Multi-level consensus algorithm for appendable-block blockchains in IoT Environments*

Roben Castagna Lunardi[1,2], **Avelino Francisco Zorzo**[2]

[1]Pontifical Catholic University of Rio Grande do Sul (PUCRS)
Porto Alegre, RS – Brazil.

[2]Federal Institute of Rio Grande do Sul (IFRS)
Porto Alegre, RS – Brazil.

roben.lunardi@restinga.ifrs.edu.br, avelino.zorzo@pucrs.br

Abstract. *Currently, there are different devices collecting data and providing services through the Internet. Some of these devices collaborate to exchange information and use them to make smarter decisions in an environment called Internet of Things (IoT). Recently, blockchain technology emerged as a possible solution to overcome security issues in IoT. Despite that, traditional blockchains (such as Bitcoin or Ethereum) are not well suited to the resource-constrained nature of IoT devices. Moreover, current proposals lack a discussion about user behavior in different contexts and how it could be adapted for different consensus algorithms. To overcome these problems, we present in the thesis a set of steps to create a multi-level consensus mechanism for different contexts using a lightweight blockchain framework called appendable-block blockchain. This approach provides a solution that can use different configurations or consensus, according to the requirements of each IoT context. Finally, the thesis shows that a multi-level consensus can produce high throughput and low latency to insert new transactions in appendable-block blockchains.*

Resumo. *Atualmente, existem diversos dispositivos que coletam dados e prestam serviços na Internet. Alguns desses dispositivos colaboram para trocar informações e usá-las para tomar decisões mais inteligentes em um ambiente chamado Internet das Coisas (IoT). Recentemente, a tecnologia blockchain surgiu como uma possível solução para superar problemas de segurança em IoT. Apesar disso, blockchains tradicionais (como Bitcoin ou Ethereum) não são adequados para a natureza de capacidade/recursos limitados dos dispositivos IoT. Além disso, as propostas atuais carecem de uma discussão sobre o comportamento do usuário em diferentes contextos e como ele pode ser adaptado para diferentes algoritmos de consenso. Para superar esses problemas, apresentamos na tese um conjunto de etapas para criar um mecanismo de consenso multinível para diferentes contextos usando uma estrutura blockchain leve chamada appendable-block blockchain. Essa abordagem fornece uma solução que permite usar diferentes configurações ou consensos, de acordo com os requisitos de cada contexto no ambiente IoT. Por fim, a tese mostra que um consenso multinível pode produzir uma alta taxa de transferência e baixa latência para inserir novas transações em appendable-block blockchains.*

*Full thesis document is available at https://repositorio.pucrs.br/dspace/handle/10923/17355

1. Introduction

Currently, smart devices became part of many people's life. The environment composed of these kind of devices - capable of processing information and communicating with other devices in order to make decisions - is called the Internet of Things (IoT). However, these devices are vulnerable to different attacks, *e.g.*, getting access to health information from a personal smartband or using different smart devices to attack a web system. For example, the Mirai botnet [Jerkins 2017] was a famous attack that used IoT devices to attack a Dynamic Domain Name System provider. In that attack, millions of devices were exploited (specially using default user and password) to produce this Distributed Denial of Service (DDoS) attack against important service providers, *e.g.*, Netflix and Twitter.

In general, an IoT solution is composed of a myriad of devices, both in quantity and diversity. Therefore, there are several concerns about performance, safety, and security risks in these heterogeneous networks. Also, the fact that critical infrastructure, such as energy grids and even human lives in the context of healthcare, can rely upon IoT devices. Thereby, new challenges arise in this large, ever-increasing, and sensitive domain. Moreover, several research propose different ways to handle those challenges, such as: limitations to the hardware capacity, sensitivity of device information, or the use of devices in botnets [Conoscenti et al. 2016]. After the popularization of blockchain frameworks, researchers proposed the adoption of blockchain in order to solve some of the security issues in IoT. Some important benefits that a blockchain can provide to IoT networks include (although not limited to these): **Decentralized Architecture**; **Tamper Resistance**; **Transparency**; and **Smart Contracts execution**.

