network. At the same

[2] Paul Baran, "On Distributed Communications Networks" (RAND Corporation Papers, 1962) 2626 <https://www.rand.org/content/dam/rand/pubs/papers/2005/P2626.pdf> accessed 15 July 2019.

time, D.W. Davis, a British physicist, also proposed the theory of distributed network in a way much the same as Baran's, except for the naming. Baran referred to the split, easy-to-transfer data as blocks. After careful consideration and consulting with linguists, Davis decided to use the term 'packet' for the data, and 'packet switching' for the way how data is split.

Thanks to specifications and protocols adopted by consensus, and open and transparent algorithms, blockchains in modern networks translate trust in humans into trust in algorithms, eliminating human intervention in the system.

The network security of the blockchain and the tamper-resistance nature of blockchain data are determined by the following two factors. First, the nature of its distributed network: once the information is verified and added to the blockchain, it is permanently stored and difficult to tamper with (unless a 51% attack occurs and more than 51% of the nodes in the distributed network are attacked and stored records are tampered with, but in the real world this hardly happens[3]).

Second, hash value verification is the basis of cryptography and blockchain technology. Through the operation on the encryption function (hash function), the electronic data will obtain a unique tamper-free ID to ensure its integrity.[4] If the input changes, the output will be completely different. However, if the input does not change, the resulting hash output will always stay the same, no matter how many times you run the hash function. In blockchain network, the hash output serves as the unique identifier of the data block. The hash value of each block is generated based on that of its previous block (which explains why the blocks are linked together to form a blockchain), and also on the data contained in the block, which means any changes made to the data will influence the block hash value.[5]

The hash values ensure the security and tamper-resistance of blockchain data, providing a prerequisite for the validity of blockchain evidence to be accepted in lawsuit cases.

---

[3] Jake Frankenfield, "51% Attack" (Investopedia, 24 May 2018) <https://www.investopedia.com/terms/1/51-attack.asp> accessed 15 July 2019.

[4] Jake Frankenfield, "Hash" (Investopedia, 20 October 2017) <https://www.investopedia.com/terms/h/hash.asp> accessed 15 July 2019.

[5] The Economist Staff, "Blockchains: The Great Chain of Being Sure About Things" (*The Economist*, 31 October 2015) accessed 15 July 2019.

As information technology has been continuously integrated with society and businesses, there is an increasing volume of legal issues and disputes in the fields of e-commerce, internet finance and intellectual property. Generally, the traditional evidence requires notarization with long response time and high preservation cost, and the application scenario cannot meet the dynamic, real-time and big data requirements of electronic evidence preservation. The blockchain evidence preservation service features a simple process, low cost and high data reliability. The right holder can use the platform for real-time evidence preservation when the infringement occurs.

"Blockchain is a decentralized database that is open, distributed and irreversible, and works as an electronic data storage platform with low cost, high efficiency and stability. In judicial practices, the legal effectiveness of electronic evidence storage should be comprehensively determined based on the principle of technology neutrality, technical description and case review," said the trial judge from the HIC.[6]

B. Legal Ground for the Validity of Blockchain Evidence Preservation: judicial Interpretations of China's Supreme People's Court (SPC)

On September 3, 2018, the SPC of China provided legal confirmation for trusted timestamps and blockchain-based evidence preservation in the form of judicial interpretations.

The SPC's 'Provisions on Several Issues Concerning the Trial of Cases by Internet Courts' (hereinafter referred to as the 'Regulations') sets forth a comprehensive series of rules for trial principles, scope of acceptable cases, trial jurisdiction, evidence exchange, and electronic data in internet judicial procedures. In addition, the Regulations facilitate the electronic institutional innovation of trial mode, electronic delivery, electronic case files, and appeal procedure.

For the first time, the SPC gave detailed judicial interpretations for the trial of cases by Internet courts. As referred to in Article 11 of the Regulations, 'Where the authenticity of the electronic data submitted by a party can be proven through electronic signature, trusted timestamp, hash value check, blockchain or any other evidence collection, fixation or

---

[6] "Hangzhou Internet Court—The First to Accept Blockchain Proof as Means of Evidence", (*Legal Daily*, 29 June 2018) <http://www.legaldaily.com.cn/index/content/2018-06/29/content_7581930.htm?node=20908> accessed 11 July 2019.

tamper-proofing technological means, or through the certification on an electronic evidence collection and preservation platform, the Internet court shall make a confirmation'.[7]

C. Infrastructure: Third-party Evidence Preservation Platforms and Judicial Blockchain Consortium

In the previous trials of dispute cases, evidence preservation usually requires the involvement of a third-party authority such as a notary office, and relevant persons are required to fix the evidence under the witness of the notary. With the more frequent use of electronic evidence, most of the third-party electronic data preservation platforms have investigated the pattern of "blockchain + evidence collection and preservation", which is applying blockchain technology to the traditional electronic evidence preservation practice (i.e., uploading the preserved evidence to a blockchain platform). If necessary, you can apply online for an expert opinion from the judicial expertise centre.

