A Systematic Review of Blockchain Hardware Acceleration Architectures

Aidan O Mahony
Department of Electrical and Electronic Engineering
University College Cork
Ireland
103837793@umail.ucc.ie

Emanuel Popovici
Department of Electrical and Electronic Engineering
University College Cork
Ireland
E.Popovici@ucc.ie

***Abstract*—The aim of this paper is to provide a systematic literature review of blockchain hardware acceleration. Blockchain technology has achieved significant attention in recent years particularly in the area of cryptocurrency however it is gaining popularity in other applications such as supply chain management and e-government.**

Based on a structured, systematic review of the relevant literature, we present a classification of the primary areas in blockchain technology that make use of heterogeneous hardware for accelerating certain blockchain functions. Based on these findings, we identify various research gaps and future exploratory directions that are anticipated to be of significant value both for academics and industry practitioners.

***Index Terms*—Blockchain, Distributed Ledger Technology, Hardware Architecture, Systematic Literature Review, Consensus Algorithms, Heterogeneous Hardware, FPGA, GPU, ASIC, CPU**

I. Introduction

A blockchain is essentially a distributed database ledger of transactions [1]. The entries in this ledger are the transactions that have been executed and shared on the blockchain network. In order to be accepted as an entry in this ledger the transaction is verified by consensus by the participants in the network. It is not possible to delete or modify entries once they have been accepted as valid by this majority.

Blockchain has applications in any area which would benefit from using a distributed ledger. Some example areas are E-government [2], IoT [3], cryptocurrency [4], supply chain information exchange [5], and smart contracts [6]. As can be easily inferred, blockchain makes use of certain cryptographic properties to ensure the ledger remains consistent. Similar to other applications, heterogeneous hardware is often introduced to computationally intense problems as a mechanism for improving performance [7].

The contribution of this paper is to provide a better understanding of the current heterogeneous hardware applications to blockchain technology, provide an analysis of the impact of these contributions, and to identify open challenges in this space.

978-1-7281-2800-9/19/$31.00

II. Background

A. Blockchain technology

Blockchain is a database that stores all transactions grouped in blocks. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. When a new transaction is created, the sender broadcasts it in the peer to peer network to all the other nodes. As the nodes receive the transaction, they validate it and keep it in their transactional pools. To validate transactions means to run predefined checks about the structure and the actions in the transaction. Special node types called miners create a new block and group some of the available transactions from their transaction pool. Then the block is mined, which is a process of finding the proof of work[1] using variable data from the new block's header. Finding the proof of work is the calculation of a cryptographic hash that fits the defined difficulty target.

The goal of mining is twofold, it verifies the legitimacy of a transaction and prevents double spending[2]. The miner that first finds a solution for its block is the winner. This candidate block becomes the new block in the chain. Because transactions are added in the mining block as they arrive, we can say that the latest block in the Blockchain contains the latest transactions. When a new block is created (mined) it is time-stamped and propagated to the network. Every node receives the block, validates it, validates the transactions in it, and adds the block to his local Blockchain copy. The transactions included in the block become authorized and non-reversible part of Blockchain in the moment the block is accepted by majority of the nodes. Blocks can also be inspected as a way of transactional and financial clearing.

In addition to transactions, every block stores some meta-data and the hash value of the previous block. So every block has a pointer to its parent block. That is how the blocks are linked, creating a chain of blocks called Blockchain. The ledger is publicly available for everybody to inspect the blocks

[1]A proof of work is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated. Bitcoin uses the Hashcash proof of work system.

[2]Double spending is the case where a single transaction is recorded twice, or in the case of currency, if the currency was spent twice

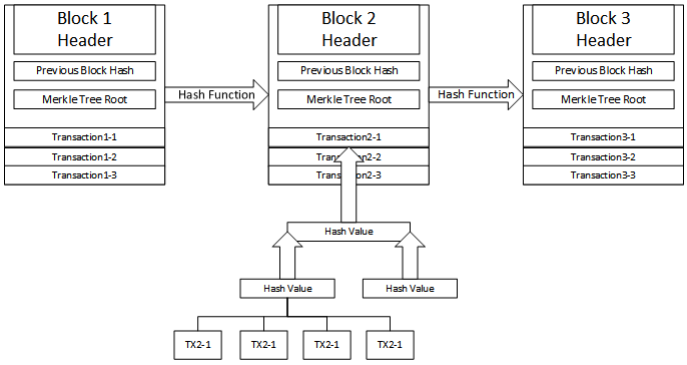

Figure 1. Blockchain Structure

and the transactions within. Figure 1 shows an example of a blockchain structure which consists of a block header (which contains version information, difficulty target, a nonce, and other information), the previous block hash, the hash of the root of the merkle tree, and the transactions contained in the block.

