Blockchain and its uses

Sherif F. Fahmy

Sherif F. Fahmy is a lecturer in the Arab Academy for Science and Technology and Maritime Transport, Sheraton, Cairo, Egypt (phone: 01224469125; e-mail: fahmy@aast.edu).

January 18, 2018

ABSTRACT

Blockchain, the technology behind most cryptocurrencies that exist today, offers a paradigm shifting technology that has the potential to transform the way that we record and verify events on the Internet. By offering a decentralized, immutable, community verified record of transactions, regardless of what these transactions represent, blockchain technology promises to transform many industries. In this paper, we provide a survey of this very important technology and discuss its possible use-cases and its effect on society. The purpose of this paper is to familiarize the reader with the current state-of-the-art in the blockchain world both in terms of technology and social impact.

Keywords:
Blockchain, cryptocurrencies, smart contracts, bitcoin, ethereum, initial coin offerings

1. INTRODUCTION

Blockchain technology, as its name implies, is a chain of blocks. Each of these blocks contains a set of transactions that have been cryptographically verified to be accurate, and these blocks are connected in a chain that respects the chronological order of the transactions contained in each block – hence the name blockchain.

A blockchain represents a distributed ledger that stores the events that occur in the system. This ledger is immutable, and its contents is verified by all the nodes in the system – community verified. This simple idea provides the basis for a surprisingly wide variety of applications. The rest of this paper reviews the technology behind blockchain and then studies its uses.

2. RATIONALE

Traditional Internet applications mostly follow a centralized client-server architecture in which the server stores all of the information that is needed by the clients. Any piece of information that needs to be stored on the Internet usually ends up in a centralized client-server architecture where the server has all the information and presents a single point of failure for the entire system in terms of both security and availability.

If that server is hacked or is administered by malicious agents, the information it contains can be compromised. Likewise, if the server fails or is taken down for maintenance, the availability of the service it provides is compromised. Methods for mitigating this, usually by replicating the data on the server, still suffer from the aforementioned issues since the replicated servers are typically controlled by the same entity and are thus subject to the same security vulnerabilities and physical circumstance that may lead to downtime.

The motivation for blockchain is to provide a distributed alternative to storing information. By freeing the data from a centralized system, its security

becomes more robust and it cannot be taken down by a physical failure at a single site. An additional motivation for the initial blockchain, the one powering the cryptocurrency bitcoin, was to free the participants of the system from the tyranny of a centralized monetary authority, such as a central bank, thus providing some measure of democratization in the currency domain. From this motivation sprung a plethora of implementations of blockchains each attempting to target a particular domain of human activity. In the next section we discuss bitcoin, the original application implemented using blockchain technology.

3. BITCOIN

In a seminal white paper [17] in 2008, at the height of the US sub-prime mortgage crisis, an anonymous author, or group of authors, using the pseudonym Satoshi Nakamto, described the implementation of a blockchain that supported the creation and use of a virtual currency. This virtual currency was dubbed bitcoin. Unlike fiat money, bitcoin is not issued by a central bank, but rather created as a reward for peers in a peer-to-peer network who take it upon themselves to add a block of verified transactions to the existing bitcoin blockchain.

Let us elaborate further on that last sentence. The bitcoin network consists of a group of globally distributed computers all running open source software. When a transaction occurs, all the nodes in the system verify its authenticity. A set of the computers in the system, referred to as miners, take it upon themselves to add blocks of verified transactions to the bitcoin blockchain – in effect recording the transaction into an immutable distributed ledger. As a reward for their work, the system creates new bitcoins and assigns the newly created bitcoins to them.

So, let us assume that two agents, Alice and Bob, in possession of bitcoins wish to perform a transaction with each other. For example, assume that Bob wishes to buy a carton of lemonade from Alice for 2 bitcoins – this lemonade may be slightly overpriced as the value of one bitcoin at the time of writing this paper is about $15,000 per coin. Once Bob takes possession of the lemonade from Alice, he goes onto his computer and transfers 2 bitcoins from his digital wallet to Alice's digital wallet. This is a transaction.

The bitcoin network needs to verify that this transaction actually occurred and that Alice did not somehow surreptitiously relieve Bob of two of his bitcoins. Bob sends the transaction he has performed with Alice to the entire network. Nodes in the system, using asymmetric key cryptography, verify that the transaction is indeed authentic.

