Editorial

Paul Mueller*

Application of blockchain technology

<https://doi.org/10.1515/itit-2018-0035>

The blockchain technology foremost known in 2008 as the underlying technology of the cryptocurrency Bitcoin is a technology which was first introduced by Stuart Haber and W. Scott Stornetta [1] in 1991 as a cryptographically secured chain of blocks. Their basic idea was to implement a system in which document timestamps could not be corrupted. This idea was extended [2] in 1992 with the so called Merkle trees accepting different certificates to be collected into one block.

Despite its earlier roots, the breakthrough of the blockchain technology only came 17 years later in 2008 when Satoshi Nakamoto (a pseudonym used by an individual or a group of peoples) published the paper “Bitcoin: A Peer-to-Peer Electronic Cash System” [3]. The basic architecture of the Bitcoin blockchain is a confluence of three basic technologies as of cryptography, peer-2-peer systems and consensus mechanisms [4]. In the light of this, it is more likely that “Satoshi Nakamoto” is a group of people coordinating the knowledge of these three fields of research rather than a single genius experienced in all these fields. Inspired by the success of Bitcoin, a lot of systems attempting to mimic Bitcoin’s success appeared, with Litecoin (2011) [5], Ripple (2012) [6], or Monero (2014) [7] as only a few¹ of the more well-known examples. Also, the Hyperledger project (2015) [8] of the Linux foundation as an umbrella project of open source blockchains and related tools, which started in 2015 should be mentioned here.

Because the Bitcoin architecture is based on a simple Forth-like scripting language called Script [9] which is not Turing complete, it has no great flexibility and is therefore mainly restricted to money transfer. Moreover, there are other shortcomings like power wastage for consensus building [10], transaction fees which are not acceptable for micro payments and data exchange in the Internet-of-Things (IoT) context, and last but not least the storage of

illegal content in the Bitcoin blockchain [11]. Moreover, currently the Bitcoin blockchain shows signs of increasingly contradicting its promised decentralized nature due to an ever-increasing centralization of the hashing power to only a few mining pools [12].

To overcome these shortcomings new approaches appeared over time. First of all, the Ethereum architecture must be mentioned [13]. Ethereum called itself a world-computer where all Ethereum nodes have a build in Turing complete programming language able to perform any programs which are called “smart contracts” [14].

Ethereum’s core innovation, the Ethereum Virtual Machine (EVM) [15] is a Turing complete software that runs on each node in the Ethereum network. Given enough time and money, the EVM enables anyone to run to run any program, regardless of the programming language. Compared to Bitcoin’s rudimentary scripting language, the EVM makes the process of creating blockchain applications much easier and efficient than before. Instead of having to build an entirely original blockchain for each new application, Ethereum enables the development of different decentralized applications (the so called DAPPS). Based on smart contracts, Ethereum can also be used to build Decentralized Autonomous Organizations (DAO) with no single leader. A DAO runs on a collection of smart contracts which are designed to replace the rules and structure of a traditional organizations by programming code. Although smart contracts bringing a number of benefits, DAPPS or DAO’s are only as good as the underlying code is faultless. Otherwise a mistake in the code can lead to unintended situations as happened to the “The DAO” project [16], which was hacked shortly after the token sale ended and subsequently lost around \$50 million dollars at the time.

Another new technology is IOTA [17], led by the IOTA Foundation which was established in Germany as a formal, non-profit organization (‘gemeinnützige Stiftung’) in 2017. IOTA departs from cryptographically secured chain of blocks and replaces it with a technology based on directed acyclic graph (DAG) based technology called Tangle. The promise of IOTA is a free of charge interchange of data especially designed for data exchange in the IoT world. Although it is in its infancy, IOTA is very promising for interconnecting the small devices in the IoT world. Although this issue does not address IOTA, it is worth to

¹ <https://coinmarketcap.com/all/views/all/>

*Corresponding author: Paul Mueller, University Kaiserslautern, D-67663 Kaiserslautern, Germany, e-mail: pmueller@rhrk.uni-kl.de

mention IOTA here because a forthcoming issue will focus on this idea.

This special issue on the Blockchain consists of five papers exploring new and demanding tasks for the Bitcoin and Ethereum blockchain. The papers focus on different application domains, from time-stamping to document ownership and supply chain management. In the following, I will highlight the contributions of each paper:

Paper 1 from Roth et al. “Message exchange on base of a blockchain-based layered architecture” presents a layered model for blockchain-based applications that are particularly modular due to this architecture. With the help of these layers, an application can be migrated by exchanging the wrapper between different blockchains or, in case of a large protocol change, simply adapted without having to adapt the application layer. This new layered model is applied to a blockchain-based messaging service.

