

# Integrating Blockchain and Fog Computing Technologies for Efficient Privacy-preserving Systems

Summary of PhD Theses

Hamza Baniata  
Supervisor: Attila Kertesz, PhD

Doctoral School of Computer Science  
Department of Software Engineering  
Faculty of Science and Informatics  
University of Szeged



Szeged  
2022



# Introduction

Blockchain (BC) technology is a distributed ledger technology in the form of a distributed transactional database, secured by cryptography, and governed by a consensus mechanism [11]. BC participants do not fully trust each other, yet they agree on the ledger's content by running the consensus algorithm [12]. BC technology was initially proposed for decentralized cryptocurrency applications and has practically proven high robustness compared to classical centralized systems. For several foundational advantages of utilizing BCs, different versions, uses, paradigms, and platforms were proposed, aiming to extend the deployment of BC beyond cash and payment purposes.

Fog Computing (FC), on the other hand, is a geographically distributed computing architecture, in which various heterogeneous devices at the edge of network are ubiquitously connected to collaboratively provide elastic computation, communication and storage services [13]. FC provides enhanced services closer to end-users in terms of time, energy, and network load.

The integration of FC with BC had been discussed by many researchers. The first integration proposal was only published in 2016 and, since then, the exploitation interest increased exponentially. On one hand, more efficient services, in terms of latency and privacy, can be provided by FC over clouds, mostly required by Internet of Things (IoT) systems. On the other hand, the BC technology can be deployed for reliable, TTP-free, and secure Transactions (TXs) ledger in such distributed environments, providing higher scalability and security potentials. However, several challenges are inherited from both technologies into their integrated solutions:

- **Challenge 1:** I have not found any reliable FC-BC simulation tools that can directly address FC-BC integration.
- **Challenge 2:** As FC provides enhanced QoS, BC tends to secure these services with methods that lower the QoS measurements.
- **Challenge 3:** BC solutions generally consume more power compared to centralized ones.
- **Challenge 4:** Privacy awareness of BC and FC technologies is a major challenge for both of these technologies. Thus, integrated FC-BC solutions must provably maintain or enhance different types of user privacy.
- **Challenge 5:** the consistency of distributed ledgers is the main challenge that BCs attempt to solve, while the distributed infrastructure of the fog subjectively implies that such solutions are needed. Other complex trade-offs are considered major factors, contributing to successful integration of FC and BC, resulting in secure, privacy-preserving, efficient and, most importantly, trusted solutions.

## Summary of Theses Results

I have attempted to address all of the aforementioned challenges, and optimize different integration models of FC and BC. First, I performed a detailed and extended literature review of related simulation tools and integration approaches [J1, J2, C1]. Accordingly,

I developed FoBSim [J2][C2]; a novel FC-BC simulation tool that allows for reliable and realistic integration simulation. FoBSim facilitates the simulation of different consensus algorithms (PoW, PoA and PoS) and different applications (e.g. cryptocurrency, smart contracts, etc.). It also allows to deploy the BC at different layers of an FC-enabled cloud system, with the advantage of easy parameterization of simulation scenarios (**Challenge 1**). Using this tool, I experimentally proved how integrating FC and BC meets my expected enhancement in terms of latency and cost (**Challenges 2 & 3**). Additionally, I analyzed different factors affecting distributed ledger consistency and trust in [C3], which motivated the development of novel methods for quantifying the consistency and reliability of BCs. Using these methods, I could introduce a decision-making model resulting in better integration potential of FC and BC technologies (**Challenges 2, 3 & 5**).

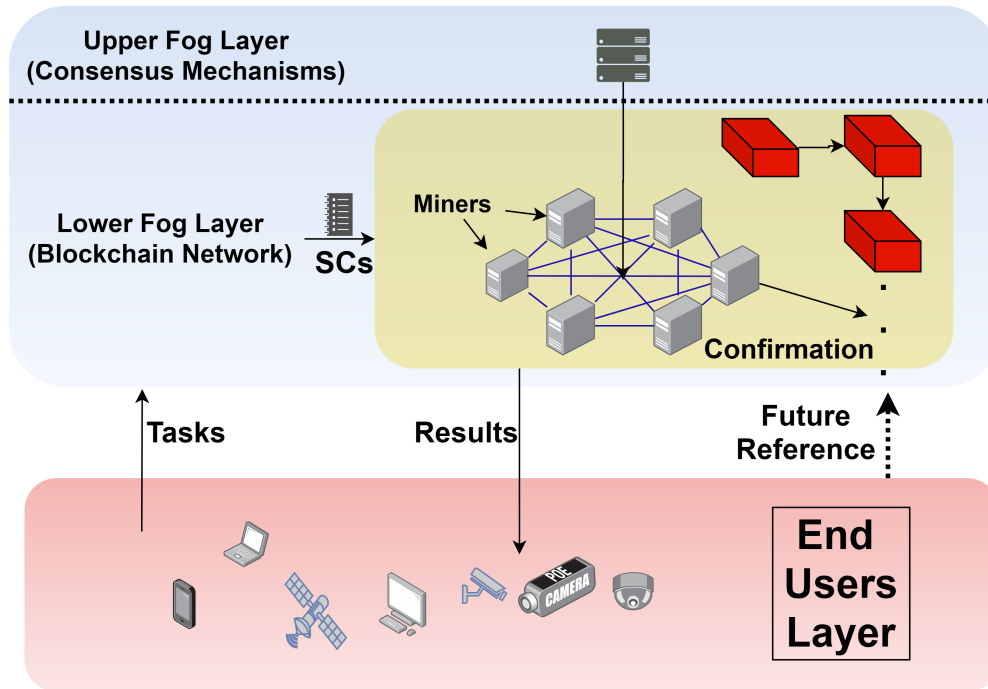
Based on the state-of-the-art, and following my experiments and their evaluation results, I designed two novel protocols aiming to enhance FC-BC integrated applications. The DONS protocol [J3] allows for dynamic and optimized neighbour selection in BC networks, which provably enhanced block finality and provided optimum message fidelity (**Challenges 2 & 3**). The AnoLE protocol [J3] allows for privacy-preserving leader election in public permissionless BCs (**Challenges 4 & 5**). I have also designed two privacy-preserving solutions where BC is exploited to enhance FC efficiency in terms of latency, namely PF-BTS [J4], and where FC is exploited to enhance BC efficiency in terms of block validation time and energy consumption, namely PF-BVM [C4] (**Challenges 2, 3, 4 & 5**). Finally, in order to exploit the advantages of integrated FC-BC solutions, I designed and developed PriFoB [J5]; a novel Blockchain-based Fog-enhanced global accreditation and credential verification system. Comparing PriFoB to widely adopted BC platforms and solutions, such as Ethereum, Hyperledger Fabric, Indy and Besu, PriFoB outperformed all of these in terms of latency and throughput. Meanwhile, PriFoB showed high levels of security and privacy, along with guaranteed compliance with the GDPR (**Challenge 5**). Following the results I obtained throughout my research, I discussed future works, regarding the utilization of FC-BC integrated systems, for trusted and robust smart system applications [C5] (**Challenge 5**).