Note that all nodes in the system verify the transaction – this is referred to as community verification. Community verification is essential to ensure that consensus has been reached in the system about the veracity of the transaction. Once the transaction has been community verified and placed in a block, the miners compete for the privilege of adding it to the blockchain. Thus, all the miners in the system now compete with each other to add the block containing Bob and Alice's transaction to blocks containing previous transactions – *i.e.*, they compete to add the newest block of transactions to the bitcoin blockchain. The miner who succeeds in doing this first gets the reward because it has proved that it has done the most work. This is referred to as proof-of-work.

Now that we have a good high-level understanding of how bitcoin works, let us turn our attention to the details of these two very import steps: 1) How do nodes verify the authenticity of transactions? and 2) What exactly do miners do while competing for the privilege of adding a block to the bitcoin blockchain?

3.1 How do nodes verify transactions?

Let us now turn our attention to the method that is used by nodes in the system to verify the authenticity of transactions in bitcoin. Revisiting the example from the previous section, when Bob sends the two bitcoins to Alice, he creates a message containing the following information 1) The source of the bitcoins he will send to Alice (*i.e.*, who sent him these coins before), 2) The amount of coins he wishes to send and 3) the address of Alice's wallet. Bob should then sign this message using his private key and send it to all nodes in the system. All the nodes receiving this message do the following: first they verify that the

message was indeed sent by Bob by checking the signature on the message using Bob's public key, then they verify that the coins Bob wants to transfer (from the source specified in the message) have not already been sent to someone else – they verify this by checking the blockchain since it acts as a distributed ledger for all transactions that have occurred until now.

3.2 What do miners do exactly?

Remember that all transactions are sent to all nodes in the system. The miners in the system accumulate all valid transactions that have occurred since the last block was mined into a new block. Thus, this new block contains all the transactions that have yet to be added to the blockchain. After a set time, the miners attempt to add this new block to the bitcoin blockchain. It is at this point that they begin their proof-of-work competition phase to see who adds the block to the blockchain and thus gets the reward.

The size of each block of transactions is currently capped at 1MB, although this is a source of contention in the bitcoin community – more about this later. The question still remains, what exactly do miners do? We will try to explain this at a high level of abstraction so as not to get lost in the mathematical details.

Each block in the blockchain has a hash value generated by computing the SHA 256 algorithm [2] on its header. The hash of the last block's header is included in the header of the newly created block. This ensures that everybody in the system can verify that the current block comes after the last block in the blockchain.

The header of the current block also contains the merkle root of the transactions in the block, essentially the root of the merkle tree of all the transactions in a block. To simplify matters, this is a way to have only one hash value, the merkle root, represent all the transactions in the block without storing the hash for each transaction in the header to reduce space consumption.

To summarize, the header of the current blocks contains the merkle root and the hash of the last block's header. The header also contains the version number of the bitcoin software, a unix timestamp of the block and, more importantly for our current exposition, a difficulty target and a nonce.

For a miner to be able to add the current block to the blockchain, it should hash the header of the current block and produce a hash that conforms to the difficulty target for the block. The difficulty target, an entry in the header of the block, is simply a requirement that the produced hash of the block's header have a certain number of leading zeros in it. Of course, the larger the number of leading zeros required, the more difficult it is to produce the necessary hash.

An attentive reader should now be asking himself/herself how it would be possible to produce a hash value with a certain number of leading zeros if the SHA 256 algorithm is applied to a fixed value (the header). Applying SHA 256 on a fixed value will always return a fixed output. No matter what the difficulty level is, it is impossible to change the output of SHA 256 on a fixed value. This is where the nonce comes in. It is a value initially set to zero. The miner computes the hash with the nonce set to zero and checks if the output conforms to the difficulty level – remember that the nonce is part of the header, so changing it will change the value of the header and hence the output of the SHA 256 algorithm. If it does not, the miner increments the nonce, making it one in the second iteration, and computes the hash again. This continues until a hash value is produced that conforms to the difficulty target – essentially, the miner brute-forces the solution to the problem.

This brute-force computation is expensive, and the algorithm is designed such that the difficultly dynamically changes to reflect the computational power in the system so that, on average, a new block is mined every ten minutes.