To tackle the security issues different proposals investigate the use of the blockchain technology [Boudguiga et al. 2017, Dorri et al. 2017, Novo 2018]. One of them, the appendable-block blockchain was proposed by the Reliability and Security Group (CONSEG) [Lunardi et al. 2018, Michelin et al. 2018, Lunardi et al. 2019a]. This blockchain was designed to present a blockchain solution to be used in IoT environments. In the thesis, we proposed to expand that blockchain with a new consensus model that adopts different consensus algorithms at different levels, allowing the parallel verification and insertion of the information produced by different nodes. The proposed solution allows the usage of different consensus or configurations at the block level and the transaction level. As a consequence, our solution aims to improve availability and integrity of information produced in IoT environments.

2. Motivation

Despite the potential benefits of using blockchain technology for IoT, the adoption of this technology depends on a design that suits IoT applications. High resource consumption, scalability, and slow transaction processing times are persisting problems for the integration of blockchain technologies for IoT. For example, the blockchain provided by Bitcoin is not suitable for IoT devices: its size (storage) and the time to insert a new information (latency) is higher than expected in an IoT environment [Conoscenti et al. 2016]. Different research [Dorri et al. 2017, Boudguiga et al. 2017, Novo 2018, Lunardi et al. 2018] focused on different aspects of blockchain (architecture, protocols, data management, and application) that contributed to the adoption of blockchain in IoT scenarios.

However, there are still open issues related to a lightweight consensus algorithm that can be used in IoT environments that considers devices' hardware constraints and low latency requirements. Consequently, there is a lack of solutions that can be used in IoT scenarios composed of devices performing different tasks in different contexts, *e.g.*, sensors that both control the lightening and the access of a room, where different kinds of access and production of information are required. Also, there are problems related to how the information is inserted in the blockchain due to the consensus algorithm, which can lead to forks and inconsistency in the blockchain. Moreover, to the best of our knowledge, there are no discussion about consensus algorithms that can be adapted for different IoT contexts, producing better relation among security and performance (time response, throughput of transactions, etc.). It is important to note that we adopt context as a scenario or application for what IoT devices are used for.

To overcome this problem, the thesis [Lunardi 2021] proposes a multi-level consensus algorithm that considers different IoT contexts and provides parallelism to the insertion of transactions in the blockchain. This multi-level consensus is based on the two levels of insertions in appendable-block blockchains: block-level (or block header insertion) and transaction level (insertions of transactions in the block ledger). Also, it allows the insertion using an adaptive mechanism for different contexts. This model is part of and is evaluated through an appendable-block blockchain framework [Lunardi et al. 2019a].

3. Objectives

In order to provide an adaptable multi-level consensus that can consider both IoT context and relevant information in different applications, this thesis aims to propose a new consensus model for blockchains in IoT (particularly to appendable-block blockchains). The main goal of this model is to guarantee better performance and security for different kinds of insertions in the blockchain. For example, data insertion that can have a higher impact, *e.g.*, temperature of a water tank in industry, in the IoT environment can require a response time different from sensors that monitor the temperature in an office work space.

Additionally, a consensus algorithm that can reduce or mitigate the presence of forks and inconsistencies in the blockchain will be provided. Also, this model should support inter operation of different contexts, *i.e.*, exchanging data about a user/device that shares information in different applications. Therefore, the following statement defines the main goal of this research: *"Propose a model for multi-level consensus algorithm that can consider different IoT contexts and applications, providing better relation among security and performance for IoT environments composed by different contexts"*.