**Thesis 1: I performed a comprehensive literature review related to integrated Fog Computing and Blockchain solutions, tools and applications. I designed a novel and extensible simulation tool called FoBSim that can comprehensively and realistically mimic such integrated systems. I experimentally validated and evaluated the simulation environment with different use cases and simulation parameters.**

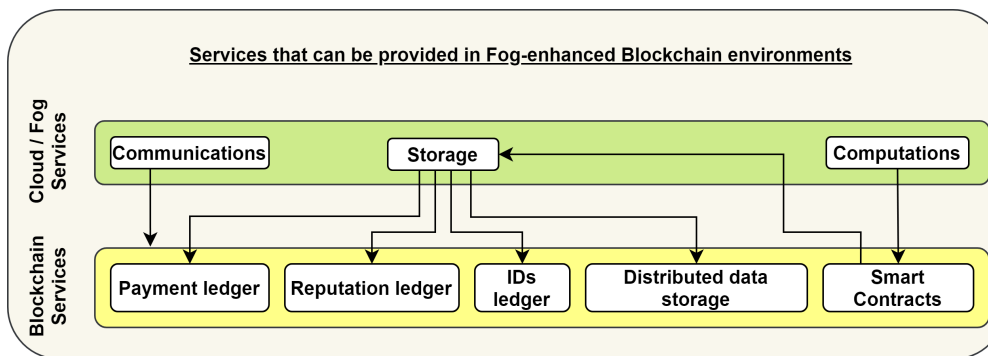
Privacy issues in Cloud Computing are one of the major concerns for many individuals and companies around the world, and still represent challenges for research and industry. The latest advances in Mobile Cloud Computing gave way to fog-enabled systems that

represent the future of current cloud systems. Accordingly, the Fog concept had been introduced in 2013 to enhance the IoT-Cloud operations in terms of latency and reliability. Blockchain (BC), on the other hand, as the base technology behind crypto-currencies, is implemented in wide range of different applications. The security and reliability, along with the distributed trust management mechanisms deployed within BC, excited the research community to integrate it with FC, in a step towards reaching a distributed and trusted, Data, Payment, Reputation, and Identity management systems.

After reviewing many projects, approaches, and solutions, I found that BC and FC technologies integration could be beneficial. Examples of organizations contributing to the R&D of these two technologies, and their integration, include Linux, IBM, Google, Microsoft, and others.



**Figure 1:** A sample integration architecture that can be simulated using the FoBSim tool, where BC is deployed in the Fog layer.



**Figure 2:** Service models provided by cloud/fog systems, and their relevant service models provided by BC systems.

In my first thesis, I analyzed and categorized surveys and solutions, published in the period 2013–2019, addressing privacy issues of the mentioned complex systems. I also discussed solutions concerning integrated FC-BC solutions, published in the period 2016–2020, with a detailed literature review and classification. I discussed and categorized the related papers according to the year of publication, domain, used algorithms, BC roles, and the placement of the BC in the FC architecture. Accordingly, detailed observations, analysis, and open challenges for the BC-FC integration were presented.

To validate an integrated Fog-Blockchain protocol or method implementation, before the deployment phase, a suitable and accurate simulation environment is needed. Such validation should save a great deal of costs and efforts on researchers and companies adopting this integration. Searching state-of-the-art simulation environments, I found that they facilitate Fog simulation, or BC simulation, but not both. To address this, I introduced a novel Fog-Blockchain simulator, namely FoBSim, with the main goal to ease the experimentation and validation of integrated Fog-Blockchain mechanisms and protocols. According to well-defined workflow of BC-FC simulation, I implemented different consensus algorithms, including PoW, PoS, and PoA. Additionally, I designed different deployment options of the BC in the FC architecture, and different functionalities of the BC in the simulation.

The current version of FoBSim allows the deployment of the BC either in the fog layer or the end-user layer. Figure 1 presents a sample integration architecture that can be simulated using FoBSim, where BC is deployed in the fog layer. In such scenario, nodes in the fog layer wear two functional hats: fog nodes representing the extension of the cloud closer to end-users, and mining nodes that perform and provide Blockchain tasks and services. Figure 2 presents how the services, classically provided by a cloud/fog system, can be interpreted into the form of services that can be provided by a BC system. We can notice in the figure that Smart Contracts can be considered relevant to cloud computational services, while different types of data saved on BC can be considered a relevant option to the centralized storage model provided by a cloud system. Accordingly, technical details and algorithms on possible simulation and integration scenarios in FoBSim were provided. I validated FoBSim by describing the technologies used within, and highlighting the novelty of the tool compared to state-of-the-art solutions. I also discussed the event validity in tool, and provided a clear walk-through validation.

**Thesis 2: I formalized and quantified the concepts of Blockchain network consistency and reliability. I developed two novel protocols (DONS and AnoLE) for the neighbor selection problem, targeting optimal block finality and privacy-preserving data propagation in public and permissionless Blockchains. I experimentally proved that Blockchain and Fog Computing integration is advantageous.**

A major component of a BC-based system is the Distributed Ledger (DL), whose consistency is a problem that describes the unreliability of DLs in dense and highly dynamic networks [14]. This problem concerns maintaining exact copies of the DL, as the appearance of different DL versions is trivially expected in realized scenarios. The absolute maximum number of different DL versions can be calculated according to Equation 1, where  $\beta$  is the number of different confirmed blocks and  $P(\beta)$  is the set consisting of all possible DL version out of  $\beta$ . However, the maximum number of different DL versions  $\xi$  within a network of distributed system with finite size  $M$ , can be determined referring to Relation 2. Reasons for such issue include both, the transmission delay between network entities and the continuous and concurrent alteration of DL data. Furthermore, the concept of Finality is usually related to the DL consistency, which is the state of the BC, under which transactions cannot be canceled, reversed or changed by any member of this network under any circumstances [15]. Trust in a BC system is majorly affected by the reliability the system provides [16].