3.3 What reward do miners get for mining?

Each time a miner adds a block to the blockchain, it is rewarded with a new issue of bitcoins as well as whatever fees were included in the transactions within the block it mined. Initially, when bitcoin was first created, the new issue of bitcoin as a reward for miners

was 50 coins. The designers of the algorithm set an upper limit to the number of bitcoins that can ever be in circulation to 21 million coins. In order to ensure that this limit is not exceeded, the reward halves every 210,000 blocks. After 64 halvings, to coin a term, the reward essentially goes down to zero, and the creation of new bitcoins ceases. We are currently at the 12.5 bitcoins reward level. The reason the designers built in this limit is to avoid money supply inflation – something that is all too common in fiat money.

3.4 Mining Hardware

The hardware that bitcoin miners use has evolved as the number of mining nodes increase in the system and, as a result, the difficulty level of the mining problem increases.

In the beginning, miners could use their CPUs to mine bitcoin. But as the difficulty increased, miners shifted to GPUs, and as the difficulty increased even further, miners shifted to custom designed hardware (ASICs – Application Specific Integrated Circuits) [10] that could solve the problem using the least amount of power consumption.

Inherent in this evolution is the fact that bitcoin mining is a tradeoff between the reward received for mining and the cost of the power consumed to perform the required calculations.

A consequences of this ever growing need for faster and more efficient hardware, is that mining has become more centralized. This occurs because it makes sense for miners to pool their resources for economies of scale and to cluster around areas with low power costs like, for example, inner Mongolia.

4. Ethereum

As can be seen, bitcoin is a digital currency application built on top of blockchain. The creators of Ethereum saw greater potential for blockchain technology [7]. Let us quickly recap what blockchain can do: it can provide an immutable distributed ledger of transactions that is community verified and that does not depend on a centralized authority for any of this. The creators of Ethereum saw that this could be used in many other fields.

Their main contribution is adding a Turing Complete Virtual Machine over the blockchain. This allows the blockchain to execute custom written code. This innovation opened the door for implementing many different ideas over blockchain.

The killer app was the design of "smart contracts" [15], software contracts that encoded agreements between two counterparties in software rules. For example, if two parties, A and B, agree that A would pay B a certain sum of money if a certain event occurs, this could be coded and placed on the blockchain.

When the triggering event occurred, the money would be transferred with no human input. The contract itself, the piece of code, would be community verified when it was entered into the system ensuring that every node in the system was aware of the terms of the contract and that they would execute it when the triggering event occurred.

Like bitcoin, the miners adding a particular block of contracts or transactions to the blockchain would be rewarded with a digital currency – Ether in the case of Ethereum.

4.1 Ethereum vs Bitcoin

The underlying technology of Ethereum is virtually the same as that used in Bitcoin, except that instead of using the SHA 256 algorithm as proof of work, Ethereum uses a more memory expensive hash function called Ethash [1].

Also, of course, Ethereum includes the Turing Complete Virtual Machine that allows users to execute code on the blockchain.

The reason that the designers of Ethereum chose a memory expensive hashing function is that they wanted to reduce the ability of hardware designers to design ASICs for mining Ether. By doing this, they thought to prevent the mining process from becoming centralized in a few custom built data centers that use custom hardware and instead leave it in the hands of ordinary users running the algorithms on their CPUs and GPUs.

4.2 DOA and the Hard Fork

One of the possibilities opened up by smart contracts is the design of a complete organization whose rules and mode of operation is encoded in a set of smart contracts.

Such an organization would not need centralized management, and would instead carry out its agenda automatically. An organization designed using this method is known as a Decentralized Autonomous Organzation (or DOA) [26].

The first DOA, called, appropriately enough, *The DOA*, unfortunately ended up in disaster [22]. *The DOA* was a venture capital firm organized around DOA principles. Initially it was a great success, and raised about $150 million through cloud-funding by May of 2016.

Unfortunately, a hacker was able to take advantage of a bug in the smart contracts of *The DOA* to siphon off about $50 million of the raised funds into a holding account. The members of Ethereum debated what to do about this and eventually created a **hard fork**, they modified the blockchain to give back the appropriated funds to their rightful owners.

This action was controversial. On one side where people who argued that by modifying the blockchain, they had essentially violated the immutable property of the chain. This may be used as a precedent by anyone in the future attempting to roll back a transaction that resulted in a loss of money.

On the other side of the argument where those who claimed that this was a one-off event that corrected an obviosly malicious attack on the funds of *The DOA*.

