MARTSIA: A Tool for Confidential Data Exchange via Public Blockchain

Michele Kryston[1,2], Edoardo Marangone[1], Claudio Di Ciccio[2], Daniele Friolo[1], Eugenio Nerio Nemmi[1], Mattia Samory[1], Michele Spina[1], Daniele Venturi[1], and Ingo Weber[3]

[1] Sapienza University of Rome, Rome, Italy
kryston.1844733@studenti.uniroma1.it; edoardo.marangone@uniroma1.it
[2] Utrecht University, Utrecht, the Netherlands, m.kryston@uu.nl; c.diciccio@uu.nl
[3] School of CIT, Technical University of Munich and Fraunhofer Gesellschaft, Munich, Germany, ingo.weber@tum.de

Abstract. Blockchain technology streamlines multi-party collaborations in decentralized settings, especially when trust is limited or difficult to establish. While public blockchains enhance transparency and reliability by replicating data across all network nodes, they also conflict with confidentiality. Here, we introduce Multi-Authority Approach to Transaction Systems for Interoperating Applications (MARTSIA) to address this challenge. MARTSIA provides fine-grained read-access control at the message-part level by combining user-defined policies with certifier-declared attributes. The approach guarantees that even though data is replicated across the network to maintain consistency, fault tolerance, and availability, its confidentiality is securely preserved through encryption. To this end, MARTSIA integrates blockchain technologies, Multi-Authority Attribute-Based Encryption, and distributed hash-table file storages. This architecture effectively balances the transparency inherent in public blockchains with the privacy required for sensitive applications. We present the tool and its applicability in a business scenario.

Keywords: Business Process Management · Blockchain Technology · Multi-Authority Attribute Based Encryption · InterPlanetary File System · Ciphertext Policy

1 Introduction

The emergence of blockchain technology has reshaped secure and transparent interactions among untrusted parties [10]. This technology provides security, ensured by cryptography; resilience, achieved through the decentralization of network nodes; and transparency, as anyone can verify past transactions recorded in the ledger. Public blockchain protocols strengthen these guarantees at scale, as they resort to an open peer-to-peer network, where data is replicated across all nodes, improving its availability and integrity. In modern business environments, these blockchain properties offer significant advantages over traditional

Pre-print copy of the manuscript published by Springer (available at link.springer.com) identified by DOI: 10.1007/978-3-031-94590-8_21

e-business models, which for decades have relied on centralized databases and intermediaries to safeguard trust and enforce processes. Centralized systems excel in effectiveness although they suffer in several aspects such as single points of failure, susceptibility to data breaches and inefficiencies in data reconciliation between multiple parties. Public blockchains typically entail non-negligible operational costs and additional processing times due to their decentralized nature, but these aspects are often compensated by the security and transparency they guarantee. As a result, blockchain technology has experienced increasing adoption in information systems within enterprise domains over the last few years [9]. Nevertheless, full data transparency may pose a problem in multi-party business settings wherein sensitive information needs to be kept confidential between involved participants [4,13].

To overcome this issue, we bridge the silos of blockchain technologies and encryption with information systems engineering. In this paper, we present the tool implementation of Multi-Authority Approach to Transaction Systems for Interoperating Applications (MARTSIA) [6], a fully decentralized framework providing confidential information sharing through public blockchain technologies, Multi-Authority Attribute-Based Encryption (MA-ABE), and distributed hash-table file storages. Inspired by the Control Access via Key Encryption (CAKE) approach [7], MARTSIA enhances decentralization by removing CAKE's central nodes needed for data encryption and decryption.

The paper proceeds as follows. In Sect. 2, we discuss the underlying technologies of the framework, while Sect. 3 introduces a running example. In Sect. 4, we present its features by depicting the application of MARTSIA in the running example. Section 5 evaluates the maturity of the framework, assessing its versions and readiness for deployment. In Sect. 6, we review related work in the literature, placing MARTSIA in the context of existing solutions. Finally, Sect. 7 concludes the paper and proposes directions for future research and development.

2 Background

Before delving into our approach, in this section we discuss its building blocks.

A **blockchain** is a decentralized and distributed ledger that stores transactions securely and tamper-resistantly. Transactions are stored in blocks linked to the previous one, forming a chain. This structure ensures transparency, security, and immutability of recorded information. Most blockchains, such as Ethereum,[4] are additionally featured with the ability to execute code, namely **smart contracts**, in a decentralized manner through virtual machines, thus allowing complex protocols to be built at an application layer.