$$|P(\beta)| = \sum_{k=0}^{\beta} \frac{\beta!}{(\beta - k)!} \quad (1)$$

$$\xi = \min\{M, |P(\beta)|\} \quad (2)$$

In my second thesis, I addressed the aforementioned issues by introducing formula 3 to quantify the DL inconsistency  $Y$ , for a given BC-based solution scenario, where  $\delta$  is the experimentally observed number of DL versions. I designed several scenarios to obtain  $\delta$  values, and to test the effect of oscillating the BC parameterization factors on  $\delta$ , and  $Y$  in general. Part of the results are provided in Table 1. The methods I used and proposed suggested that  $Y$  is theoretically and experimentally proportional to  $\delta$  and inversely proportional to  $\xi$ . Consequently, I could approach the optimization of BCs in terms of DL consistency by observing and reporting Relations 4 and 5. In these relations,  $\eta$  is  $1/N$  if  $N/M \leq 1\%$  and is  $N$  otherwise,  $N$  is the average number of neighbors per miner,  $\tau$  is the average transmission delay between neighbors,  $\Omega$  is the consensus puzzle difficulty, and  $\lambda$  is  $M$  if  $M \leq |P(\beta)|$ , and is  $1/|P(\beta)|$  otherwise.

$$Y = \delta/\xi \quad (3)$$

$$\delta \propto \frac{M \times \eta \times \tau \times \beta}{\Omega} \quad (4)$$

$$Y \propto \frac{\lambda \times \eta \times \tau \times \beta}{\Omega} \quad (5)$$

**Table 1:** Number of chain versions at the end of each simulation run, the average number of chain versions for each scenario, and the observed effect of oscillating the corresponding factor on the average number of chain versions

| Scenario          | Param.          | run-1 | run-2 | run-3 | run-4 | run-5 | Average $\delta$ | Effect |
|-------------------|-----------------|-------|-------|-------|-------|-------|------------------|--------|
| <b>Scenario-1</b> | $M = 100$       | 1     | 1     | 1     | 1     | 3     | <b>1.4</b>       |        |
|                   | $M = 500$       | 5     | 1     | 4     | 2     | 2     | <b>2.8</b>       | ↑      |
|                   | $M = 1000$      | 37    | 11    | 4     | 2     | 9     | <b>12.6</b>      | ↑      |
|                   | $M = 1500$      | 26    | 57    | 54    | 28    | 24    | <b>37.8</b>      | ↑      |
| <b>Scenario-2</b> | $N = 2$         | 91    | 105   | 78    | 69    | 91    | <b>86.8</b>      |        |
|                   | $N = 3$         | 87    | 66    | 42    | 65    | 79    | <b>67.8</b>      | ↓      |
|                   | $N = 5$         | 45    | 50    | 53    | 65    | 64    | <b>55.4</b>      | ↓      |
|                   | $N = 8$         | 117   | 73    | 71    | 45    | 71    | <b>75.4</b>      | ↑      |
|                   | $N = 15$        | 417   | 418   | 409   | 374   | 413   | <b>406.2</b>     | ↑      |
| <b>Scenario-3</b> | $\Omega = 5$    | 138   | 125   | 142   | 134   | 144   | <b>136.6</b>     |        |
|                   | $\Omega = 10$   | 143   | 123   | 128   | 126   | 142   | <b>132.4</b>     | ↓      |
|                   | $\Omega = 15$   | 129   | 135   | 125   | 140   | 136   | <b>133</b>       | ↑      |
|                   | $\Omega = 20$   | 22    | 14    | 20    | 9     | 31    | <b>19.2</b>      | ↓      |
|                   | $\Omega = 25$   | 1     | 1     | 1     | 8     | 1     | <b>2.4</b>       | ↓      |
| <b>Scenario-4</b> | $\beta=2$       | 3     | 3     | 3     | 3     | 3     | <b>3</b>         |        |
|                   | $\beta=3$       | 4     | 3     | 4     | 4     | 3     | <b>3.6</b>       | ↑      |
|                   | $\beta=5$       | 66    | 72    | 42    | 52    | 89    | <b>64.2</b>      | ↑      |
|                   | $\beta=8$       | 38    | 51    | 39    | 62    | 58    | <b>49.6</b>      | ↓      |
|                   | $\beta=12$      | 393   | 376   | 389   | 405   | 379   | <b>388.4</b>     | ↑      |
|                   | $\beta=18$      | 459   | 461   | 469   | 466   | 460   | <b>463</b>       | ↑      |
| <b>Scenario-5</b> | $\tau = 0$ ms.  | 2     | 5     | 2     | 1     | 17    | <b>5.4</b>       |        |
|                   | $\tau = 5$ ms.  | 26    | 47    | 7     | 24    | 6     | <b>22</b>        | ↑      |
|                   | $\tau = 10$ ms. | 21    | 46    | 2     | 6     | 40    | <b>23</b>        | ↑      |
|                   | $\tau = 15$ ms. | 31    | 72    | 37    | 11    | 103   | <b>50.8</b>      | ↑      |

Additionally, I introduced an unreliability presentation model,  $R$ , of a given BC-solution.  $R$  shall directly affect the trust factor of the solution. Equation 6 describes a simple approach to calculate  $R$ , where  $t$  is the TX/B rate, and  $T$  is the average number of TXs per predefined time (e.g. a day). As  $Y$  provides the absolute observable fork probability,  $R$  indicates the relative fork probability of a specific, newly submitted block. The higher  $Y$ , the higher  $R$  and, thus, the lower the trust in the BC system. In simple comprehension,  $1/R$  is the expected number of system operational days until a new fork appears.

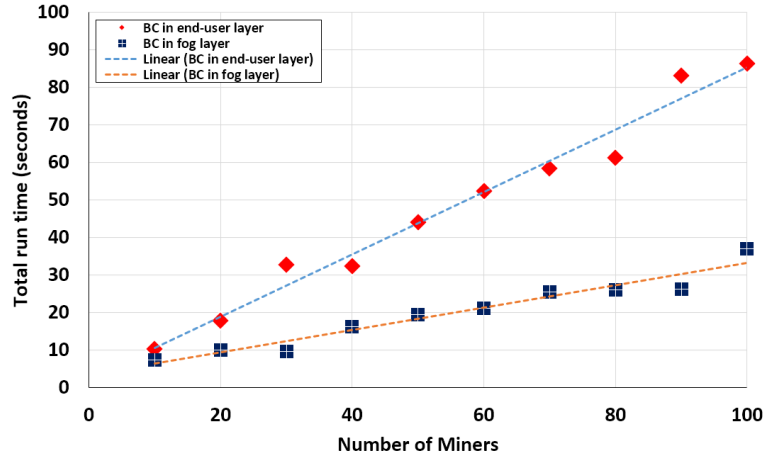
$$R = \frac{t \times (Y/2)}{T} \quad (6)$$

I built on these concepts and proposed a decision-making model mainly concerned with the deployment security. Formalized in Equation 7, where  $\Psi$  is an always positive value,  $f$