5. Altcoin

The success of bitcoin and it successor Ethereum has resulted in the development of a plethora of digital currencies built on blockchain. These currencies are collectively known as altcoin, short for alternatives to bitcoin. In fact, technically speaking, Ether is an altcoin. These variations of the technology typically change the proof-of-work algorithm to make it more memory intensive or otherwise tweak the underlying technology to, for example, speed up transaction processing time. Some examples of altcoin include *Litecoin, Dogecoin, Peercoin, Feathercoin, Zetacoin, and Novacoin.* These currencies are not sufficiently different from Ether and Bitcoin to warrant more extensive explanation in this paper.

6. Uses of Blockchain

Blockchain can be used for many different applications other than digital currency. In addition, the introduction of smart contracts in Ethereum opened the door for many financial applications using blockchain. In this section we will discuss some of the most prominent use-cases of blockchain.

6.1 Financial Contracts

Introducing smart contracts to blockchain allows a plethora of financial contracts to be automated on blockchain [23, 11, 13].

Financial contracts known as derivatives are particularly well suited for blockchain implementation. This is due to the fact that they are contracts built on an underlying asset. The behavior of the underlying asset provides the triggering event that causes the contract to be executed. Thus, it is easily programmed as *if(underlying asset meets a certain condition) then (do something else).*

Remember that blockchain offers community verification, this means that the terms of the contract is known to everyone and cannot be reneged on. Thus, providing security to counterparties engaging in financial contracts. It is also, in theory at least, immutable, thus providing a permanent and public record of all the contracts and what happened in them that can be used by regulatory organizations to understand the events in the market – in short, it has transparency built in.

By automating financial derivatives, it is possible to improve efficiency, increase visibility of market operation for regulatory organizations, and reduce transaction costs. Most financial derivates today are traded over the counter (OTC) which means that their pricing is untransparent and may allow market making organisations to extract large fees for their

role as financial intermediaries. Blockchain cuts out the middle-man, so to speak.

It is beyond the scope of this paper to describe all the different types of financial derivatives, but we will explain at least one, Credit Default Swaps (CDSs), as an example.

Credit Default Swaps (CDSs) are a perfect fit for the model of blockchain. In CDSs, a party, A, that is exposed to a certain credit risk – *i.e.*, that has lent some money to another entity and wishes to mitigate the risk that that entity would default on its debt – can enter into a CDS with a third party, B, that believes that the risk of default on this particular debt is acceptable.

As long as the borrower underlying this contract keeps paying its interest rates regularly, A pays regular premiums to B. If a credit event occurs, if the borrower stops paying due interest or declares bankruptcy for instance, B pays the entire face value of the debt as well as the premiums it had been receiving to A. It is sort of like insurance on the debt. This contract can easily be encoded using a programming language and executed on a blockchain so that it is automated.

6.2 Asset Tracking

Another possible use-case for blockchain is as an asset tracking tool for ascertaining proof of ownership or provenance of a particular asset [24, 8, 21].

The presence of stolen goods and so-called blood diamonds in the international supply chain is a problem that needs addressing. It is required to have a system of publicaly viewable, immutable, verified records of ownership that can be examined at any time to determine the provenance of any particular item.

Blockchain provides exactly this set of attributes and thus is a perfect fit for this application. It would make it easy for everyone to agree on who owns what, and to trace back all the transactions involving any particular item as it changed hands in the global supply chain.

6.3 Payment System

It is possible to use blockchain to implement payment systems in fiat curreny [18, 25, 5]. This is a natural extension of its ability to manage payments and transaction in cryptocurrencies.

6.4 Digital Identity

Just as blockchain can be used to track ownership and provenance of goods, it can also be used to store the identity of people [6, 16, 19, 4]. Imagine that your passport is stored on a blockchain and the visas you get and your entry and departure from countries is recorded as blockchain transactions. This means that they are immutable, community verified and decentralized. By adding smart contracts to the system it may also be possible to encode rules for denying entry to certain people – sanctions against countries of origin, security reasons or any other reason – and have them automatically implemented on the blockchain. The rules would be visible to all and automated which would reduce the possibility of human error entering into the process.

7. Distributed File Storage

Instead of placing all your data in one location on the cloud and providing a single point of failure in terms of security, privacy and reliability, it is possible to have your files stored on a blockchain [14, 27, 12].

The blockchain can be used to negotiate a price for storing your files on certain computers and its replication would provide security against data loss. Of course, the data itself would be encrypted to ensure privacy.