The cost of performing a transaction primarily depends on the amount of information being stored and, in the case of a smart contract, on the computational effort required for execution. For this reason, users often leverage additional technologies, such as distributed hash-table file storages, to store large

[4] https://ethereum.org/, accessed: 2025-03-12.

Pre-print copy of the manuscript published by Springer (available at link.springer.com)
identified by DOI: 10.1007/978-3-031-94590-8_21

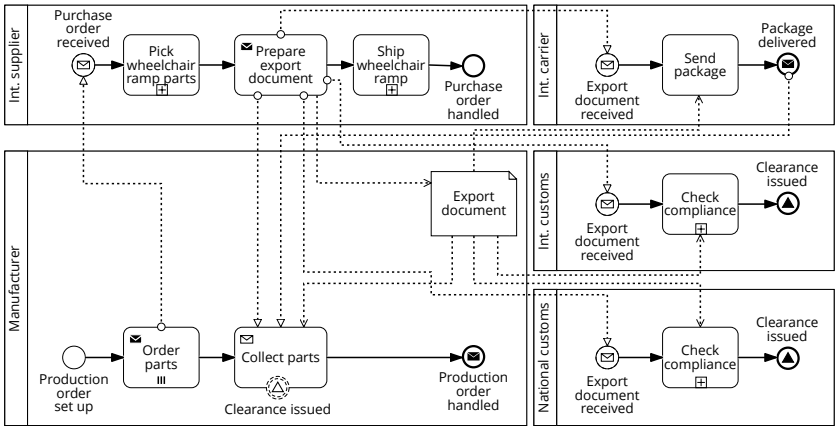

Fig. 1. A segment of the collaboration diagram illustrating the control and data flow of the process

amounts of data. An example is **InterPlanetary File System** (**IPFS**). As on public blockchains, data stored on IPFS are decentralized and transparent, making them accessible to anyone. IPFS allows data retrieval via content-addressed locators, e.g., the hash of the stored data. In this way, a single-byte difference between two data generates a completely different locator. These locators can then be stored on the blockchain to benefit from its properties.

Access to data stored on IPFS can be restricted to specific users through the application of **Attribute-Based Encryption (ABE)**. ABE, a public-key encryption scheme, links encrypted data with corresponding decryption keys via attributes. One type of ABE is Ciphertext-Policy Attribute-Based Encryption (CP-ABE), where each user is associated with attributes and data are encrypted using policies, e.g., logical formulas built upon user attributes. However, CP-ABE relies on a single authority to generate user decryption keys. MA-ABE [1] overcomes this limitation by improving decentralization. In MA-ABE, multiple authorities generate partial decryption keys. The user who requests the partial keys can merge them, obtaining a complete key to decrypt the data.

3 Running Example

In this section, we introduce a running example that we will use throughout the paper to provide a clearer explanation of MARTSIA.

Figure 1 depicts a Business Process Model and Notation (BPMN) collaboration diagram illustrating a fragment of a supply-chain process in the automotive sector: the production of a custom car for an individual with paraplegia. In this fragment of the process, the Manufacturer proceeds to acquire the necessary ramp components for the cars if they are unavailable; in this situation, the Manufacturer orders them from an International supplier. International customs

Pre-print copy of the manuscript published by Springer (available at link.springer.com) identified by DOI: 10.1007/978-3-031-94590-8_21

Table 1. The Export document in clear, sent by the International supplier

Slice	Recipients	Data	Policy

1	Manufacturer
	Nat. customs
	Int. customs
	Int. carrier
		`Manufacturer:Beta`
		`Delivery: 8, B Lane`
		`E-mail: b@mail.com`
		`Ramp run: 3`
		`Kickplate: 12`
		`Amount_paid: $5000`
			`Customs@A or`
			`((Supplier@C and`
			`International@B) or`
			`Manufacturer@A or`
			`(Carrier@B and`
			`International@C))`

2	Nat. customs
	Int. customs
		`Workers_rights: Ok`
		`Human_rights: Ok`
		`Ecosys_protection: Ok`
			`Customs@A or`
			`(Supplier@D and`
			`International@B)`

