1st International Conference on Advances in Civil & Environmental Engineering, University of Engineering & Technology Taxila, Pakistan

Conference date 22 &23 Feb 2022

A Brief Introduction to Blockchain Technology and its Applications in Civil Engineering and Construction

Vagelis Plevris
Department of Civil and Architectural Engineering
College of Engineering, Qatar University, Doha, Qatar
vplevris@qu.edu.qa

ABSTRACT

Blockchain is a novel technology which permits the recording of data in a way that it is extremely difficult to change, hack or cheat. It is a promising technology that is considered as a general-purpose technology (GPT), by many. GPTs are technologies that have the power to influence and change an entire economy, affecting economic growth and the way people behave in their everyday lives and do business. We present some technical details about blockchain, how it began and its possible applications today, with focus on civil engineering and the construction industry. We also examine future applications of the technology, the challenges and opportunities it brings and its potential to reshape the construction industry to the better.

KEYWORDS: blockchain, general purpose technology, civil engineering, construction, engineering

1 INTRODUCTION

The Architecture, Engineering, and Construction industry has entered a period of major change caused by a host of new digital technologies that have been proven helpful due to the benefits and the potential they offer. These technologies include Virtual Reality, Artificial Intelligence, Geographic Information Systems, Building Information Modelling (BIM), Augmented Reality, the Internet of Things (IoT), Big Data, Sensors, among others [1]. Lately, a new digital technology has appeared, Blockchain, which promises to change the way people do transactions, keep their records, validate their data, and more. For many, blockchain is a general-purpose technology (GPT) that can change both our everyday lives and the way we do business.

By looking at the most recent scientific literature, one can realize how important blockchain technology has become lately. The word "blockchain" returns 27,959 results in the Scopus database (www.scopus.com) when searching within "Article title, Abstract and Keywords" (query made on Feb. 20, 2022). 27,715 of these results (99.1%) have a publication year of 2017 or later, as only 244 papers were published in the topic between 1990-2016. The trend is similar if we limit the search within the "Engineering" field, where we similarly receive 11,641 results (documents) in total. Figure 1 shows these search results, per year. It should be noted that for the most recent year 2021 the process of indexing and adding papers is still in progress in Scopus.

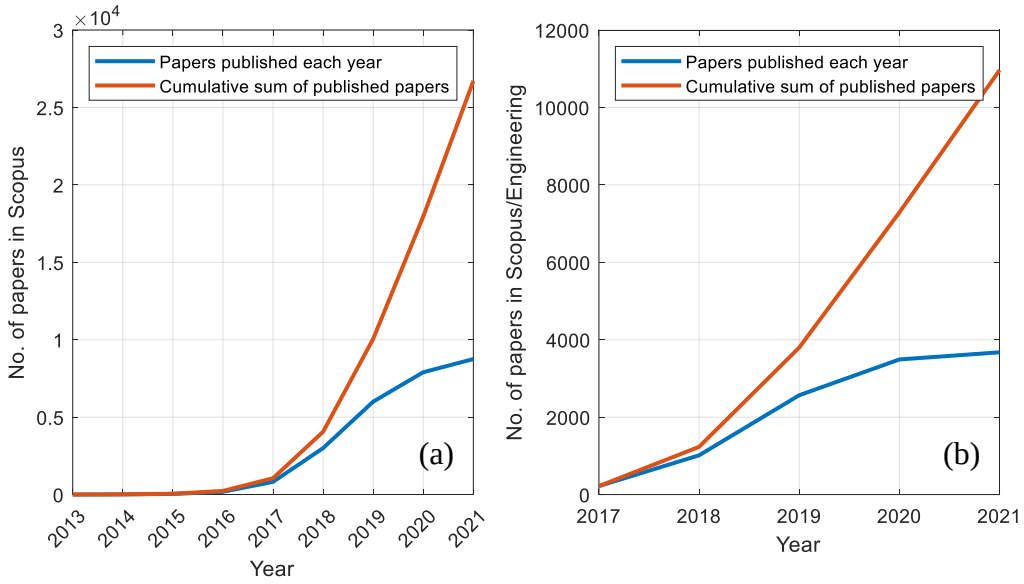

Figure 1: Papers in "blockchain" in Scopus database: (a) All fields, (b) Engineering field.

2 BITCOIN: THE FIRST IMPLEMENTATION OF BLOCKCHAIN

In the long past, there were no monetary mediums. People would exchange goods using barter agreements. Then came money, in the form of a metal coin, a piece of paper or another object that people could use as a medium of exchange. The 21st century and the evolution of computers and digital technology gave rise to "digital money", allowing electronic, mobile payments between different parties. Such digital payments offer the advantage that the parties involved need not be in the same physical location. Unlike cash payments which are "peer-to-peer", mobile payments are made through an institution (usually a bank) which acts as an intermediary. This can cause problems, such as high transaction fees, censorship of transactions, while not all people can have access to a bank account due to bank restrictions or other reasons.