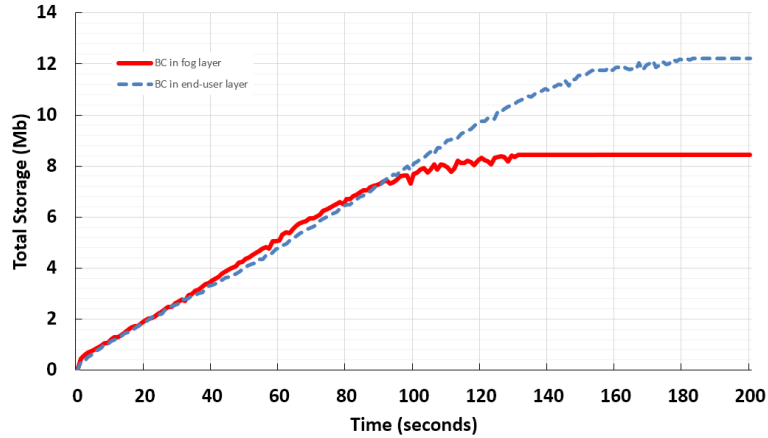


is fog layer and  $e$  is end-user layer. If the value of  $\Psi$  is less than 1, then the BC is better be deployed in  $f$ , because such deployment guarantees higher DL consistency. Otherwise, the BC is better be deployed in  $e$ . I used FoBSim to simulate case studies and analyze the obtained results, where deploying the BC network in the fog layer showed enhanced QoS in terms of total run time and total storage cost. Figures 3 and 4 present some of the results discussed in this thesis.

$$\Psi = \frac{Y_f}{Y_e} \quad (7)$$

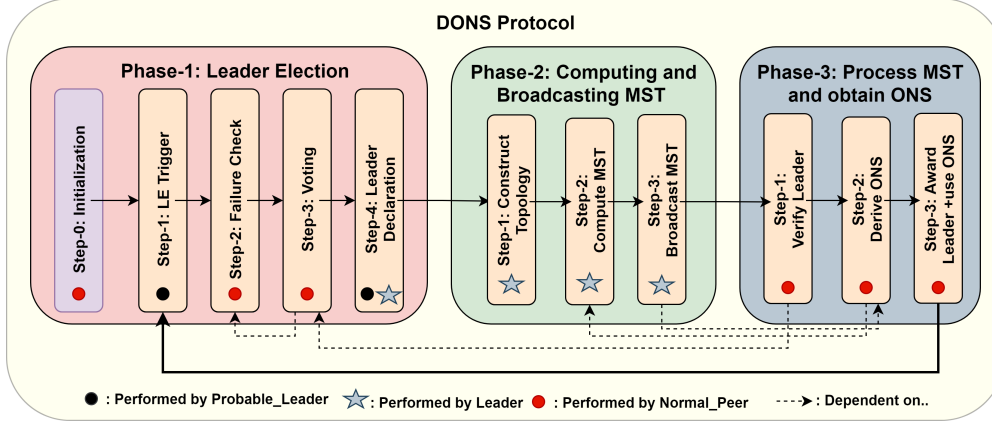


**Figure 3:** Total run time of simulation scenarios run with BC in end-user layer vs. BC in Fog layer



**Figure 4:** Total storage cost of simulation scenarios run with BC in end-user layer vs. BC in Fog layer

Depending on the results I obtained thus far, I designed a Dynamic and Optimized Neighbor Selection (DONS) protocol. That is, I have proven that different system criteria impose different readings of the DL, e.g. the fluctuating transmission delay between nodes and the continuous alteration of data. Furthermore, I have proven that more neighbors per miner and higher delivery time rates between neighbors, both lead to lower levels of DL



**Figure 5:** Phases and steps of the DONS protocol. Each step is performed by one (or more) system entity(s). A step may depend on the result of a preceding step of the current round, or on the result of a subsequent step of the previous round

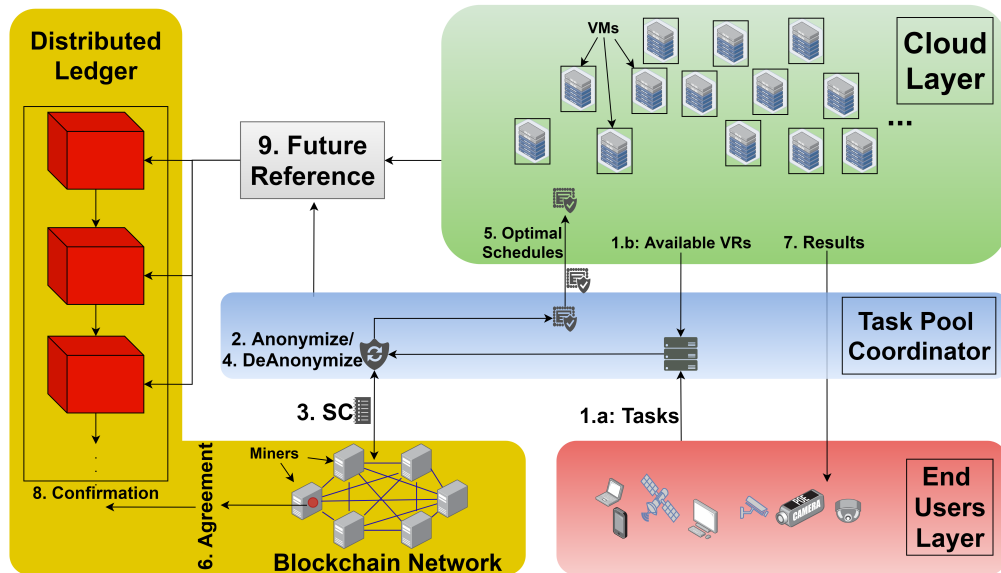
**Table 2:** Performance of the DONS protocol against RTT-NS and RNS protocols, on two random network models with different sizes

| Model | Net Size | peer per node | Finality time ( $\mu$ s) |        |        | Fidelity (msg.) |        |       |
|-------|----------|---------------|--------------------------|--------|--------|-----------------|--------|-------|
|       |          |               | DONS                     | RTT-NS | RNS    | DONS            | RTT-NS | RNS   |
| BA    | 50       | 5             | 204                      | 2,343  | 8,463  | 50              | 74     | 253   |
|       | 100      | 5             | 367                      | 5,139  | 24,667 | 100             | 142    | 751   |
|       | 150      | 7             | 310                      | 5,008  | 40,870 | 150             | 182    | 1,514 |
|       | 200      | 10            | 176                      | 6,927  | 61,429 | 200             | 251    | 2,241 |
| ER    | 50       | 0.1           | 629                      | 4,176  | 14,510 | 50              | 79     | 371   |
|       | 100      | 0.1           | 450                      | 3,558  | 14,533 | 100             | 123    | 496   |
|       | 150      | 0.1           | 257                      | 5,795  | 26,932 | 150             | 199    | 851   |
|       | 200      | 0.1           | 260                      | 4,363  | 45,656 | 200             | 236    | 1,676 |