Paper 2 from Petersen et al. “Mapping the Sea of Opportunities: Blockchain in Supply Chain and Logistics” presents a survey that looks at the expectations of Blockchain technologies and its use in supply chains. The authors look beyond the blockchain hype and shed light on the expectations of industry professionals towards the benefits and challenges of the blockchain technology. They also categorize current Blockchain applications that are expected to provide tangible benefits for supply chain and logistics processes.

Paper 3 from Hepp et al. “OriginStamp: A System for Decentralized Trusted Timestamping” introduces a system for decentralized trusted Timestamping called OriginStamp. A current problem with certified timestamps is that they are certified by a central authority. This paper builds on a concept of decentralized trusted timestamping. The authors provide a detailed description of a system, illustrating the building and functionality of a decentralized timestamping service.

Paper 4 from Hepp et al. “On-chain vs. Off-chain Storage for Supply- and Blockchain integration” discusses blockchain technologies with respect to on-chain and off-chain storage, verification cost, and secure data sharing. The paper’s links to this issue’s theme are quite strong, because supply chains, which are an integral building block of commerce, have a natural information exchange (flow) between adjacent links in the chain. Hence, questions arise about the correctness and integrity of processes within the supply chain.

Paper 5 from Rizk et al. “Brokerless Inter-domain Virtual Network Embedding: A Blockchain-based Approach” first discusses first centralized and decentralized virtual network embedding (VNE) approaches and shows how a

blockchain approach can be applied to this domain. The approach comprises of a broker-less blockchain-based system, that uses smart contracts and a partitioning algorithm based on the Vickrey auction model. The article then proceeds to investigate the feasibility of the proposed approach by finalizing the behavior of the introduced auction model in adverse conditions and by evaluating the blockchain performance given different consensus protocols.

References

1. Haber, S.; Stornetta, W. S.: “How to time-stamp a digital document”. In: *Journal of Cryptology*. 3 (2), 1991, pp. 99–111.
2. Bayer, D.; Haber, S.; Stornetta, W. S.: Improving the Efficiency and Reliability of Digital Time-Stamping. In: *Journal Sequences II: Methods in Communication, Security and Computer Science*, 1993, pp. 329–334.
3. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
4. Müller, P.; Bergsträßer, S.; Rizk, A. and Steinmetz, R.: The Bitcoin Universe: An Architectural Overview of the Bitcoin Blockchain. In: *Lecture Notes in Informatics (LNI)*, Vol. 283, 2018, pp. 1–20.
5. Litecoin: URL <https://litecoin.org/> (accessed Nov. 2018).
6. Ripple: URL <https://ripple.com/> (accessed Nov. 2018).
7. Monero: URL <https://getmonero.org/> (accessed Nov. 2018).
8. Hyperledger: URL <https://www.hyperledger.org/> (accessed Nov. 2018).
9. Script: URL <https://en.bitcoin.it/wiki/Script> (accessed Nov. 2018).
10. Energy Consumption: URL <https://digiconomist.net/bitcoin-energy-consumption> (accessed Nov. 2018).
11. Matzutt, R.; Hiller, S.; Henze, M.; Ziegeldorf, J. H.; Müllmann, D.; Hohlfeld, O. and Wehrle, K.: A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin, In: *Proc. 22nd International Conference on Financial Cryptography and Data Security*, 2018.
12. Hashing Pools: URL <https://www.blockchain.com/en/pools> (accessed Nov. 2018).
13. Buterin, V.: Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2013, URL <https://github.com/ethereum/wiki/> (accessed Nov. 2018).
14. Szabo, N.: Formalizing and securing relationships on public networks. *First Monday*, 2 (9), 1997, URL <http://firstmonday.org/ojs/index.php/fm/article/view/548> pools (accessed Nov. 2018).
15. Wood, G.: Ethereum: A Secure Decentralised Generalised Transaction Ledger, 2018, URL <https://ethereum.github.io/yellowpaper/paper.pdf> (accessed Nov. 2018).
16. The DAO project: URN [https://en.wikipedia.org/wiki/The_DAO_\(organization\)](https://en.wikipedia.org/wiki/The_DAO_(organization)) (accessed Nov. 2018).
17. Popov, S.: The Tangle, 2018, URL <https://www.iota.org/research/academic-papers> (accessed Nov. 2018).

Bionotes

Prof. Dr. Paul Mueller
University Kaiserslautern, D-67663
Kaiserslautern, Germany
pmueller@rhrk.uni-kl.de

Prof. Dr. Paul Müller studied Mathematics, Information-Technology, and Economics at the University of Bochum. He started his academic career as a researcher at the University of Tübingen and Ulm, where he received his doctoral degree in Mathematics in 1983. In 1995 he accepted an offer from the University of Kaiserslautern on a full professor position in the department of computer science in conjunction with heading the university's central computing center. His research group "Integrated Communications Systems Lab. (ICSY)" within the department of computer science is aiming at the development of services to implement integrated communication within the context of distributed systems. Based on his experience on Internet based distributed systems he is also active in the emerging field of distributed ledger technology since 2010.