4. Contributions & Results

We proposed a model that can help blockchains to handle information from different contexts. This can help to adapt the blockchain to the application requirements. Thus, we propose a multi-level consensus mechanism that allows using different consensus algorithms for different contexts and, at the same time, provides parallelism in the consensus procedure (*e.g.*, allowing the execution of a consensus algorithm for each context in parallel). Also, the SpeedyChain framework was improved considering the advances obtained in the thesis. In accordance with our goals, the main contributions of this work are related to our feature interaction approach and they are listed next:

1. A study to investigate the state of the art about consensus algorithms used for blockchains in IoT (presented in Chapter 3 of the thesis);

2. Discussion about appendable-block blockchains and how consensus affects this blockchain (presented in Chapter 4 of the thesis);
3. The improvement of appendable-block blockchains to support different consensus algorithms for blockchains in IoT (presented in Chapter 4 of the thesis);
4. The proposal of context-based consensus algorithms at the transaction level on appendable-block blockchain (presented in Chapter 5, particularly on Section 5.1);
5. The proposal of a multi-level consensus model, allowing the adoption of different consensus algorithms for blocks and transactions (presented in Chapter 5, particularly in Section 5.2 of the thesis);
6. Analysis of different experiments, considering different IoT scenarios to evaluate the impact of consensus algorithms over block insertion in the blockchain (presented in Chapter 6 of the thesis);
7. Context-based consensus evaluation and discussion on the adoption of different configurations (presented in Chapter 7 of the thesis).

5. Subproducts of the thesis

During the first year of the PhD, the first steps of the research and partial results were published in peer-reviewed venues [Lunardi et al. 2018, Michelin et al. 2018, Zorzo et al. 2018]. Additionally, a work called "Performance concern in IoT Ledgers" was accepted as a poster (although not published in the proceedings) presented at the 22nd Financial Cryptography and Data Security (2018) conference. At that point, the work was in the early stages and it received valuable feedback from renowned researchers in blockchain and cybersecurity. These initial efforts works focused on the design of the appendable-block blockchain, which was developed and used during the PhD thesis.

After that - during the design, development and improvements on appendable-block blockchain - we also published our research in conferences and journals [Lunardi et al. 2019a, Nunes et al. 2020, de Arruda et al. 2020, Dedeoglu et al. 2020, Lunardi et al. 2020, Lunardi et al. 2022b]. Some of these papers were produced in collaboration with other international research groups, in particular with researchers from the University of New South Wales (UNSW) and Commonwealth Scientific and Industrial Research Organisation (CSIRO) - both from Australia - and researchers from Newcastle University - from United Kingdom. Also, as part of the academic results in the CONSEG/PUCRS research group, papers not directly related to the thesis subject were published [Neu et al. 2018, Neu et al. 2019, Bertoglio et al. 2019, Neu et al. 2020].

Furthermore, we helped in the knowledge diffusion through the publication of book chapters about blockchains in IoT. The work with shared knowledge in the collaboration with PUCRS, UNSW, and CSIRO was published as a chapter for the book "**Advanced Applications of Blockchain Technology**" [Dedeoglu et al. 2020]. Also, a work about appendable-block blockchains was published as a book chapter for the book "**Advances in Information Security, Privacy, and Ethics**" [Michelin et al. 2021]. Finally, as the result of the collaboration with Newcastle Univerisity, an overview about the applications of blockchain in Smart Cities was discussed in a book chapter for the "**Blockchains - A Handbook on Fundamentals, Platforms and Applications**"[Lunardi et al. 2022a]. A complete list of publications is presented in Table 1.

Moreover, during the PhD, it was possible to participate in three different research projects about blockchain with companies: with a financial institution and with

Table 1. Publications during the PhD research.