consistency. These results served as a motivation to the proposal of DONS. This protocol shall require minimal number of neighbors per miner, directing the miners to communicate with globally-optimized selection of neighbors. I discussed how DONS decreases the number of cycles within a path, that shared data walks, from any peer to any other peer (i.e. no cycles, hence a Spanning Tree is an optimal solution [17]). I also showed how DONS decreases the maximum time spent from generating data, by any peer, till it reaches all the peers of the network. Additionally, I discussed how DONS addresses the scalability issues of the network, leading to adaptive optimization of NS in spite of continuous change in network topology. The main steps, phases and dependencies of the DONS protocol are presented in Figure 5. Partial performance results of DONS, against currently used RNS and RTT-NS methods, are presented in Table 2. The main challenge in deploying DONS in permissionless BCs was missing an agreed-on entity that performs MST computations for the network. To solve this, I further proposed an Anonymized Leader Election (AnoLE) protocol represented by Phase-1 in Figure 5.

**Thesis 3: I designed and developed two privacy-aware protocols for FC latency enhancement using BC, namely PF-BTS, and for BC energy efficiency using FC, namely PF-BVM. PF-BTS allows the fog layer to exploit BC in a privacy-aware manner to provide optimal task schedules for cloud infrastructures. PF-BVM allows BC networks to exploit fog nodes for faster privacy-aware block validation.**

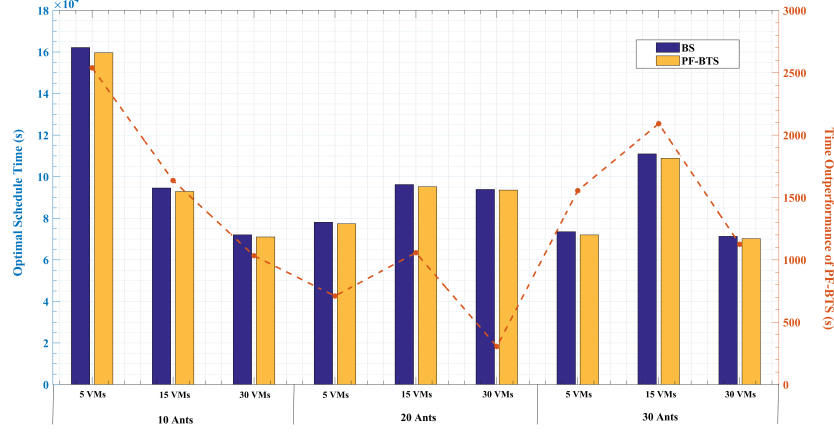
In my third thesis, I designed and implemented two integrated solutions, one shows how Blockchain technology can enhance the efficiency of the fog layer, and the other shows how enabling the fog into BC-based systems shall enhance Blockchain efficiency.



**Figure 6:** The Fog-Cloud architecture in which the fog and BC are deployed to perform the PF-BTS protocol.

First, I deployed an Ant Colony Optimization (ACO) algorithm in a fog-enabled Blockchain-assisted scheduling model, namely PF-BTS. The general Fog-Cloud architecture in which PF-BTS was deployed is depicted in Figure 6. The protocol and algorithms of PF-BTS exploit BC miners for generating efficient assignment of tasks to be executed in virtual resources of a cloud infrastructure using ACO, and award miner nodes for their contribution in generating the best schedule. PF-BTS further allows the fog to process, manage, and perform the tasks to enhance latency measurements. While this processing and managing is taking place, the fog is enforced to respect the privacy of system components, and assure that data, location, identity, and usage information are not exposed. I evaluated and compared PF-BTS performance, with current Blockchain-based task scheduling protocols, in a simulated environment. Sample performance comparison of PF-BTS against other similar approach is presented in Figure 7. My evaluation and experiments showed

high privacy awareness of PF-BTS, along with noticeable enhancement in execution time and network load. Generally, this application shows how a fog-enabled system can benefit from BC technology.



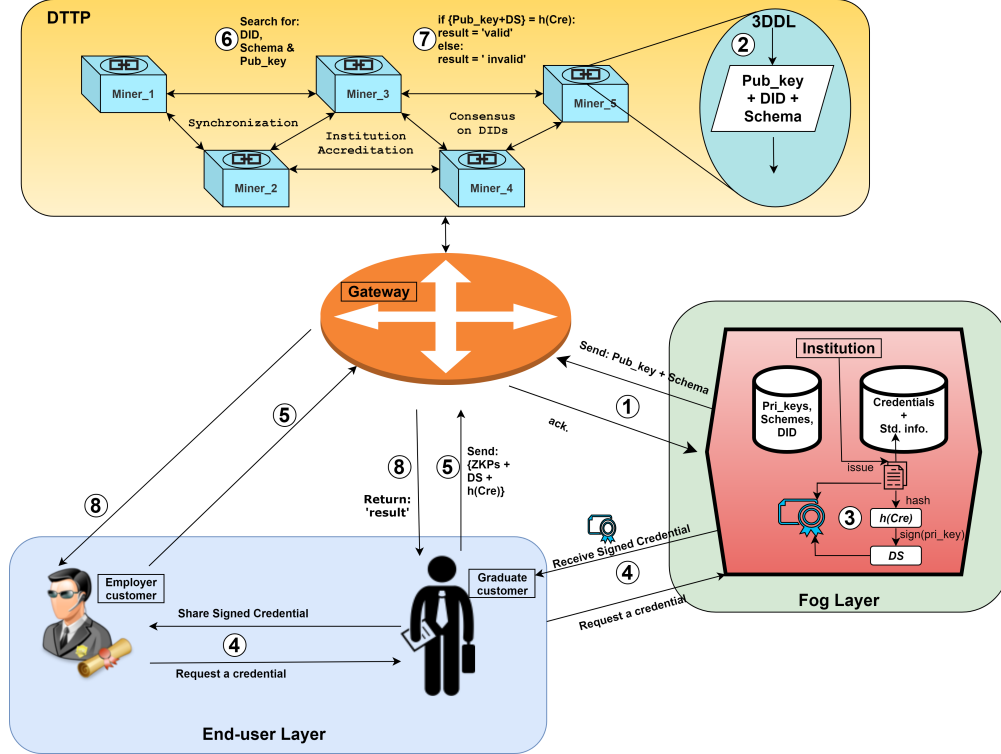
**Figure 7:** Optimal schedule generation time using different configurations of PF-BTS, against a recently proposed BC-based scheduler. Bars are correlated with the main Y access on the left and dashed curve is correlated with the secondary Y access on the right

Second, I proposed a novel BC validation mechanism (PF-BVM) that maintains an equivalent consensus feature, where trusted fog nodes are able to validate transactions on behalf of blockchain nodes authenticated with them. Meanwhile, all nodes are deployed for the block confirmation and mining. The proposed mechanism is an approach for reducing the heavy load on the BC network, represented by extended validation time, and high energy consumption. On the other hand, the privacy-awareness property is preserved in PF-BVM by limiting the number of network nodes verifying a transaction generator. According to the experiments conducted for evaluating PF-BVM, I found that, in relation to total number of validator nodes, it could linearly reduce the energy and validation time consumption. Generally, this application shows how BC-based systems can benefit from the Fog Computing technology.