B. Hardware Acceleration

There are several types of hardware accelerators available today and we provide a brief description of a number of these accelerators in this section.

A field-programmable gate array (FPGA) is an integrated circuit (IC) that is structurally reconfigurable at hardware level and can be reprogrammed regularly after manufacturing. Major effort has been made by technology leaders to better integrate FPGA accelerators within data center servers (e.g. Microsoft Catapult, IBM CAPI, Intel Xeon+FPGA) as well as applications for machine learning.

A Graphics Processing Unit (GPU) is a single-chip processor primarily used to manage and boost the performance of video and graphics. The most popular GPUs are manufactured by Nvidia, Intel, and AMD. This type of technology has found areas of applications outside of graphics including bioinformatics and artificial intelligence.

Application Specific Integrated circuits (ASICs) are highly optimised circuits dedicated to a specific domain of applications ranging from communications and networking to computing to storage. There are many companies offering ASIC solutions for these domains which require high performance circuits.

We also consider application specific hardware within General Purpose CPUs as hardware acceleration. Examples of application specific CPU hardware acceleration is the CLMUL instruction set from Intel and AMD which improves performance of applications which use Galois multiplications (e.g. Elliptic Curve Cryptography).

III. Related Work

There is substantial research already in existence in terms of systematic reviews of Blockchain technology. In [8] the authors extracted 41 primary papers from scientific databases which highlight the majority of research in this area is concentrated on bitcoin however there is a certain amount of research into other application e.g. smart contracts and licensing.

In [9], the authors found 18 use cases of blockchain in the literature used in IoT use cases. And there are literature reviews on the topics of Blockchain and Smart Government [2], Blockchain and Bitcoin [4], Blockchain and Smart Contracts [6], and Blockchain and Big Data [10]. However, to the best of our knowledge, there is no systematic review concerned with Blockchain and Hardware Acceleration.

IV. Research Methodology

A. Literature Search

To conduct the study, we followed the guidelines on Systematic literature review (SLR) provided by Kitchenham et al [11] and Budgen et al [12] and [13]. An extensive search was performed in the following databases: IEEE Xplore; ACM Digital Library; SpringerLink; ScienceDirect; Google Scholar; ProQuest. We gathered 2497 papers.

B. Literature Selection

In order to decide which of the research to deeply analyze, we performed three exclusion stages. Firstly we filtered the papers based on titles, excluding titles which clearly were not relevant. Secondly, in reading the abstracts, we excluded papers regarding non-engineering aspects (e.g. papers addressing ethical issues of the blockchain or purely economic aspects of cryptocurrencies). After the second phase we were left with 37 papers. Finally, on reading these 37 papers, we arrived with 22 papers which dealt specifically with hardware acceleration of blockchain functions.

C. Categorization

From reading the 22 papers we were able to create seven categories:

1) Blockchain searching - four papers in the area of blockchain queries.
2) Hardware-Assisted Trusted Execution Environments - four papers taking advantage of trusted executed environments.
3) Cryptographic Acceleration - three papers in a area of cryptographic acceleration related to blockchain technology.
4) Currency Mining - three papers in the area of currency mining (this area contains significantly more research than three papers however our review is not concerned solely with currency mining).
5) Internet of Things - two papers detailed IoT specific blockchain application acceleration.
6) Physical Unclonable Functions - three papers exploring PUFs.
7) Miscellaneous Blockchain Hardware - two papers which did not fit into any of the previous categories.

We discuss these categories in more detail in the next section.