Paper Title	Venue or Book Name	# citations	Qualis[a]
Publications related to the Thesis - First Author			
1. Distributed access control on IoT ledger-based architecture [Lunardi et al. 2018]	**IEEE/IFIP Network Operations and Management Symposium**	*47*	A2
2. Impact of consensus on appendable-block blockchain for IoT [Lunardi et al. 2019a][b]	**EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services**	*14*	A4
3. Context-based consensus for appendable-block blockchains [Lunardi et al. 2020]	**IEEE International Conference on Blockchain**	*7*	A4
4. Performance and cost evaluation of smart contracts in collaborative health care environments [Lunardi et al. 2019b]	**International Conference for Internet Technology and Secured Transactions**	*4*	A4
5. Consensus algorithms on appendable-block blockchains: impact and security analysis [Lunardi et al. 2022b]	**Mobile Networks and Application Journal**	-	A2
6. Estruturando diferentes aplicações com Blockchain [Lunardi and Zorzo 2020]	**SBC Horizontes**	-	C
7.When Blockchain meets Smart Cities: Opportunities, Security and Future Research [Lunardi et al. 2022a][c]	**Blockchains - A Handbook on Fundamentals, Platforms and Applications**	-	-
Publications related to the Thesis - not first author			
8. SpeedyChain: A framework for decoupling data from blockchain for smart cities [Michelin et al. 2018]	**EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services**	*105*	A4
9. Blockchain technologies for IoT [Dedeoglu et al. 2020]	**Advanced Applications of Blockchain Technology**	*56*	-
10. Dependable IoT using blockchain-based technology [Zorzo et al. 2018]	**Latin-American Symposium on Dependable Computing**	*33*	A4
11. A journey in applying blockchain for cyberphysical systems [Dedeoglu et al. 2020]	**International Conference on COMmunication Systems NETworkS**	*21*	A3
12. Data-Driven Model-Based Analysis of the Ethereum Verifier's Dilemma [Alharby et al. 2020]	**IEEE/IFIP International Conference on Dependable Systems and Networks**	*8*	A1
13. Context-based smart contracts for appendable-block blockchains [Nunes et al. 2020]	**IEEE International Conference on Blockchain and Cryptocurrency**	*7*	A4
14. Appendable-block Blockchain Evaluation over Geographically-Distributed IoT Networks [de Arruda et al. 2020]	**IEEE International Black Sea Conference on Communications and Networking**	*2*	A4
15. Avaliação do uso de Smart Contracts para Sistema de Saúde Colaborativa [Branco et al. 2019][b]	**Escola Regional de Redes de Computadores**	*2*	-
16. Modelo de negócio para saúde colaborativa usando smart contracts: caso TokenHealth [Branco et al. 2020]	**Revista Brasileira de Computação Aplicada**	*2*	B3
17. SpeedyChain - A framework for decoupling data from blockchain [Zorzo et al. 2018]	**INPI - Instituto Nacional da Propriedade Industrial**	-	-
18. Appendable-Block Blockchains: Overview, Applications, and Challenges [Michelin et al. 2021]	**Enabling Blockchain Technology for Secure Networking and Communications**	-	-
Other cybersecurity publications			
19. Lightweight IPS for port scan in OpenFlow SDN networks [Neu et al. 2018][b]	**IEEE/IFIP Network Operations and Management Symposium Workshops**	*13*	A2
20. Gerenciamento de incidentes em SIEM seguindo ITIL[Neu et al. 2020]	**Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação**	*1*	B4
21. Pentest on an Internet Mobile App: A Case Study using Tramonto [Bertoglio et al. 2019]	**International Conference for Internet Technology and Secured Transactions**	*1*	A4
22. Extração e Gerenciamento de Incidentes em SIEM [Neu et al. 2019]	**Escola Regional de Redes de Computadores**	*1*	-

[a] According to Qualis 2019

[b] Best paper of the conference.

[c] Accepted to be published.

two software development companies. These projects helped to understand important aspects that should be considered for the adoption of blockchains in real scenarios [Branco et al. 2019, Lunardi et al. 2019b, Branco et al. 2020]. Finally, the proposed Framework - called SpeedyChain - was registered as software in the National Institute of

Industrial Property (INPI), entitled "**SpeedyChain - A framework for decoupling data from blockchain**" and with process number BR512018001343-0 [Zorzo et al. 2018].

5.1. International Collaborations

We collaborated with renowned researchers to improve the quality of the research in the blockchain. First, in a research internship funded by the Australian Academy of Science, we could visit and collaborate with Salil S. Kanhere from the University of New South Wales - Australia. Also, in a PhD Sandwich funded by CAPES, we could improve our solution and collaborate with Professor Aad van Moorsel and other researchers from Newcastle University - UK.

These collaborations helped to guide the research and the development of this thesis, as well to improve the definition of the scope of this work. Also, it helped to expand the research, considering different aspects. As result, we published in different conferences, journals, and book chapters (Table 1).