**Thesis 4:** I developed a Fog-enhanced Blockchain-based solution (called PriFoB) to realize privacy-aware institution accreditation and credential validation. I designed a novel hybrid Proof-of-Authority and Signatures-of-Work consensus algorithm to enhance security and efficiency. I proposed a partially immutable, three dimensional, DAG-based Distributed Ledger to support revoking on-chain data.

In my fourth thesis, I provided real-world applications for FC-BC integration. The results and discussion presented in this thesis highlight the benefits of FC-BC integration, and

furnish a wide collection for future work directions. The presented, detailed simulation and emulation results proved that FC and BC integrated solutions not only outperform centralized alternatives, but also BC alternatives that do not utilize FC.



**Figure 8:** The general architecture and framework of entities in a PriFoB system. The circled numbers indicate the order of steps to remotely accredit an issuer, publish new schemes, issue a new VC by an accredited issuer and verify that VC

First, I utilized a public-permissioned Blockchain and a Fog layer to implement PriFoB; a GDPR-compliant and efficient system for global institution accreditation and credential verification. The BC in PriFoB acts as a Distributed Trusted Third Party (DTTP), in which miners are national accreditation bodies (e.g. national ministry of higher education, ministry of foreign affairs or ministry of health affairs, etc.). On the other hand, fog nodes are realized by credential issuer bodies (e.g. universities, hospitals, vaccination centers, etc.). I designed PriFoB to guarantee privacy and security of system entities, by deploying the robust Proof-of-Authority (PoA) [18] algorithm, a realized application of the secure Signatures-of-Work (SoW) [19] scheme, RSA, Digital Signatures (DS), and Zero Knowledge Proof (ZKP) mechanisms. The SoW deployment, specifically, is an additional and optional consensus sub-layer for practical realization of PriFoB as a secure global accreditation solution. I also deployed a novel, relaxed and efficient multi-dimensional BC model, where blocks are partially (instead of fully) immutable. Each dimension holds a different type of TXs, which enhances the overall efficiency of the validation process. Furthermore, I used an improved Directed Acyclic Graph (DAG) based block relations within each dimension, which outperforms the classical linear model in terms of total throughput and response latency [20]. In addition to those reasons, the proposed ledger model further supports safely revoking on-chain data, as the third dimension is dedicated for revocation blocks. The general architecture and framework of the PriFoB solution are presented in

Figure 8. Part of the performance results of PriFoB against several well-known BC platforms, are presented in Table 3.

**Table 3:** *PriFoB comparison with previous related works, in terms of utilized Blockchain platform, granting institution accreditation services (A), number of Miners (M), assessed request type (T), lower and upper bounds of request per second rates (req/s) and the lower and upper bounds of response Latency measured as second per request (s/req)*

| Solution | CA        | A   | M        | T              | req/s  | Latency (s/req) |
|----------|-----------|-----|----------|----------------|--------|-----------------|
| Indy     | PBFT      | NO  | 4        | DID (write)    | 1–250  | 2–6             |
|          |           |     |          | Any (read)     |        | 0.08–1.6        |
|          |           |     | 8        | DID (write)    |        | 2–10            |
|          |           |     |          | Any (read)     |        | 0.1–2.5         |
| Besu     | PoA       | NO  | 4        | Any (write)    | 10–100 | 3.34–4.60       |
|          |           |     |          | Any (read)     |        | 0.04–0.56       |
| Fabric   | RAFT      | NO  | 2        | Any (wirte)    | 50–250 | 0.6–0.8         |
| Fabric   |           |     | 4        | Any (write)    |        | 0.7–0.95        |
|          |           | NO  | 2        | Any (read)     | 10–100 | 0.6–0.8         |
| Ethereum | PoW       | NO  | 2        | Any (write)    | 10–100 | 5.03–5.58       |
| Ethereum | PoA       | NO  | 2        | Any (read)     | 25–100 | 0.02–0.06       |
|          |           |     | N/A      | Any (write)    |        | 5–34            |
| Ethereum | PoW       | YES | Main Net | Any (read)     |        | 0.2–0.4         |
| Ethereum | PoW       | YES | Main Net | DID (write)    | 1–100  | 47–114          |
| Ethereum | PoW       | YES | Main Net | DID (write)    | N/A    | 5–40            |
| PriFoB   | SoW + PoA | YES | 2–6      | DID (write)    | 1–250  | 0.013–1.09      |
|          |           |     |          | Schema (write) |        | 0.006–0.6       |
|          |           |     |          | Revoke (write) |        | 0.005–0.09      |
|          |           |     |          | Any (read)     |        | 0.003–0.14      |

I also discussed in this thesis my future plans for extending FoBSim to support complex models for simulating the scheduling and provisioning process of the entire application. The simulation models shall adaptively respond to significant changes in the pool of available simulated smart devices (Cloud or Fog instances) during application execution. Additionally, they shall identify provisioned devices that do not provide good performance for a given smart application component. Extensions will further enable the the simulation and replacement of low-performing infrastructure, e.g., provisioned as VMs or containers that no longer meet the application requirements, or reconfigure existing ones (increase number of CPUs to a VM running).

I also focused my future plans on smart applications related to the prevention of virus spreading or to the management of societal problems, such as travel restrictions caused by the pandemic. The vast majority of such applications are mainly centralized and non-smart, which makes them carry single-point-of-failure, privacy, high latency, and legal issues, along with the lack of efficient handling of mobile smart devices. The adoption and mass acceptance of such applications, e.g. COVID-19-related applications, are greatly hindered by the general lack of trust associated with the nature of tracing apps, and the reluctance of people to share their personal data. To overcome these issues, I discuss my

plans to revisit current solutions, and design methods addressing their privacy-preserving, privacy-awareness, explainability and interoperability requirements.

## Publications, Theses and Citations

Table 4 summarizes the relation between the theses and the corresponding publications.