In practice, the court will also review the qualifications of the evidence preservation platform. In the opening case, as the shareholder and business scope of the operating company affiliated to the third-party evidence preservation platform is independent of that of the plaintiff Huatai Yimei, and the platform also passes the integrity check conducted by the National Quality Supervision and Testing Center for Information Network Products (NTI), the HIC therefore recognized the platform's qualification as a third-party electronic evidence preservation platform.

Third-party evidence preservation platforms and the judiciary are working together to establish a pilot judicial blockchain consortium that centers on both internet courts and traditional courts.

In September 2018, the HIC, one year after its establishment, applied blockchain in its online lawsuit handling system, where appellants can submit contracts, rights protection procedures, service process details and other electronic evidence through online portals under the witness and verification of the nodes including the notary offices, judicial expertise centers, CA/RA (certification/ registration authorities), courts, Ant Financial Services Group (Alipay's credit and finance service system). As of 1 May 2019, the HIC's

[7] "Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Cases by Internet Courts" (China's Supreme People's Court, Interpretation No. 16 [2018], 3 September 2018).

judicial blockchain platform now has access to a notary office, a judicial expertise center, and 32 third-party blockchain evidence platforms.[8]

Since the launch of HIC's blockchain-based system, most of the cases have been successfully closed through mediation. As of late April 2019, the rate of copyright disputes withdrawn through mediation increased from 82.3% to 95.3%.[9]

As for the Beijing Internet Court (BIC), its electronic evidence platform—Scale Chain, or 'Tianping Chain' in Chinese, jointly established with the leading blockchain enterprises in China, was launched in December 2018. Within the first three months following its establishment, 17 judicial blockchain nodes were built, application data of 24 Internet platforms/third-party data platforms was successfully integrated with the data of blockchain evidence platforms.[10] As of March 22, 2019, the Scale Chain had collected more than 3.3 million data entries on the Internet. In addition, as the ecosystem involves multiple blockchain evidence platforms, there in fact may be tens of millions of corresponding entries.[11]

III. APPLYING BLOCKCHAIN TO TRACE ONLINE SALES AND PROTECT CONSUMER RIGHTS

In 2018, China's online retail sales amounted to RMB 9006.5 billion yuan, an increase of 23.9% over the previous year. The online retail sales of physical goods reached RMB 7019.8 billion yuan, an increase of 25.4% and accounting for 18.4% of the total retail sales of consumer goods,[12] resulting in a surge of consumer complaints against online retailers.

---

8 "Hangzhou: Over 90% of Copyright Disputes Withdrawed Thanks to Blockchain" (Xinhuanet, 1 May 2018) <http://www.xinhuanet.com/legal/2019-05/01/c_1210124225.htm> accessed 11 July 2019.

9 (n 8).

10 "3 Months after Release, the Beijing Internet Court's 'Tianping Chain' Has Collected Over 1 Million Data Entries", (*Beijing News*, 23 December 2018) <https://baijiahao.baidu.com/s?id=1620609464467575438&wfr=spider&for=pc> accessed 11 July 2019.

11 "Data Volume of the Beijing Internet Court's 'Tianping Chain' May Have Reached Tens of Millions" (*People's Daily* Online, 29 March 2019) <http://blockchain.people.com.cn/n1/2019/0329/c417685-31002730.html> accessed 13 July 2019.

12 "Total Retail Sales of Consumer Goods Increase by 9.0% from January to December 2018" (National Bureau of Statistics of China, 21 January 2019) <http://www.stats.gov.cn/tjsj/zxfb/201901/t20190121_1645784.html> accessed 17 July 2019.

A. Surging E-commerce Consumer Disputes and "Off-Radar" Counterfeits

As shown by the consumer complaints against hundreds of online retailers handled by the third-party e-commerce consumer dispute mediation platform (www.315.100ec.cn, formerly known as "China E-Commerce Complaints and Consumer Protection Platform"), the complaints received in the year 2018 have witnessed a year-on-year increase of 38.36%, second only to the 48.02% in 2017. Among them, the domestic online shopping complaints represent the highest percentage, accounting for 55.19% of all complaints; cross-border online shopping complaints accounted for 6.82%.[13]

Among all the online orders, luxury goods have become the hardest-hit area for torts and disputes. The feedback received from Chinese consumers who bought luxury goods from online retailers in 2018 shows a dissatisfaction rate of 42%. As some 73% of the luxury goods online retailers in China purchase from unofficial channels, and the shipment rates of unofficial channels have reached 81%, customers are 48% or more likely to be cheated by fake luxury goods.[14] The huge profit margin of brand counterfeiting and proficiency at fake goods fabrication have contributed to the surge of fake fabrication. Moreover, the counterfeit goods team can even manage to get the fake-proof code numbers, so that even if the customer checks, he or she is highly unlikely to tell whether it is fake or not.