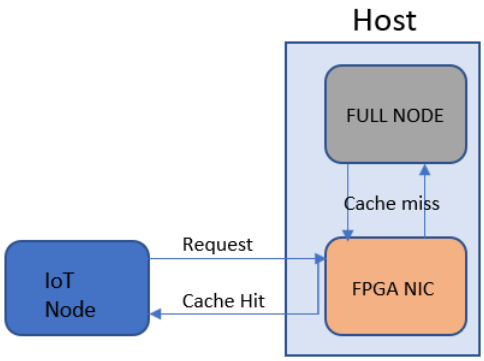

Figure 2. FPGA NIC in IoT environment

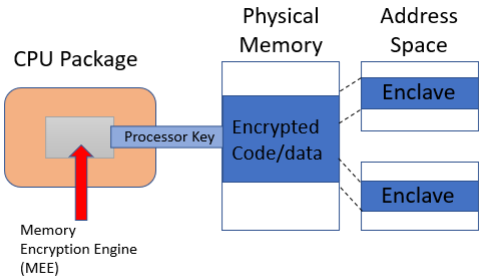

Figure 3. SGX Enclave

V. Blockchain Hardware

A. Blockchain searching

A key-value database, or key-value store, is a data storage paradigm designed for storing, retrieving, and managing associative arrays, a data structure more commonly known today as a dictionary or hash table. As mentioned earlier, blockchain is analogous to a distributed database and one popular type of database which scales out well is that of the Key-Value database [14]. Three papers we reviewed dealt with accelerating Key-Value Stores (KVS) which store transmission IDs (TXID) as a key and Merkle Root as a value.

In [15] the authors designed and implemented a prototype NIC with a key-value data store written in a P4 language on the FPGA that has four 10Gigabit Ethernet(10GbE) interfaces. One of the primary drivers for the improved throughput[3] is the integration of this FPGA-NIC into an IoT environment. The IoT devices in this environment are not capable of storing the blockchain and therefore depend on a server to provide a part of the blockchain in order for the IoT to verify if the transaction has already been approved by the blockchain. Therefore, reducing the load of the "full node" (the node which does have a copy of the blockchain) is important and can be achieved by using this KVS FPGA-NIC and is illustrated in figure 2.

The authors of [16] and [17] take advantage of the Reduced Latency Dynamic Random Access Memory (RLDRAM) of the FPGA to get some of their latency reduction. They also make reference to how they believe their solution is particularly important for IoT devices. Their solution improved the throughput of blockchain queries by a factor of 1.97.

An alternative to FPGAs for searching is presented in [18]. In this paper the authors propose an acceleration method of Blockchain search using GPUs. More specifically, they introduce an array-based Patricia tree structure[4] suitable for GPU processing so that more effective use of the Blockchain feature that there are no update and delete queries can be taken advantage of.

[3]Throughput is measured as the number of successful transactions per second starting from the first transaction deployment time.

[4]A Patricia tree is a mixture of Radix tree and Merkle tree [19]

B. Hardware-Assisted Trusted Execution Environments

A Trusted Execution Environment (TEE) is a secure area inside a main processor which guarantees that the code and data loaded in the TEE are protected with respect to confidentiality and integrity. A number of hardware vendors support TEEs, including Software Guard Extensions (SGX) from Intel [20] and TrustZone from ARM.

In [21] the authors present a message aggregation technique that combines hardware-based trusted execution environments with secret sharing. Using the TEE facilitates a reduction in the number of communication phases required for Byzantine Fault Tolerance (BFT) protocols.

ShadowEth [22] is a trust-less off-chain smart contract system which uses Intel SGX. This application uses SGX to provide remote attestation. The goal of ShadowEth is to provide a confidential platform to execute private smart contracts which can be integrated with existing public blockchain such as Ethereum.

The authors of [23] present a cryptocurrency exchange system which overcomes the problem of frontrunning attacks by using Intels SGX trusted execution environment. Frontrunning is a course of action where someone benefits from early access to market information about upcoming transactions and trades. In the case of blockchain, frontrunning can be exploited by the miner who has knowledge of the transactions contained in a new block.

SGX is used in [24] to construct a more efficient blockchain mining framework. Instead of using a Proof-of-Work (PoW) system, they introduce a Proof of Useful Work (PoUW) mechanism to reduce resource wastage. The PoUW is created by using information generated by a hardware protected key combined with an SGX protected enclave.

A final point to make with regard to hardware-assisted TEE is recent publication of SGX exploits. A recent published attack - *Foreshadow* [25] - can extract data from SGX enclaves, and a very recent paper details a SGX-ROP attack [26] which demonstrates the first enclave malware which impersonates its host application.