8. Crypocurrencies in the financial markets

We now return to the first application developed on blockchain: Cryptocurrencies. Cryptocurrencies have two important roles in the financial markets, the first is as assets in as off themselves and the second is as a novel method for raising funds for a startup. In

this section of the paper, we will discuss both these roles of cryptocurrencies.

8.1 Cryptocurrencies as an asset class

There are two ways to obtain cryptocurriences, you can either mine them as described above, or you can buy them. In this section of the paper we will concentrate on the latter. Buy and selling cryptocurrencies converts them into an asset class that can be invested or speculated in.

At the time of writing this paper, bitcoin, the cryptocurrency with the highest market capitalization, traded at about $15,000 per coin. To put this into perspective, the price of a bitcoin seven years ago was a quarter of a cent. No other asset class in the market can beat this yield.

Despite the upward trend in the market, the price of cryptocurrencies is very volatile – mainly due to small market capitalization and limited liquidity. These two factors combine to make any speculative move by investors in the asset able to move the market significantly.

The current price of $15,000 is a drop from almost $20,000 a while ago. This drop was caused by a series of bad news reports about bitcoin and cryptocurrencies in general.

Some investors claim that the current high valuation of cryptocurrencies is akin to a bubble and that buying into the market at this stage can lead to serious financial loss if the bubble bursts, but this hasn't, so far, had a lasting effect on the price of bitcoin.

So cryptocurrencies as an asset class offers the opportunity of significant yield, especially in the current low yield environment of most other assets. However, an investor getting into the market should consider the bubble like valuation of most cryptocurrencies and exercise due diligence when deciding whether or not to get into the market for the first time.

8.2 Cryptocurrencies as a fund raising mechanism

A new innovation in the financial markets is the Initial Coin Offering (or ICO) [9, 20, 3]. ICOs are an alternative to the traditional Initial Public Offering (IPO) in which firms issue equity in their company for the first time to raise operational funds.

However, unlike IPOs, ICOs do not give investors equity in a firm – at least in most cases. A ICO occurs when a new enterprise creates a new cryptocurrency (token) and then sells this token to the general public in exchange for other more established cryptocurrencies, like bitcoin or Ether, or for fiat money.

The company can then either sell the acquired bitcoin or Ether for fiat money to finance its operations or it can use the cryptocurriences to finance its operations directly, or spend the fiat money it received in return for its tokens for the same.

The issued tokens, which investors get, can then be use to buy services within the ecosystem of the newly created company – for example, buying apps on an app store or buying powerups in a digital game.

Rarely do the issued tokens confer ownership, equity, rights to the investor. They usually only offer the opportunity for investors to use them to buy services on the newly created platform. ICOs have exploded in popularity in 2017, with some estimates putting the amount raised in 2017 using this mechanism at $1.2 billion.

However, given the fact that ICOs are largely unregulated, the risk of fraud and scams is high. Recently, governments have stepped up regulation of ICOs. Countries in east Asia like China and South Korea banned them outright, while the US is considering a more nuanced approached.

The US appears to be distinguishing between two types of ICOs, those in which the tokens do not grant investors any right to partake in profits earned by the new firm and are solely a form of "money" to be used in the ecosystem of the new firm, and those that grant investors a stake in the profits earned by the new firm.

Tokens that grant investors a stake in the profit earned by the new firm are considered a security, and are thus regulated by relevant authorities as such. Tokens that do not, receive much less regulatory oversight.

This new trend has applied a little break to the burgeoning ICO market, but it is also a sign that the market is maturing and becoming more stable.

9. Disagreement and Hard Forks

Despite the fact that all cryptocurrencies are supposed to be developed using consensus, developers sometimes disagree. When such a disagreement occurs, and both sides of the argument have sufficient numbers, two different versions of the underlying blockchain and software may develop.

This scenario is referred to as a hard fork, and has occurred a number of times in the established cryptocurrencies domain. Take, for example, bitcoin. It has experienced two major hard forks. The first resulted in a new cryptocurrency called "bitcoin cash" and the second resulted in a new cryptocurrency called "bitcoin gold".

In a hard fork, the blockchain of the divergent versions are exactly the same up to a certain block, and then they diverge. In order not to start from scratch, the new branch of the cryptocurrency gives all participants in the system exactly the same amount of coins that they had before the hard fork.