B. Difficulties in Producing Evidences make it Hard for Online Consumers to Defend their Rights

According to Article 64 of China's Civil Procedure Law: 'It is the duty of a party to an action to provide evidence in support of his allegations'.[15] First, the consumer has to provide the purchase record to prove that he or she has a buyer-seller relationship with the online retailer. Then, he or she needs to provide prima facie evidence to prove that the retailer sells fake products. There are three valid bases: (1) The seller acknowledges sales of

---

[13] 2018 China E-Commerce User Experience and Complaint Monitoring Report, (E-Commerce Research Center, 12 March 2019) <http://www.100ec.cn/zt/2018yhts/> accessed 17 July 2019.

[14] China Digital Luxury Report 2019 (Yaok Institute, June 2019) <https://finance.sina.com.cn/chanjing/gsnews/2019-06-17/doc-ihvhiqay5899941.shtml> accessed 11 July 2019.

[15] Standing Committee of the National People's Congress, "Civil Procedure Law of the People's Republic of China" (approved on 9 April 1991, revised on 28 October 2007 and 31 August 2012) <http://www.npc.gov.cn/wxzl/gongbao/2012-11/12/content_1745518.htm > accessed 17 July 2019.

counterfeits; (2) The brand provides appraisal reports; (3) The state authorities of industry and commerce provide expert evidence.

Generally, the most effective way to produce evidence is to get appraisal reports from the brand. However, in practice, very few brands are willing to provide consumers with authenticity identification services. Also, most third-party appraisal agencies only accept the judicial expertise entrustment, and in most cases do not provide consumers with authenticity identification services. In judicial practice, if the right holder (the brand suspected of being infringed) cannot be found, the judicial authority will entrust a third-party agency to authenticate. The report issued by the agency is not an authenticity appraisal report, but an 'inconsistencies comparison' report, stating that the entrusted product is inconsistent with the original sample.[16]

Among the reported online shopping infringement disputes, there is a typical scenario where the buyer finds inconsistencies between the product bought online and the counter product, and then the seller is required to provide the source information and certificate of the product, which the seller is not able to provide; then the buyer therefore contacts the e-commerce customer service centre to make a complaint, only to get refused by the e-commerce platform on the grounds that 'the chat history that indicates the seller cannot provide the authenticity identification' and 'the comparison photos of the purchased product and the counter product' are not convincing enough; while waiting for the result of the complaint, the buyer will find the product link already invalid: 'the product you are viewing does not exist or may have been sold out or transferred'.[17]

C. Blockchain-supported Product Traceability and Consumer Protection

On 1 January 2019, the 'E-Commerce Law of the People's Republic of China' officially came into force, complementing China's Cybersecurity Law and Consumer Rights Protection Law. This has strengthened the responsibilities and obligations of e-commerce operators, especially third-party platforms, contributing to better consumer protection.

---

[16] "Joint and Several Liability Mechanism Forces the E-Commerce Platform to Crack Down on Counterfeits" (*Yanzhao Evening News*, 1 November 2017) <http://zj.sina.com.cn/news/zhuazhan/2017-11-01/detail-ifynmnae0893834.shtml> accessed 17 July 2019.

[17] "How Can We Protect Online Shopping Against Counterfeits? Legal Opinion: E-Commerce Platform Should Compensate First" (*People's Daily Online*, 24 January 2018) <http://www.xinhuanet.com/yuqing/2018-01/24/c_129797536.htm> accessed 17 July 2019.

Article 38 of the E-commerce Law clearly states that 'Where an operator of an e-commerce platform fails to take necessary measures when it knows or should know of the fact that operators on its platform sell commodities or offer services that fail to safeguard personal or property safety, or commit any other acts that impair the lawful rights and interests of consumers, the operator of such e-commerce platform shall be jointly held liable together with the violating operators on its platform'.[18]

Professor Qi Aimin, dean of the National Cybersecurity Protection and Rule of Law Strategy of Big Data Institute of Chongqing University, referring to the first case where blockchain proof was accepted as means of evidence, points out that the new Internet technology represented by the blockchain may bring about new trends in tracing the source of e-commerce products, evidence collection and preservation.