Figure 4. Ant Miner

C. Mining

As there is no central authority or central bank, there has to be a way of gathering every transaction carried out in order to create a new block. Network nodes that carry out this task called dubbed ”miners”. Every time a number of transactions are grouped into a block, this is appended to the blockchain. Whoever appends the block is rewarded with cryptocurrency. In order to successfully create a block, it must be accompanied by a cryptographic hash (typically SHA-256) that fulfills certain requirements (e.g. in the case of bitcoin the hash must have a value below a certain target). The only feasible way to arrive at a hash matching the correct criteria is to simply calculate as many as possible and wait until you get a matching hash. The promise of a reward is a motivator for hardware acceleration.

In [27] the author presents a SHA-256 accelerator with a DMA module which is integrated into a tile (called Single-ISA Heterogeneous MAny-core Computer, *SHMAC*) and a system with multiple cores is used to exploit the thread-level parallelism provided by the platform. The author noted that this approach did not lead to a performance gain when compared to FPGA based miners but the author noted that this approach lends itself well to thread-level parallelism.

The authors of [28] introduces us to the ”ASIC Cloud”. This paper also provides a useful introduction to the four generations of mining hardware; first generation CPU based, second generation GPU based, third generation FPGA based, and fourth generation ASIC based. An ASIC cloud is a purpose-built datacenter comprising large arrays of ASIC accelerators (we see an example of an ASIC miner in figure 4). This paper deals quite a bit with the power consumption of ASIC cloud mining.

In [29] the methods of performing Bitcoin mining on custom and non-custom hardware are discussed. In the non-custom hardware space the author investigates SHA256 computations on CPU via the SSE2 instruction set and GPU via CUDA/OpenCL . With regard the custom hardware the author presents ASIC and FPGA miner. There are conclusions made and the author also discusses some illegal methods of mining.

The topic of SHA hardware acceleration is a wide field and could indeed be the subject of another systematic review.

D. Cryptographic Acceleration

This section is concerned with cryptographic acceleration outside of the SHA algorithm which is used in blockchain mining.

In [30] a proposal for a smart gas payment system containing an embedded bitcoin payment module is proposed. This smart meter consists of a processor with the bitcoin wallet stored on it and a ATECC108A cryptographic offload chip from Atmel which implements Elliptic Curve Cryptography.

The authors of [31] examine the implementation and acceleration of the Poly1305 authentication algorithm on the IBM z14 mainframe computer. The authors restructured the Poly1305 algorithm to take advantage of a new instruction, vector multiply sum logical (VMSL), which employs floating-point hardware to perform highspeed high-throughput multiplications and then they create better scheduling for parts of the algorithm that are performance bottlenecks. This achieved a 7% reduction in processing time. The Poly1305 algorithm is a proposed cipher for use within some blockchain implementations.

In [32] the authors propose a novel two-stage scalable modular multiplication algorithm. Their experimental results (implemented using a CMOS-based ASIC) show that the improves the energy efficiency by 45.9%, the area efficiency by 93.6% and achieves 8x of throughput per area compared with the state-of-the-art CMOS-based implementation. The connection with blockchain is not as clear with this example however the RSA algorithm and elliptic curve cryptography are used in blockchain.

E. Internet of Things

The Internet of Things (IoT) refers to the network of numerous physical objects (20 billion by 2020, according to Gartner [33]) which are provided with an internet connection.

In [34] the authors describe the challenge with regard to blockchain employment in the context of IoT due to the IoT device’s hardware limitations. To address the challenge, this paper proposes an IoT ledger-based architecture to ensure access control on heterogeneous scenarios. This research applies the new architecture to conventional devices used in IoT networks, such as Arduino, Raspberry and Orange Pi boards.

An evaluation on RSA and ECC-Based Cipher Suites for IoT applications is presented in [35] where a high-security energy-efficient fog and mist computing architecture and a testbed is presented. This research used the ESP32 microcontroller and an Orange Pi. This article not only presents a novel mist computing testbed, but also provides guidelines for future researchers to find out efficient and secure implementations for advanced IoT devices.