**Table 4:** *Relation between the theses and publications.*

| no. | Publication      | Year | Thesis |   |   |   | Citations |
|-----|------------------|------|--------|---|---|---|-----------|
|     |                  |      | 1      | 2 | 3 | 4 |           |
| 1.  | [J1] IEEE-Access | 2020 | •      |   |   |   | 35        |
| 2.  | [C1] FMEC        | 2020 | •      |   |   |   | 5         |
| 3.  | [C2] CSCS        | 2020 | •      | • |   |   | 1         |
| 4.  | [J2] PeerJ-CS    | 2021 | •      | • |   |   | 5         |
| 5.  | [C3] Euro-Par    | 2021 |        | • |   |   | 5         |
| 6.  | [J3] FGCS        | 2022 |        | • |   |   | 5         |
| 7.  | [C4] CLOSER      | 2020 |        | • | • |   | 6         |
| 8.  | [J4] IPM         | 2021 |        |   | • |   | 58        |
| 9.  | [C5] CERCIRAS    | 2021 |        |   |   | • | –         |
| 10. | [J5] JNCA        | 2022 |        |   |   | • | –         |

## Journal publications

- [J1] Hamza Baniata and Attila Kertesz. A survey on blockchain-fog integration approaches. *IEEE Access*, VOL(8), 102657-102668, 2020.
- [J2] Hamza Baniata and Attila Kertesz. FoBSim: an extensible open-source simulation tool for integrated fog-blockchain systems. *PeerJ Computer Science*, VOL(7), e431, 2021.
- [J3] Hamza Baniata, Ahmad Anaqreh, and Attila Kertesz. Dons: Dynamic optimized neighbor selection for smart blockchain networks. *Future Generation Computer Systems*, VOL(130), 75–90, 2022.
- [J4] Hamza Baniata, Ahmad Anaqreh, and Attila Kertesz. PF-BTS: A Privacy-Aware Fog-enhanced Blockchain-assisted task scheduling. *Information Processing & Management*, VOL(58.1), 102393, 2021.
- [J5] Hamza Baniata and Attila Kertesz. PriFoB: A Privacy-aware Fog-enhanced Blockchain-based system for Global Accreditation and Credential Verification *Journal of Network and Computer Applications*, VOL(205), 103440, 2022.

## Conference proceedings

- [C1] Hamza Baniata, Wesam Almobaideen, and Attila Kertesz. A privacy preserving model for fog-enabled mcc systems using 5g connection. In *Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*. IEEE, 223-230, 2020.
- [C2] Hamza Baniata. Fog-enhanced blockchain simulation. In *The 12th Conference of PhD Students in Computer Science (CS2)*, University of Szeged. 2020.
- [C3] Attila Kertesz and Hamza Baniata. Consistency Analysis of Distributed Ledgers in Fog-enhanced Blockchains.. In *27th International European Conference on Parallel and Distributed Computing (Euro-Par)*, 2021.
- [C4] Hamza Baniata and Attila Kertesz. PF-BVM: A Privacy-aware Fog-enhanced Blockchain Validation Mechanism.. In *The 11th International Conference on Cloud Computing and Services Science (CLOSER)* SCITEPRESS, 430-439, 2020.
- [C5] Hamza Baniata, Dragi Kimovski, Radu Prodan, and Attila Kertesz. Towards Blockchain-based Smart Systems. In *1st Workshop on Connecting Education and Research Communities for an Innovative Resource Aware Society*, CERCIRAS Cost Action CA19135. 2021.

## Further related publications

- [J6] Hamza Baniata, Sami Mahmood, and Attila Kertesz. Assessing anthropogenic heat flux of public cloud data centers: current and future trends. *PeerJ Computer Science*, VOL(7), e478, 2021.
- [J7] Hamza Baniata, Ahmad Sharieh, Sami Mahmood, and Attila Kertesz. GRAFT: A Model for Evaluating Actuator Systems in terms of Force Production. *Sensors*, VOL(20(7)), 1894, 2020.
- [C6] Hamza Baniata, Pflanzner, T., Feher, Z., & Kertész, A. Latency Assessment of Blockchain-based SSI Applications Utilizing Hyperledger Indy In *CLOSER, 2022*, (pp. 264-271)
- [J8] Tamas Pflanzner, Hamza Baniata, and Attila Kertesz. Latency Analysis of Blockchain-Based SSI Applications. *Future Internet*, VOL(14(10)), 282, 2022.

## Other References

- [11] Roman Beck, Michel Avital, Matti Rossi, and Jason Bennett Thatcher. Blockchain technology in business and information systems research. *Business & information systems engineering*, 59(6):381–384, 2017.



- [12] Carlos Faria and Miguel Correia. Blocksims: blockchain simulator. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 439–446. IEEE, 2019.
- [13] Shanhe Yi, Zijiang Hao, Zhengrui Qin, and Qun Li. Fog computing: Platform and applications. In *2015 Third IEEE workshop on hot topics in web systems and technologies (HotWeb)*, pages 73–78. IEEE, 2015.
- [14] Gabriel R Carrara, Leonardo M Burle, Dianne SV Medeiros, Célio Vinicius N de Albuquerque, and Diogo MF Mattos. Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking. *Annals of Telecommunications*, 75(3):163–174, 2020.
- [15] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis. Consensus in the age of blockchains. *arXiv preprint arXiv:1711.03936*, 2017.
- [16] Victoria L Lemieux. Blockchain and distributed ledgers as trusted recordkeeping systems. In *Future technologies conference (FTC)*, volume 2017, 2017.
- [17] Petrică C Pop. The generalized minimum spanning tree problem: An overview of formulations, solution procedures and latest advances. *European Journal of Operational Research*, 283(1):1–15, 2020.
- [18] Pranav Kumar Singh, Roshan Singh, Sunit Kumar Nandi, and Sukumar Nandi. Managing smart home appliances with proof of authority and blockchain. In *International conference on innovations for community services*, pages 221–232. Springer, 2019.
- [19] Juan A Garay, Aggelos Kiayias, and Giorgos Panagiotakos. Consensus from signatures of work. In *Cryptographers’ Track at the RSA Conference*, pages 319–344. Springer, 2020.
- [20] Huma Pervez, Muhammad Muneeb, Muhammad Usama Irfan, and Irfan Ul Haq. A comparative analysis of dag-based blockchain architectures. In *2018 12th International conference on open source systems and technologies (ICOSST)*, pages 27–34. IEEE, 2018.