3	Manufacturer	`Manufacturer:Beta`
		`Address: 8, B Lane`
		`Reference: 26487`
			`(Supplier@2+ and`
			`International@B) or`
			`Manufacturer@A`

4	Manufacturer
	Nat. customs
	Int. customs
		`Invoice_ID: 101711`
		`Billing: 5, G Lane`
		`Gross_total: $5000`
		`Company_VAT: U12345678`
		`Issue_date: 2022-05-12`
			`Customs@A or`
			`((Supplier@C and`
			`International@B) or`
			`Manufacturer@A)`

supervises the international transit of goods, while National customs supervises the national transit. Both dispense Customs clearance. Thereafter, the International carrier ships the goods to the Manufacturer. We will focus on the Export document in Fig. 1, which comprises multiple records, presented in Table 1 as four distinct slices. Given a single sender, the International supplier, we have different recipients for each slice: the Manufacturer, the National customs, the International customs, and the International carrier.

4 Innovations and Features

In this section, we explain the components and operations of MARTSIA considering the example described in Sect. 3.

Figure 2 outlines the general architecture of MARTSIA. Our solution provides three main functionalities: *(i)* **Store actor metadata**, assigning attributes to users. Considering our example, the chosen attributes designated to match the actors' names are: `Supplier`, `Manufacturer`, `Customs`, and `Carrier`. Furthermore, we introduce the `International` attribute. The International supplier, the International customs, and the International carrier are thus characterized by the conjunction of the `International` attribute with `Supplier`, `Customs`, and `Carrier`, respectively; *(ii)* **Store encrypted data**, applying a policy expressed as a propositional formula built upon users' attributes, thereby restricting access only to authorized actors. Table 1 outlines the policies governing read access to the Export document; *(iii)* **Read encrypted data**, accessing and decrypting data if the requester's attributes satisfy the access policy. In the example, column *Data* in Table 1 shows the decrypted data. These three functionalities include the support of other tasks (depicted in grey in the figure) we explain next.

Our solution employs three fundamental components: *(i)* the **Certification Manager** records the attributes the users hold in a collaborative process; *(ii)* the **Data Manager** encrypts and stores data; and the *(iii)* **Key Manager** gener-

Pre-print copy of the manuscript published by Springer (available at link.springer.com)
identified by DOI: 10.1007/978-3-031-94590-8_21

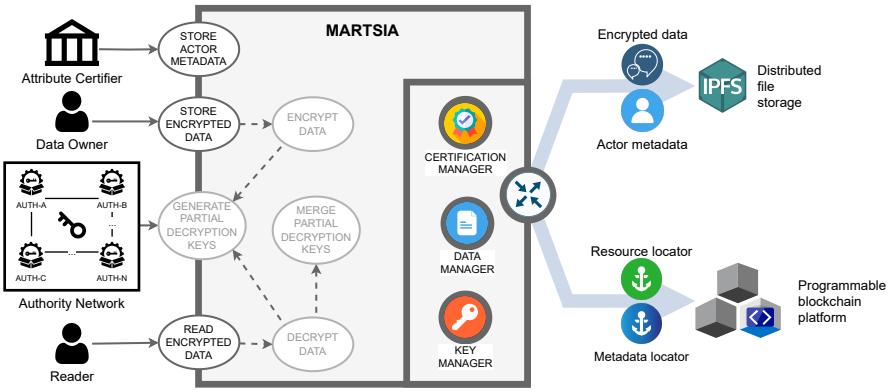

Fig. 2. An overview of the MARTSIA architecture

ates partial decryption keys derived from the user's attributes. The user merges these partial decryption keys into a single key to read encrypted data.

Four main classes of actors are involved in the interaction: *(i)* the **Attribute Certifier** deploys the smart contracts, and assigns and stores the actors' metadata; *(ii)* the **Data Owner** encrypts, determines reading access to the data, and stores it for sharing. In our example, this role is played by the International supplier, who encrypts the Export document; *(iii)* the **Reader** interested in reading the shared data. In the example, this role is fulfilled by the International supplier and the Recipients in Table 1; *(iv)* the **Authority Network** generates partial decryption keys tailored to the Reader's attributes. Henceforth, we assume that the network consists of four Authorities: A, B, C, and D.