F. Physical Unclonable Functions

A Physical Unclonable Functions (PUF) is a platform-unique function which, when supplied with an input challenge,

produces an output response determined by the behavior of a complex, unclonable physical system. PUFs can be used for authentication of chips and can generate secret keys required for cryptographic operations without the need for expensive non-volatile memories.

The authors of [36] describe a combination of Blockchain and sensor based PUF authentication for solving real-time but non-repudiable access to IoT devices in a Smart Home. It achieves this by utilizing a mining less consensus mechanism for the provision of immutable assurance to users and IoT devices transactions. As this paper describes a private blockchain, the usual rewards for mining are not required and since this blockchain is run in a private network there is no mining required at all. The PUF function is based on a biometric based user fingerprint implementation.

In [37] PUFs are used to counter impersonation and data tampering attacks in IoT environments. The paper incorporates PUFs with Ethereum (a blockchain with smart contracts) in these environments. In this situation the PUF and IoT functions are integrated into a system-on-chip (SoC). The authors then describe how this SoC blockchain/PUF approach can counter IoT attacks.

An embedded physically unclonable function which is used to establish the legitimacy of an IC's current owner is presented in [38]. This is carried out by using the PUF with other information to construct a record of the IC ownership. This information is then stored in an *ownership* blockchain. The owners of an IC are assigned an address which is generated from an ECDSA public/private key. This paper also describes a protocol for ownership transfer.

G. Miscellaneous Blockchain Hardware

There were a number of papers that dealt with blockchain hardware which did not fit into any of the other categories. These are presented here.

A Raspberry Pi is the focus in [39]. The authors present a blockchain based distributed controller for the efficient share of energy storage systems in energy communities. Blockchain has a growing number of uses regarding the energy sector and the smart grid [40].

In [41] the authors describe a situation where abnormality detection in the Blockchain at high speed is computationally heavy. The reasons put forward is that there is a need to repeat the detection process using various feature quantities and the feature extractions which become overhead. In order to accelerate abnormality detection, they propose a method which caches transaction information required in GPU device memory and perform both feature extraction and abnormality detection in the GPU. They employ abnormality detection using K-means algorithm based on the conditional features and when the number of users is one million and the number of transactions is 100 millions, this proposed method is 37.1 times faster than CPU processing method and 16.1 times faster than GPU processing method that does not perform feature extraction on the GPU.

VI. Discussion/Research Questions

From the analysis of the selected literature, a series of insights can be derived concerning the limitations of the blockchain technology and its usability across a wide area of domains. There are several technical areas discussed in [42] which are relevant from a hardware acceleration perspective. These are

- Throughput (read or transaction) - defined as how many read operations (RPS) or transactions per time unit (TPS) can be carried out.
- Latency - (read or transaction) - defined as the time between when the read request is submitted and when the reply is received or the time taken for a transaction's effect takes to be usable across the network.
- Size - defined as the size of the blockchain database. If the throughput of bitcoin increases to the levels of VISA it is predicted that the bitcoin blockchain could grow 214PB each year. This is a serious concern.
- Security - blockchain is susceptible to the 51% attack[5].
- Wasted resources - Bitcoin emissions alone could push global warming above 2°C [43] within less than three decades. As one could imagine, this is a serious concern.

Throughput is addressed in [17] [17] [16] via caching, latency is addressed in [31] [32], security is discussed in [36] [37] [38], and wasted resources is touched on in [39].

There are gaps in blockchain research in the areas of size and bandwidth with regard to blockchain acceleration architecture. Based on a cursory search of the literature, blockchain size is addressed primarily by data reduction (e.g. Lempel-Ziv, entropy encoding) however there is no application of hardware architectures to the problem of blockchain size.

VII. Conclusion

While blockchain applications are being widely deployed, many issues have yet to be addressed. Some of these issues have serious implications to blockchain adoption (i.e. power consumption and wasted resources) and require further examination. Once these issues are resolved, blockchain will be more scalable and efficient and therefore will be more widely adopted.

Our research has identified the gap in research into heterogeneous architectures and hardware acceleration to the problem of resource wastage and the size of blockchain.

VIII. Acknowledgments

This paper has been supported in part by Intel Programmable Solutions Group and by the Insight Centre for Data Analytics.

[5]51% attack refers to an attack on a blockchain by a group of miners controlling more than 50% of the network's mining hash rate, or computing power. The attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. They would also be able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins.