In 2008, Satoshi Nakamoto introduced Bitcoin. In his novel work [2] the brilliant idea of a system for electronic transactions which does not rely on a "trusted third party" is explained. It was the first implementation of blockchain technology. Blockchain allowed Bitcoin to transfer value in a decentralized network without any central authority, for the first time, offering an elegant solution to the "double spending" problem in digital currency, and opening horizons for other important applications in the future. Bitcoin is a peer-to-peer digital cash system which uses cryptography and the concept of "proof-of-work" (PoW) to record transactions.

In Bitcoin there is no bank or any other intermediary playing a special role. It is a fully decentralized network where all parties are "equal", having the same rights. It uses a decentralized approach, based on the creation of blocks linked together, forming a chain of blocks (blockchain). In the blockchain, every transaction and every block have a timestamp and blocks are linked together with their hash values and PoW. The record of a transaction is distributed among many nodes in the system, making it impossible for a bad actor to manipulate the ledger to their advantage. Using PoW, the amount of computational power needed to reverse

or change a transaction is enormous. This technology allows bitcoin to transfer value in a decentralized way without the need for any trusted third.

3 TECHNICAL DETAILS

3.1 Asymmetric cryptography

Asymmetric cryptography uses a pair of keys (Public and Private key) to encrypt/decrypt a message. The private key is private, while the public key can be shared with anyone. A message which is encrypted with the private key can only be decrypted with the public key, and vice-versa. There are two main uses: (i) Sender authentication, and (ii) Receiver authentication. The first is used to ensure that a message came from the stated sender, while the second is used to ensure that a message can only be read by the intended recipient. In Bitcoin and similar blockchain-based networks, the two keys are used to ensure the integrity of transactions.

3.2 Cryptographic hash functions

A hash function is a one-way function that maps data of an arbitrary size to fix-sized values [3]. Its return is called the hash value or digest. A hash function is deterministic and designed to be irreversible, i.e. it is not possible to generate the input from the hash. Additional properties of a cryptographic hash function are: (i) Quick computation, (ii) impossibility to generate a message that will give a given hash, (iii) impossibility to find two messages giving the same hash, (iv) a slight change in a message results to a drastic change in the hash. Bitcoin uses the SHA-256 algorithm which was designed by the US National Security Agency and first published in 2001 [4]. The value set of SHA-256 contains $2^{256} = 16^{64} \approx 10^{77}$ different message digests.

3.3 Proof of Work and Proof of Stake

Calculating the hash function of a block is a computationally easy operation. The bitcoin protocol and other blockchain networks make it harder by introducing a level of difficulty. A miner has to add a special integer number into the header of a block, to achieve a hash that has a value lower than a predefined threshold (i.e. the hash has a number of leading zeros). Since hash values cannot be predicted and the outcome is “random”, a miner has to try many times with different numbers until it finds the right hash. This concept, called “Proof of work” (PoW) is used in Bitcoin as a consensus mechanism requiring members in a decentralized network to do some computational work to prevent bad actors from harming the system. An alternative approach is Proof of Stake (PoS), which extends the voting power to the stakeholders of the system. In PoS, participants owning crypto coins can stake them, which gives them the right to check new blocks, validate them and add them to the blockchain. PoS, which is used in some other blockchains, is newer and it is tremendously more energy efficient than PoW.

4 BLOCKCHAIN

Distributed Ledger Technology (DLT) or blockchain is a technology able to simplify and secure transactions among parties. It has to do with a growing number of blocks containing records such as transaction data or any other data that can be recorded. The blocks are linked together using hash values created with a cryptographic hash function. Each new block of data is connected with the previous, using the cryptographic hash. The hash value of a given block is part of the information stored in the next block. As a result, any small change in a block would lead to a

new hash value for the block, which would automatically invalidate all subsequent blocks. Additionally, the ledger is distributed in thousands of copies among the nodes of the network, which are also asked to validate the blocks containing the transactions [5].

General Purpose Technologies (GPTs) can affect an entire economy. They can impact economic growth and transform both our everyday lives and the ways we do business [6]. Examples of GPTs include electricity, the electric motor, the computer and the internet. Given its unique characteristics, such as immutability, transparency, and distribution [7], blockchain is recognized by many as a form of GPT. Although blockchain is still at the infrastructure building stage, it is expected to unleash several applications across different verticals within the next 5-15 years. Like the internet in its first years, blockchain is difficult to predict or even understand well, but in the future, it could become ubiquitous in the exchange of physical and digital goods.