For example, let us assume that participant A had 20 bitcoins before the bitcoin cash fork. After the fork, A would have 20 bitcoins as well as 20 bitcoin cash coins. This ensures that if A chooses to continue with bitcoin cash instead of bitcoin, he/she does not suffer any monetary loss.

So what was the reason for these hard forks? In the case of the hark fork that resulted in the creation of bitcoin cash, the point of contention was the size of a block in the blockchain. As previously mentioned, the size of a block in bitcoin has an upper bound of 1MB.

Some saw this as a limitation that would slow down the processing of transactions. Given the increasing number of transactions that are likely to occur as adoption of bitcoin increases, the contention was that we needed larger block sizes to increase transaction processing speeds.

The developers of bitcoin cash raised the block size to 8MB, thus bitcoin forked. The reason for the bitcoin gold fork is different.

As previously mentioned, the computationally and power expensive proof of work algorithm used in bitcoin, SHA 256, has resulted in a concentration of mining power in a number of large data centers that employ custom ASICs to perform the mining. In an attempt to reduce the reliance on ASICs, and bring mining back to normal computers, the founders of bitcoin cash changed the proof of work algorithm to Equihash, a memory expensive algorithm that makes it difficult to design ASICs to solve the mining problem.

10. CONCLUSION

In conclusion, blockchain has the potential to be a game changing technology that will affect industries as diverse as finance and cloud computing. By offering a community verified, immutable, distributed ledger of transactions it allows a plethora of use-cases that would benefit society and the economy.

Cryptocurrencies, one of the use-cases of blockchain, offer the opportunity of creating a new currency that is not controlled by a centralized authority and that is limited in amount, thus, reducing money supply inflationary pressure that occurs when central banks print more money to encourage economic growth – as the quantitative easing begun during the 2008-2009 financial crisis exemplifies.

In countries torn by run-away inflation and conflict, cryptocurrencies offer a safe haven and store of value that can be used to hedge against these risks. Financial innovations like ICOs also offer the potential to surcharge the economy by offering less expensive methods for raising money to fund new companies.

Blockchain can also be use to store proof of ownership, identity and files. All of this in a distributed, non-centralized environment. In addition, the introduction of a Turing Complete Virtual Machine on some blockchains allow them to implement smart contracts, a development that has far reaching implications for financial markets and business organization.

In short, blockchain, like machine learning, big data, and the Internet of things, is a paradigm shifting technology that will have significant effects on how we lead our lives in the coming years. This pa-

per offered a brief overview of the field and its applications, we encourage the reader to delve deeper into the technical literature surrounding this topic as we believe it is a hot research area.

REFERENCES

[1] "Ethash ethereum/wiki wiki github," https://github.com/ethereum/wiki/wiki/Ethash, (Accessed on 11/14/2017).

[2] "Sha-2 - wikipedia," https://en.wikipedia.org/wiki/SHA-2, (Accessed on 11/14/2017).

[3] R. Alvseike and G. A. G. Iversen, "Blockchain and the future of money and finance: a qualitative exploratory study of blockchain technology and implications for the monetary and financial system," Master's thesis, Norwegan School of Economics, Norway, June 2017.

[4] D. Augot, H. Chabanne, O. Clémot, and W. George, "Transforming face-to-face identity proofing into anonymous digital identity using the bitcoin blockchain," *arXiv preprint arXiv:1710.02951*, October 2017.

[5] M. Avital, J. Hedman, L. Albinsson, and M. Design, "Smart money: Blockchain-based customizable payments system," *Dagstuhl Reports*, vol. 7, no. 3, pp. 104–106, August 2017.

[6] A. Bakre, N. Patil, and S. Gupta, "Implementing decentralized digital identity using blockchain," *International Journal of Engineering Technology Science and Research*, vol. 4, no. 10, pp. 379–385, October 2017.

[7] V. Buterin, "Ethereum white paper," 2013.

[8] L. R. Cohen, L. Samuelson, and H. Katz, "How securitization can benefit from blockchain technology," *The Journal of Structured Finance*, vol. 23, no. 2, pp. 51–54, August 2017.

[9] J. P. Conley, "Blockchain and the economics of crypto-tokens and initial coin offerings," Vanderbilt University Department of Economics, Nashville, USA, Tech. Rep., June 2017.