REFERENCES

[1] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman *et al.*, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, no. 6-10, p. 71, 2016.

[2] H. Hou, "The application of blockchain technology in e-government in china," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, July 2017, pp. 1–4.

[3] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, Feb 2017, pp. 464–467.

[4] P. Vigna and M. J. Casey, *The age of cryptocurrency: how bitcoin and the blockchain are challenging the global economic order*. Macmillan, 2016.

[5] D. Dujak and D. Sajter, "Blockchain applications in supply chain," in *SMART Supply Network*. Springer, 2019, pp. 21–46.

[6] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *2016 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2016, pp. 467–468.

[7] S. Suneja, E. Baron, and R. Johnson, "Accelerating the cloud with heterogeneous computing." in *HotCloud*, 2011.

[8] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?a systematic review," *PloS one*, vol. 11, no. 10, p. e0163477, 2016.

[9] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the internet of things: A systematic literature review," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. IEEE, 2016, pp. 1–6.

[10] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *IEEE EUROCON 2017-17th International Conference on Smart Technologies*. IEEE, 2017, pp. 763–768.

[11] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," *Information and software technology*, vol. 51, no. 1, pp. 7–15, 2009.

[12] D. Budgen and P. Brereton, "Performing systematic literature reviews in software engineering," in *Proceedings of the 28th international conference on Software engineering*. ACM, 2006, pp. 1051–1052.

[13] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55 – 81, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0736585318306324

[14] G. DeCandia, D. Hastorun, M. Jampani, G. Kakulapati, A. Lakshman, A. Pilchin, S. Sivasubramanian, P. Vosshall, and W. Vogels, "Dynamo: amazon's highly available key-value store," in *ACM SIGOPS operating systems review*, vol. 41, no. 6. ACM, 2007, pp. 205–220.

[15] Y. Sakakibara, Y. Tokusashi, S. Morishima, and H. Matsutani, "Accelerating blockchain transfer system using fpga-based nic."

[16] Y. Sakakibara, S. Morishima, K. Nakamura, and H. Matsutani, "A hardware-based caching system on fpga nic for blockchain," *IEICE Transactions on Information and Systems*, vol. 101, no. 5, pp. 1350–1360, 2018.

[17] Y. Sakakibara, K. Nakamura, and H. Matsutani, "An fpga nic based hardware caching for blockchain," in *Proceedings of the 8th International Symposium on Highly Efficient Accelerators and Reconfigurable Technologies*. ACM, 2017, p. 1.

[18] S. Morishima and H. Matsutani, "Accelerating blockchain search of full nodes using gpus," in *Parallel, Distributed and Network-based Processing (PDP), 2018 26th Euromicro International Conference on*. IEEE, 2018, pp. 244–248.

[19] D. Vujičić, D. Jagodić, and S. Ranđić, "Blockchain technology, bitcoin, and ethereum: A brief overview," in *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*. IEEE, 2018, pp. 1–6.

[20] S. Gueron, "A memory encryption engine suitable for general purpose processors." *IACR Cryptology ePrint Archive*, vol. 2016, p. 204, 2016.

[21] J. Liu, W. Li, G. O. Karame, and N. Asokan, "Scalable byzantine consensus via hardware-assisted secret sharing," *IEEE Transactions on Computers*, vol. 68, no. 1, pp. 139–151, 2019.

[22] R. Yuan, Y.-B. Xia, H.-B. Chen, B.-Y. Zang, and J. Xie, "Shadoweth: Private smart contract on public blockchain," *Journal of Computer Science and Technology*, vol. 33, no. 3, pp. 542–556, 2018.

[23] I. Bentov, Y. Ji, F. Zhang, Y. Li, X. Zhao, L. Breidenbach, P. Daian, and A. Juels, "Tesseract: Real-time cryptocurrency exchange using trusted hardware." *IACR Cryptology ePrint Archive*, vol. 2017, p. 1153, 2017.

[24] F. Zhang, I. Eyal, R. Escriva, A. Juels, and R. Van Renesse, "{REM}: Resource-efficient mining for blockchains," in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, 2017, pp. 1427–1444.