4.1 Blockchain in Civil Engineering and Construction

Construction is one of the largest industries in the world. Blockchain has the potential to play a significant role in construction industry in the future and reshape it to the better. Shojaei [8] explored the applications of blockchain in improving information management systems in the construction industry concluding that blockchain has the potential of addressing various problems. Nawari and Ravindran [9] reviewed blockchain, how it is related to the built environment and its potential applications in the AEC industry, focusing mainly on BIM. Blockchain can be used to provide live and trustworthy information for BIM, by information sharing among present and future information owners. Furthermore, it can help enhance the benefits of BIM by allowing architects and engineers to design on the same BIM model with clear ownership, while design and construction decisions can be recorded on the blockchain for future analysis and liability.

Smart contracts, working on an "if/then" principle can identify accountabilities and trigger payments based on milestones [10]. They are executed automatically reducing the necessity of intermediaries and saving time and money. They can be used to automate agreements, thus revolutionizing construction contracts and payments which usually rely on traditional methods. Construction project management (CPM) can potentially benefit from an agile and more decentralized approach based on blockchain, with high transparency, and the parties being compensated for outcomes and work performed. The construction industry has been historically reported as one of the slowest sectors in the adaptation of information technology. Given that, the question of whether blockchain is hype or real in the construction industry was addressed by Perera et al. [11]. Their work aimed at analysing the potential of blockchain applications in construction. According to the study, blockchain has a credible potential in the construction industry, due to its exponential general use, the investments involved, and a number of start-up businesses contributing to Industry 4.0.

As urbanization is increasing rapidly, offering improved liveability and a higher standard of living, the concept of "smart cities" is one of the main focus areas of many governments attempting to establish special strategies for transforming their cities. Smart cities enable operational efficiency, maximize environmental sustainability efforts and create new citizen services. Blockchain innovation can be utilized to make cities smarter, enhancing them and

providing for better economic development and liveability [12]. Another major problem in construction and supply chain management is the disconnect between construction and design, due to the lack of trustworthy and open information across the supply chain. Blockchain can adverse these issues using open and transparent transactions [13].

5 CONCLUSION

New opportunities arise as we are moving to a digital economy where financial and physical assets will have digital representations. Although nobody can predict the degree to which Blockchain will affect the economy and our lives in the long run, most experts agree that it has the potential to play a significant role in the future, in a wide range of fields. The present study briefly examined the technical details and main concepts of blockchain technology and aimed at formulating a brief picture of the current state and practice of its use in civil engineering and construction. The study also summarized application areas related to the AEC industry where blockchain has the potential to provide new solutions. The general conclusion of the study is that although blockchain technology is new and there are certainly several early challenges to tackle, it has great potential to become an extremely positive force of change in the construction industry, in the near future.

REFERENCES

1. Wang, M., et al., *A Systematic Review of Digital Technology Adoption in Off-Site Construction: Current Status and Future Direction towards Industry 4.0.* Buildings, 2020. **10**(11): p. 204.
2. Nakamoto, S., *Bitcoin: A peer-to-peer electronic cash system.* 2008.
3. Estébanez, C., et al., *Performance of the most common non-cryptographic hash functions.* Software: Practice and Experience, 2014. **44**(6): p. 681-698.
4. Penard, W. and T. van Werkhoven, *On the Secure Hash Algorithm family*, in *Cryptography in Context*, G. Tel, Editor. 2008: Utrecht. p. 1-18.
5. Xu, J., H. Liu, and Q. Han, *Blockchain technology and smart contract for civil structural health monitoring system.* Computer-Aided Civil and Infrastructure Engineering, 2021. **36**(10): p. 1288-1305.
6. Bresnahan, T.F. and M. Trajtenberg, *General purpose technologies 'Engines of growth'?* Journal of Econometrics, 1995. **65**(1): p. 83-108.
7. Sandner, P. and P.M. Schulden, *Speciality Grand Challenges: Blockchain.* Frontiers in Blockchain, 2019. **2**(1).
8. Shojaei, A. *Exploring applications of blockchain technology in the construction industry*. in *ISEC 2019 - 10th International Structural Engineering and Construction Conference*. 2019.
9. Nawari, N.O. and S. Ravindran, *Blockchain and the built environment: Potentials and limitations.* Journal of Building Engineering, 2019. **25**: p. 100832.
10. Vigliotti, M.G., *What Do We Mean by Smart Contracts? Open Challenges in Smart Contracts.* Frontiers in Blockchain, 2021. **3**(45).
11. Perera, S., et al., *Blockchain technology: Is it hype or real in the construction industry?* Journal of Industrial Information Integration, 2020. **17**: p. 100125.
12. Valtanen, K. *Design challenges of developing a blockchain-enabled smart home*. in *2021 Conference on Information Communications Technology and Society, ICTAS 2021 - Proceedings*. 2021.
13. Tezel, A., et al., *Insights into Blockchain Implementation in Construction: Models for Supply Chain Management.* Journal of Management in Engineering, 2021. **37**(4): p. 04021038.