Due to the costs associated with storing data directly on the blockchain, MARTSIA stores on InterPlanetary File System (IPFS)[5] the encrypted data and the actors' metadata, along with additional information. Smart contracts on the blockchain are employed to record IPFS locators, ensuring data integrity. Consequently, although anyone can access the public ledger, it cannot discern information about the encrypted data, the Data Owners, or the Readers. Confidentiality with recipients is preserved by uniquely denoting each process instance with an identifier. This identifier, automatically added to the policies by MARTSIA, is used to characterize the actors involved, thereby limiting the range of potential Readers. The Data Owner must specify the Authorities responsible for validating each policy. Considering the running example in Sect. 3, the complete access policy of the third slice in Table 1 reads as follows: `(43175279@4+ and ((Supplier@2+ and International@B) or Manufacturer@A))`. In this case: the process instance `43175279` needs to be verified by all the Authorities, the attribute `Supplier` by at least two, attribute `International` by Authority B, and attribute `Manufacturer` by Authority A. This policy specifies that the International supplier (the sender) and the Manufacturer involved in process instance

[5] https://ipfs.tech/, accessed: 2025-03-12.

Pre-print copy of the manuscript published by Springer (available at link.springer.com) identified by DOI: 10.1007/978-3-031-94590-8_21

43175279 can access this slice. A detailed explanation of the policies and their grammar can be found in [5].

Following the encryption phase, the International supplier uploads the document to IPFS through MARTSIA. The corresponding IPFS resource locator (e.g., `Qmb4Hz[...]CAd8iG`) is then stored on the blockchain and associated with a unique *message ID*. Since the Export document includes multiple slices for various recipients, each record has also a unique *slice ID*. To obtain the decryption key, a Reader must request all the partial decryption keys to the Authorities. The Authorities generate these partial keys using the Reader's metadata retrieved from the blockchain. Then, the Reader assembles the key parts, obtaining the final key necessary to read the encrypted data. To retrieve them, we have implemented secure channels resorting to TLS (direct) and RSA (via blockchain). In our example, if the Manufacturer intends to read the third slice of the Export document (Table 1), they must request the decryption keys to all the Authorities. If the Manufacturer is involved in the process instance 43175279 and possesses the correct `Manufacturer` attribute, they meet the policy requirements for decryption. In contrast, the National customs, which only holds the `Customs` attribute, does not meet the access policy and is consequently unable to decrypt the content. An actor lacking authorization from all the Authorities cannot decrypt the data. Although different Authorities collaborate in validating the policy's formulae, the record can be decrypted only by the requesting actor.

Here, we can derive a core feature of MARTSIA. Multiple Readers read distinct slices out of a single encrypted data object. Therefore, one message can be generated for multiple Readers interested in separate parts of it, rather than sending a copy for each such part, at the risk of potential inconsistency and communication overhead. In our example, we have one Export document sliced into four parts, accessible by four, two, one, and three participants, respectively. However, the message remains one, rather than being spread across ten replicas.

5 Maturity

In this section, we describe the current state of the MARTSIA tool.

We implemented MARTSIA in two different variants, to show its platform-independence. Its smart contracts run on the Ethereum Virtual Machine (EVM) and the Algorand Virtual Machine (AVM). Smart contracts are written in Solidity v. 0.8.20 for EVM and PyTeal v. 0.20.0 for AVM. All other scripts are encoded in Python, including the integration with IPFS. The source code and documentation with implementation details are available at `github.com/apwbs/MARTSIA`. Among other things, the tool also includes additional features such as the possibility to use multiple Attribute Certifiers employing multi-signature operations, and the customizability of the communication means to exchange partial decryption keys (either direct, via TLS channels, or indirect, via blockchain). Furthermore, we include the input data, launching scripts, and experimental results of performance tests run on different EVM blockchains to verify transaction costs and latency, and a Wiki offering a step-by-step tutorial on system setup

Pre-print copy of the manuscript published by Springer (available at link.springer.com)
identified by DOI: 10.1007/978-3-031-94590-8_21

and operation. To demonstrate MARTSIA's versatility across key domains, we integrated and tested our prototype with three publicly available DApps from different domains: NFT trading, supply-chain management, and retail [5].

The scripts and Wiki to reproduce this demo for the EVM version are available at github.com/apwbs/MARTSIA-Demo. For a brief video showcase, visit youtube.com/watch?v=RAcifWw1_B0.