[10] L. Dadda, M. Macchetti, and J. Owen, "The design of a high speed ASIC unit for the hash function SHA-256 (384, 512)," in *Proc. of Design, Automation and Test in Europe Conference and Exhibition, 2004.*, vol. 3. Paris,France: IEEE, February 2004, pp. 70–75.

[11] P. Danzi, M. Angjelichinoski, Č. Stefanović, and P. Popovski, "Distributed proportional-fairness control in microgrids via blockchain smart contracts," *arXiv preprint arXiv:1705.01453*, May 2017.

[12] Y. Fu, "Meta-key: A secure data-sharing protocol under blockchain-based decentralised storage architecture," *arXiv preprint arXiv:1710.07898*, October 2017.

[13] P. Gordon, M. Hood, and H. Materne-Smith, "Crypto-contracts: The coming of the blockchain revolution," *Bulletin (Law Society of South Australia)*, vol. 39, no. 3, p. 34, April 2017.

[14] H. Kopp, D. Mödinger, F. Hauck, F. Kargl, and C. Bösch, "Design of a privacy-preserving decentralized file storage with financial incentives," in *Proc. of Security and Privacy Workshops (EuroS&PW), 2017 IEEE European Symposium on.* Paris, France: IEEE, April 2017, pp. 14–22.

[15] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. Security and Privacy (SP), 2016 IEEE Symposium on.* California, USA: IEEE, May 2016, pp. 839–858.

[16] S. Muftic, "Blockchain identity management system based on public identities ledger," Apr. 25 2017, uS Patent 9,635,000.

[17] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," October 2008.

[18] H. Peter and A. Moser, "Blockchain-applications in banking & payment transactions: Results of a survey," *European Financial Systems 2017*, p. 141, June 2017.

[19] T. Poot, "Blockchain, for an enhanced passenger experience at Amsterdam Airport Schiphol," Master's thesis, Delft University of Technology, Netherlands, October 2017.

[20] J. Rohr and A. Wright, "Blockchain-based token sales, initial coin offerings, and the democratiza-

tion of public capital markets," *The Social Science Research Network (SSRN)*, October 2017.

[21] M. Ruta, F. Scioscia, S. Ieva, G. Capurso, and E. Di Sciascio, "Poster: Supply chain object discovery with semantic-enhanced blockchain," in *Proc. of 15th ACM Conference on Embedded Networked Sensor Systems*. Delft, The Netherlands: ACM, November 2017. [Online]. Available: http://sisinflab.poliba.it/publications/2017/RSICD17b/ruta_et_al_SenSys2017.pdf

[22] C. Shier, M. I. Mehar, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, M. Laskowski, and H. M. Kim, "Understanding a revolutionary and flawed grand experiment in blockchain: The dao attack," *The Social Science Research Network (SSRN)*, August 2017.

[23] M. Swan, *Blockchain: Blueprint for a new economy*. California, USA: O'Reilly Media, Inc., February 2015.

[24] D. Verma, N. Desai, A. Preece, and I. Taylor, "A blockchain based architecture for asset management in coalition operations," in *Proc. of SPIE Defense+ Security*. California, USA: International Society for Optics and Photonics, May 2017, pp. 101 900Y–101 900Y.

[25] J. Wang, Q. He, Y. Xu, Q. Han, and Z. Zhou, "An unified payment method of charging piles based on blockchain," in *Proc. of The 7th International Conference on Computer Engineering and Networks.* Shanghai, China: CENet, July 2017. [Online]. Available: https://pos.sissa.it/cgi-bin/reader/conf.cgi?confid=299

[26] J. d. Wit, "Dao, can it be viable? an exploratory research on the viability of a blockchain based decentralized autonomous organization," Master's thesis, Radbout University, Germany, July 2017.

[27] I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev, and L. Yalansky, "Ensuring data integrity using blockchain technology," in *Proc. of Open Innovations Association (FRUCT)*. St. Petersburg, Russia: IEEE, April 2017, pp. 534–539.

Authors

Sherif F. Fahmy obtained his BSc from the Computer Engineering Department in 2002 from the Arab Academy for Science and Technology and Maritime Transport in Egypt. He obtained his MSc from the same institution in 2005. In 2010 he obtained his PhD from Virginia Tech, USA. He is currently the department chair of the Computer Engineering Department in the Arab Academy for Science and Technology and Maritime Transport in Cairo, Egypt. He is also an IEEE member and is under review for promotion to senior IEEE member. Sherif F. Fahmy has been in academia for 15 years.