6. Final Considerations

We proposed and presented in thesis a multi-level consensus model for appendable-block blockchains. This model supports consensus at the block level and transaction level, as well as supporting the execution of different consensus for each context. We presented experiments, showing the results of using different consensus algorithms at the block level in appendable-block blockchain. Even using scenarios composed by a million of transactions, consensus was performed in less than a second in emulated scenarios.

Furthermore, we evaluated a context-based consensus at the transaction level. Our solution can solve two existing issues in appendable-block blockchains, namely the Eclipse attack performed by a single malicious gateway and the lack of transaction consensus. Also, the evaluation achieved a total latency under 550ms and throughput above 100 transactions per second. The best results were obtained using multiple contexts with a limited number of gateways and a limited number of transactions per consensus round. Our proposed solution uses a blockchain with a different data structure with better performance than many commercial blockchain solutions (*e.g.*, Bitcoin and IOTA).

Finally, different consensus and configurations leads to improvements in performance or resilience. Consequently, we could present a consensus mechanism that can handle different blockchain applications (using contexts) that can be adapted to have a better relation among performance and security for different IoT environments.

References

Alharby, M., Castagna Lunardi, R., Aldweesh, A., and van Moorsel, A. (2020). Data-Driven Model-Based Analysis of the Ethereum Verifier's Dilemma. In *IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 209–220.

Bertoglio, D. D., Girotto, G., Neu, C. N., and Lunardi, R. C. (2019). Pentest on an Internet Mobile App: A Case Studyusing Tramonto. In *International Conference for Internet Technology and Secured Transactions*, pages 1–6.

Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., and Sirdey, R. (2017). Towards Better Availability and Accountability for IoT Updates by Means of a Blockchain. In *IEEE European Symposium on Security and Privacy Workshops*, pages 50–58.

Branco, V., Lippert, B., Lunardi, R., Nunes, H., Neu, C., Zorzo, A., Pirolla, D., and Spacov, S. (2020). Modelo de negócio para saúde colaborativa usando smart contracts: caso TokenHealth. *Revista Brasileira de Computação Aplicada*, pages 134–144.

Branco, V., Lippert, B., Nunes, H., Lunardi, R., and Zorzo, A. (2019). Avaliação do uso de smart contracts para sistema de saúde colaborativa. In *Escola Regional de Redes de Computadores*, pages 9–16, Porto Alegre, RS, Brasil. SBC.

Conoscenti, M., Vetro, A., and Martin, J. C. D. (2016). Blockchain for the Internet of Things: A systematic literature review. In *IEEE/ACS International Conference of Computer Systems and Applications*, pages 1–6.

de Arruda, E. H. P., Lunardi, R. C., Nunes, H. C., Zorzo, A. F., and Michelin, R. A. (2020). Appendable-block Blockchain Evaluation over Geographically-Distributed IoT Networks. In *IEEE International Black Sea Conference on Communications and Networking*, pages 1–6.

Dedeoglu, V., Dorri, A., Jurdak, R., Michelin, R. A., Lunardi, R. C., Kanhere, S. S., and Zorzo, A. F. (2020). A Journey in Applying Blockchain for Cyberphysical Systems. In *International Conference on COMmunication Systems NETworkS*, pages 383–390.

Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R. C., Michelin, R. A., Zorzo, A. F., and Kanhere, S. S. (2020). *Blockchain Technologies for IoT*, chapter 3, pages 55–89. Springer Singapore.

Dorri, A., Steger, M., Kanhere, S. S., and Jurdak, R. (2017). BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Communications Magazine*, 55(12):119–125.

Jerkins, J. A. (2017). Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code. In *IEEE Computing and Communication Workshop and Conference*, pages 1–5.

Lunardi, R. C. (2021). *Multi-level consensus algorithm for appendable-block blockchains in IoT Environments*. PhD thesis, Ponitical Catholic University of Rio Grande do Sul (PUCRS). Full thesis is available at https://repositorio.pucrs.br/dspace/handle/10923/17355.

Lunardi, R. C., Alharby, M., Nunes, H. C., Dong, C., Zorzo, A. F., and van Moorsel, A. (2020). Context-based consensus for appendable-block blockchains. In *IEEE International Conference on Blockchain*, pages 401–408.