## Summary in Hungarian

A blokklánc (BL) technológia egy elosztott főkönyvi technológia, mely egy elosztott tranzakciós adatbázist valósít meg, kriptográfia és konszenzusos mechanizmusok alkalmazásával, melyet eredetileg decentralizált kriptovaluta alkalmazásokhoz hoztak létre. A Kód Számítások olyan földrajzilag elosztott számítási architektúrát definiálnak, melyben a hálózat szélén található különféle eszközök összekapcsolásával rugalmas számítási szolgáltatásokat nyújtanak. A Kód ezáltal olyan szolgáltatásokat nyújt a végfelhasználókhoz közel, melyek csökkentik a végrehajtási időt, az energiát és a hálózati terhelést. A Kód és a BL integrációja hatékonyabb szolgáltatásokat eredményezhet a késleltetés és az adatvédelem tekintetében, melyet leginkább a Dolgok Internete alkalmazásai igényelnek.

Disszertációmban ezen rendszerek integrációs kihívásait vizsgáltam. Részletes szakirodalmi áttekintést végeztem a kapcsolódó szimulációs eszközökről és integrációs megközelítésekről. Kifejlesztettem egy új szimulációs eszközt a FoBSim-et, mely részletesen paraméterezhető Kód-BL integrációs szimulációkat tesz lehetővé. Megkönnyíti a különböző konszenzusos algoritmusok és alkalmazások vizsgálatát, és lehetővé teszi a BL telepítésének modellezését Kód- és Felhő-alapú rendszerek különböző rétegeiben. Segítségével igazoltam, hogy a Kód és a BL integráció miként javíthat a különféle alkalmazások végrehajtásán késleltetés és hatékonyság tekintetében. Elemeztem az elosztott főkönyvi konzisztenciát és a bizalmat befolyásoló különböző tényezőket, melyekhez új módszereket dolgoztam ki a BL-ok konzisztenciájának és megbízhatóságának számszerűsítésére. Így olyan döntéshozatali modellt tudtam kifejleszteni, mely a Kód és a BL technológiák hatékonyabb integrációját eredményezi.

Kidolgoztam két új vezérlési protokollt, melyek célja a Kód-alapú BL rendszerek hatékonyságának növelése optimalizált szomszéd választással. Kifejlesztettem két adatvédelmi módszert is, melyekkel a magánszféra biztonságának növelése mellett a késleltetés is csökkenthető Kód-BL alkalmazások számára. Végezetül megterveztem és kifejlesztettem egy új, Kód- és BL-alapú globális akkreditációs és hitelesítő rendszert a PriFoB-ot, mely biztonságos tanúsítványkezelést tesz lehetővé.

## Declaration

In the PhD dissertation of Hamza Baniata entitled "Integrating Blockchain and Fog Computing Technologies for Efficient Privacy-preserving Systems", Hamza Baniata and his Supervisor share the following joint and undividable contributions:

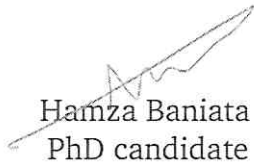
- design methods for modelling Fog Computing and Blockchain systems; design methods for Blockchain consistency analysis and network optimization; and the design of a methodology for privacy-aware Fog-enhanced and Blockchain-based application management [J1, J2, J3, J4, J5, C3, C5].

In the PhD dissertation of Hamza Baniata entitled "Integrating Blockchain and Fog Computing Technologies for Efficient Privacy-preserving Systems", Hamza Baniata's contribution was decisive in the following results:

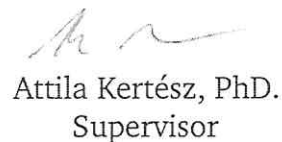
- In **Thesis I**: survey of integrated Fog Computing and Blockchain solutions, the development and implementation of the FoBSim simulation tool, and experiments and evaluation made with FoBSim with different use cases [J1, J2, C1, C2].
- In **Thesis II**: the formalization of Blockchain network consistency and reliability metrics, the development of DONS and AnoLE protocols, and their validation experiments [J2, J3, C3, C4].
- In **Thesis III**: the development and implementation of two privacy-aware protocols called PF-BTS and PF-BVM, and their validation [J4, C4].
- In **Thesis IV**: the development and implementation of a privacy-aware institution accreditation and credential validation called PriFoB, the development of the hybrid Proof-of-Authority and Signatures-of-Work consensus algorithm and the three dimensional, DAG-based Distributed Ledger [J5, C5].

These results cannot be used to obtain an academic research degree, other than the submitted PhD thesis of Hamza Baniata.

Szeged, 2022.11.16.



Hamza Baniata  
PhD candidate



Attila Kertész, PhD.  
Supervisor

The head of the Doctoral School of Computer Science declares that the declaration above was sent to all of the coauthors and none of them raised any objections against it.

Szeged, 2022.11.16.



Mark Jelasity, DSc.  
Head of the Doctoral School

- [J1] Hamza Baniata and Attila Kertesz. A survey on blockchain-fog integration approaches. *IEEE Access*, vol. 8, 102657-102668, 2020.
- [J2] Hamza Baniata and Attila Kertesz. FoBSim: an extensible open-source simulation tool for integrated fog-blockchain systems. *PeerJ Computer Science*, vol. 7, e431, 2021.
- [J3] Hamza Baniata, Ahmad Anaqreh, and Attila Kertesz. Dons: Dynamic optimized neighbor selection for smart blockchain networks. *Future Generation Computer Systems*, vol. 130, 75–90, 2022.
- [J4] Hamza Baniata, Ahmad Anaqreh, and Attila Kertesz. PF-BTS: A Privacy-Aware Fog-enhanced Blockchain-assisted task scheduling. *Information Processing & Management*, vol. 58, i. 1, 102393, 2021.
- [J5] Hamza Baniata and Attila Kertesz. PriFoB: a Privacy-aware Fog-enhanced Blockchain-based system for Global Accreditation and Credential Verification. *Journal of Network and Computer Applications*, vol. 205, 103440, 2022.
- [C1] Hamza Baniata, Wesam Almobaideen, and Attila Kertesz. A privacy preserving model for fog-enabled mcc systems using 5g connection. In *Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*. IEEE, 223-230, 2020.
- [C2] Hamza Baniata. Fog-enhanced blockchain simulation. In *The 12th Conference of PhD Students in Computer Science (CS2)*, University of Szeged. 2020.
- [C3] Attila Kertesz and Hamza Baniata. Consistency Analysis of Distributed Ledgers in Fog-enhanced Blockchains.. In *27th International European Conference on Parallel and Distributed Computing (Euro-Par)*, 2021.
- [C4] Hamza Baniata and Attila Kertesz. PF-BVM: A Privacy-aware Fog-enhanced Blockchain Validation Mechanism.. In *The 11th International Conference on Cloud Computing and Services Science (CLOSER)* SCITEPRESS, 430-439, 2020.
- [C5] Hamza Baniata, Dragi Kimovski, Radu Prodan, and Attila Kertesz. Towards Blockchain-based Smart Systems. In *1st Workshop on Connecting Education and Research Communities for an Innovative Resource Aware Society*, CERCIRAS Cost Action CA19135. 2021.