[25] O. Weisse, J. Van Bulck, M. Minkin, D. Genkin, B. Kasikci, F. Piessens, M. Silberstein, R. Strackx, T. F. Wenisch, and Y. Yarom, "Foreshadow-NG: Breaking the virtual memory abstraction with transient out-of-order execution," *Technical report*, 2018, see also USENIX Security paper Foreshadow [44].

[26] M. Schwarz, S. Weiser, and D. Gruss, "Practical enclave malware with intel sgx," 2019.

[27] T. Langland and K. K. Skordal, "Mining bitcoins using a heterogeneous computer architecture," Master's thesis, NTNU, 2015.

[28] I. Magaki, M. Khazraee, L. V. Gutierrez, and M. B. Taylor, "Asic clouds: Specializing the datacenter," in *Computer Architecture (ISCA), 2016 ACM/IEEE 43rd Annual International Symposium on*. IEEE, 2016, pp. 178–190.

[29] J. A. Dev, "Bitcoin mining acceleration and performance quantification," in *Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on*. IEEE, 2014, pp. 1–6.

[30] A. Xu, M. Li, X. Huang, N. Xue, J. Zhang, and Q. Sheng, "A blockchain based micro payment system for smart devices," *Signature*, vol. 256, no. 4936, p. 115, 2016.

[31] U. S. Gadriwala, C. K. Anand, C. D'Alves, and B. O'Farrell, "Accelerating poly1305 cryptographic message authentication on the z14," in *Proceedings of the 27th Annual International Conference on Computer Science and Software Engineering*. IBM Corp., 2017, pp. 48–54.

[32] T. Luo, B. He, W. Zhang, and D. L. Maskell, "A novel two-stage modular multiplier based on racetrack memory for asymmetric cryptography," in *Computer-Aided Design (ICCAD), 2017 IEEE/ACM International Conference on*. IEEE, 2017, pp. 276–282.

[33] I. Gartner, "Gartner says 6.4 billion connected" things" will be in use in 2016, up 30 percent from 2015," *Stamford, Conn. Obtenido de: http://www. gartner. com/newsroom/id/3165317*, 2015.

[34] R. C. Lunardi, R. A. Michelin, C. V. Neu, and A. F. Zorzo, "Distributed access control on iot ledger-based architecture," in *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2018, pp. 1–7.

[35] M. Suárez-Albela, P. Fraga-Lamas, and T. Fernández-Caramés, "A practical evaluation on rsa and ecc-based cipher suites for iot high-security energy-efficient fog and mist computing devices," *Sensors*, vol. 18, no. 11, p. 3868, 2018.

[36] K. Rahim, H. Tahir, and N. Ikram, "Sensor based puf iot authentication model for a smart home with private blockchain," in *2018 International Conference on Applied and Engineering Mathematics (ICAEM)*. IEEE, 2018, pp. 102–108.

[37] U. Javaid, M. N. Aman, and B. Sikdar, "Blockpro: Blockchain based data provenance and integrity for secure iot environments," in *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems*. ACM, 2018, pp. 13–18.

[38] M. N. Islam, V. C. Patii, and S. Kundu, "On ic traceability via blockchain," in *VLSI Design, Automation and Test (VLSI-DAT), 2018 International Symposium on*. IEEE, 2018, pp. 1–4.

[39] J. Schlund, L. Ammon, and R. German, "Ethome: Open-source blockchain based energy community controller," 06 2018, pp. 319–323.

[40] T. Fernndez-Carams and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32 979–33 001, 05 2018.

[41] S. Morishima and H. Matsutani, "Acceleration of anomaly detection in blockchain using in-gpu cache."

[42] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[43] C. Mora, R. L. Rollins, K. Taladay, M. B. Kantar, M. K. Chock, M. Shimada, and E. C. Franklin, "Bitcoin emissions alone could push global warming above 2 c," *Nature Climate Change*, vol. 8, no. 11, p. 931, 2018.

[44] J. Van Bulck, M. Minkin, O. Weisse, D. Genkin, B. Kasikci, F. Piessens, M. Silberstein, T. F. Wenisch, Y. Yarom, and R. Strackx, "Foreshadow: Extracting the keys to the intel {SGX} kingdom with transient out-of-order execution," in *27th {USENIX} Security Symposium ({USENIX} Security 18)*, 2018, pp. 991–1008.