Lunardi, R. C., Michelin, R. A., Alharby, M., Dedeoglu, V., Nunes, H. C., de Arruda, E., , Zorzo, A. F., and Moorsel, A. (2022a). When Blockchain meets Smart Cities: Opportunities, Security and Future Research. In *Blockchains - A Handbook on Fundamentals, Platforms and Applications*, page 43 p. Springer. To be published soon.

Lunardi, R. C., Michelin, R. A., Neu, C. V., Nunes, H. C., Zorzo, A. F., and Kanhere, S. S. (2019a). Impact of Consensus on Appendable-Block Blockchain for IoT. In *2EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, page 228–237. Association for Computing Machinery.

Lunardi, R. C., Michelin, R. A., Neu, C. V., and Zorzo, A. F. (2018). Distributed access control on IoT ledger-based architecture. In *IEEE/IFIP Network Operations and Management Symposium*, pages 1–7.

Lunardi, R. C., Michelin, R. A., Nunes, H. C., Neu, C. V., Zorzo, A. F., and Kanhere, S. S. (2022b). Consensus algorithms on appendable-block blockchains: impact and security analysis. *Mobile Networks and Applications*, Springer:1–12.

Lunardi, R. C., Nunes, H. C., Branco, V., Lippert, B., Neu, C. V., and Zorzo, A. F. (2019b). Performance and Cost Evaluation of Smart Contracts in Collaborative Health Care Environments. In *International Conference for Internet Technology and Secured Transactions*, pages 1–6.

Lunardi, R. C. and Zorzo, A. F. (2020). Estruturando diferentes aplicações com blockchain. SBC Horizontes, ISSN 2175-9235.

Michelin, R. A., Castagna Lunardi, R., Nunes, H. C., Dedeoglu, V., Neu, C. V., Zorzo, A. F., and Kanhere, S. S. (2021). Appendable-Block blockchains. In *Advances in Information Security, Privacy, and Ethics*, pages 66–88. IGI Global.

Michelin, R. A., Dorri, A., Steger, M., Lunardi, R. C., Kanhere, S. S., Jurdak, R., and Zorzo, A. F. (2018). SpeedyChain: A Framework for Decoupling Data from Blockchain for Smart Cities. In *EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pages 145–154. ACM.

Neu, C., Trebien, E., Bertoglio, D., Lunardi, R., and Zorzo, A. (2019). Extração e gerenciamento de incidentes em SIEM. In *Escola Regional de Redes de Computadores*, pages 190–195, Porto Alegre, RS, Brasil. SBC.

Neu, C., Trebien, E., Bertoglio, D., Lunardi, R., and Zorzo, A. (2020). Gerenciamento de incidentes em siem seguindo itil. *Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação*, 3(1):1–10.

Neu, C. V., Tatsch, C. G., Lunardi, R. C., Michelin, R. A., Orozco, A. M. S., and Zorzo, A. F. (2018). Lightweight IPS for port scan in OpenFlow SDN networks. In *IEEE/IFIP Network Operations and Management Symposium Workshops*, pages 1–6.

Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal*, 5(2):1184–1195.

Nunes, H. C., Lunardi, R. C., Zorzo, A. F., Michelin, R. A., and Kanhere, S. S. (2020). Context-based Smart Contracts For Appendable-block Blockchains. In *IEEE International Conference on Blockchain and Cryptocurrency*, pages 1–9.

Zorzo, A. F., Neu, C. V., Michelin, R. A., and Lunardi, R. C. (2018). Speedychain - a framework for decoupling data from blockchain. Patente: Programa de Computador. Número do registro: BR512018001343-0, data de registro: 01/08/2018. Instituição de registro: INPI - Instituto Nacional da Propriedade Industrial.

Zorzo, A. F., Nunes, H. C., Lunardi, R. C., Michelin, R. A., and Kanhere, S. S. (2018). Dependable IoT Using Blockchain-Based Technology. In *Latin-American Symposium on Dependable Computing*, pages 1–9.