Traditional fake-proof tools (barcode, QR code, etc.) use centralized approaches: product information is controlled by manufacturers and is easy-to-replicate, which does not guarantee the rights of consumers. Look at how blockchain is used for product-tracing and anti-counterfeiting: the product is marked by the Internet of Things (IoT, such as the Smartdust[19]) and AI recognition to form identity information with unique physical characteristics of the product, which is later stored in the blockchain network; in every link from manufacturing to distribution, the product (together with the "marks") is compared with the physical characteristics and identity information stored in blockchain through AI recognition, crawler technology, and hash verification[20], to guarantee the authenticity of the product. The information generated in each link will be stored in blockchain; the information is encrypted, verified, and packaged into blocks through the blockchain distributed network to constitute a tamper-free, interlocked and bidirectionally-traceable record chain; at last, consumers can track through online queries.

---

[18] Standing Committee of the National People's Congress, "E-commerce Law of the People's Republic of China" (approved on 18 December 2018) <https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E7%94%B5%E5%AD%90%E5%95%86%E5%8A%A1%E6%B3%95/16467544?fromtitle=%E7%94%B5%E5%95%86%E6%B3%95&fromid=22679227&fr=aladdin> accessed 17 July 2019.

[19] Charles Brett, "DECENT's 3IPK: Blockchain For Aviation Supply Chain, And More" (*Enterprise Times*, 13 September 2018) <https://www.enterprisetimes.co.uk/2018/09/13/decents-3ipk-blockchain-for-aviation-supply-chain-and-more/> accessed 17 July 2019.

[20] "Whitepaper on Tracing with Blockchain (Version 1.0)" (Trusted Blockchain Initiatives, October 2018) <http://www.caict.ac.cn/kxyj/qwfb/bps/201810/P020181023464389645849.pdf> accessed 17 July 2019.

Product-tracking in this way will minimize human intervention, as it relies on the neutrality and reliability of technologies to build trust between the brand, e-commerce platform and consumer to eliminate counterfeiting, and at the same time provide sellers and buyers with credible evidence when product authenticity is questioned or damage during shipping arises.

In addition, consumers can turn to third-party blockchain evidence preservation platforms to store the product information, promotional information, return/change commitments provided by online retailers in web pages, apps, advertisements and chat boxes. Consumers can preserve evidence for potential disputes without worrying that the sellers might refuse to admit or delete relevant information.

The E-Commerce Law also puts higher demands on the protection and fair use of big data. Based on the underlying technologies of blockchain, big data technologies that can guarantee privacy protection, security and high efficiency will soon be recognized and widely used in the market.

IV. A GLOBAL PERSPECTIVE OF THE BLOCKCHAIN-BASED EVIDENCE PRESERVATION AND RELEVANT DEVELOPMENTS IN THE JUDICIAL DOMAIN

In May 2018, Ohio Senator Matt Dolan submitted to the state legislature a bill intended to clarify the legal status of blockchain signatures and contracts. The bill, SB300, failed to advance but portions of its language were inserted as amendments into another bill, SB220. The full language that survived intact focuses on blockchain contracts and signatures: (1) "A record or contract that is secured through blockchain technology is considered to be in an electronic form and to be an electronic record." (2) "A signature that is secured through blockchain technology is considered to be in an electronic form and to be an electronic signature." Later in August 2018, Ohio passed the bill and signed it, which means that Ohio has legally recognized the validity of blockchain data.

In July 2018, the Dubai International Financial Centre (DIFC) Courts announced that it is partnering with the Smart Dubai initiative to set up what it calls the world's first "court of the blockchain". Based on the current dispute resolution mechanism, the two sides will first explore how to help the Courts verify the judgment on cross-border law enforcement. The research will combine expertise and resources to investigate disputes arising from private and public chains, as well as coding rules and contractual

terms of smart contracts. According to this blockchain strategy, Dubai will be able to run 100% of applicable government transactions on blockchain by 2020.

In August 2018, the UK government announced an initiative to explore the use of blockchain technology to secure electronic evidence. The pilot project aims to assess whether the distributed ledger technology (DLT) can be utilized to simplify and streamline the present-day court processes, according to Balaji Anbil, the head of the Digital Architecture and Cyber Security team at HM Courts & Tribunals Service (HMCTS), Ministry of Justice.

In November 2018, Azerbaijan announced the country would start using blockchain in notaries, courts, penitentiaries, NGOs and registries. The Azerbaijani Internet Forum is preparing for the adoption of blockchain by the government, starting with the Ministry of Justice. The agency currently provides over 30 electronic services, and also about 15 information systems and registries. The "electronic notaries", "electronic courts", penitentiary services, information systems of NGOs, and population registration are all included. The planned project entitled as "Mobile Notary Office", can assemble all notarial documents in one case. The DLT is expected to enhance the transparency of the country's legacy systems that are vulnerable to the falsification of the population registration and database.