6 Related Work

In recent years, blockchain technology has experienced significant developments due to its distinctive properties, sparking growing interest in solutions to ensure data confidentiality. Zou et al. [14] propose SPChain, a system built upon blockchain to guarantee privacy and effortless sharing of medical data. This is achieved through a proxy re-encryption scheme and local databases of medical institutions. Gan et al. [3] present a search method for encrypted medical data stored on a blockchain, resorting to an access control mechanism. Their architecture relies on: a consortium blockchain built on Ethereum for experimental analysis; several encryption methods such as probabilistic encryption and order-preserving encryption; and a non-relational database to store data. Remaining in the medical field, Miyachi and Mackey [8] introduce a framework for data privacy based on both on-chain and off-chain systems. They leverage consortium blockchains and asymmetric cryptography, while storing data off-chain. Unlike [3,8,14], MARTSIA operates on public blockchains to store IPFS locators, encrypts sensitive information with MA-ABE, and stores data on IPFS.

Yan et al. [12] illustrate a scheme providing fine access control with low computational consumption. Their work leverages blockchain to store metadata, IPFS to store data, and proxies for encryption and decryption. In addition, their scheme provides policy hiding and attribute revocation. However, two centralized entities are employed: the Proxy encryption server (ES) and the Proxy decryption server (DS). Wu et al. [11] in their work present an efficient attribute-based encryption scheme to ensure privacy. Their method leverages the blockchain for non-repudiation and data integrity. Feng et al. [2] introduce a scheme utilizing blockchain for data storage; and identity-based encryption (IBE) and attribute-based encryption (ABE) for sharing and verifying the correctness of data. In their scheme, there is a centralized entity called Private Key Generator that takes care of the setup phase and attribute key generation. In contrast to [2,11,12], our solution utilizes a decentralized attribute-based encryption scheme.

7 Conclusion and Future Work

In this paper, we introduced MARTSIA, a framework leveraging blockchain and MA-ABE to control data access in multi-party business scenarios. Our approach resorts to IPFS to store encrypted data and actors' metadata, and to smart contracts to link IPFS resource locators to the blockchain. MARTSIA guarantees access control, data reliability, immutability, and auditability in a decentralized

Pre-print copy of the manuscript published by Springer (available at link.springer.com)
identified by DOI: 10.1007/978-3-031-94590-8_21

manner. Areas for future development include data access revocation through InterPlanetary Name System (IPNS), automatic policy validation, conducting robustness field tests, and expanding the policy language to open the door to secure data calculations using TEEs.

Acknowledgments. This work was partly funded by projects SERICS (PE00000014) under the NRRP MUR program funded by the EU-NGEU, PINPOINT (B87G22000450001) under the PRIN MUR program, and Health-e-Data, funded by the EU-NGEU under the Cyber 4.0 NRRP MIMIT programme.

References

1. Chase, M.: Multi-authority attribute based encryption. In: TCC. vol. 4392, pp. 515–534 (2007)
2. Feng, T., Wang, D., Gong, R.: A blockchain-based efficient and verifiable attribute-based proxy re-encryption cloud sharing scheme. Inf. **14**(5), 281 (2023)
3. Gan, C., Yang, H., Zhu, Q., Zhang, Y., Saini, A.: An encrypted medical blockchain data search method with access control mechanism. Inf. Process. Manag. **60**(6), 103499 (2023)
4. Köpke, J., Necemer, M.: Measuring the effects of confidants on privacy in smart contracts. In: BPM (Blockchain and RPA Forum). vol. 459, pp. 84–99 (2022)
5. Marangone, E., Di Ciccio, C., Friolo, D., Nemmi, E.N., Venturi, D., Weber, I.: Enabling data confidentiality with public blockchains. CoRR **abs/2308.03791** (2023)
6. Marangone, E., Di Ciccio, C., Friolo, D., Nemmi, E.N., Venturi, D., Weber, I.: MARTSIA: enabling data confidentiality for blockchain-based process execution. In: EDOC. vol. 14367, pp. 58–76 (2023)
7. Marangone, E., Di Ciccio, C., Weber, I.: Fine-grained data access control for collaborative process execution on blockchain. In: BPM (Blockchain and RPA Forum). vol. 459, pp. 51–67 (2022)
8. Miyachi, K., Mackey, T.: hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Inf. Process. Manag. **58**(3), 102535 (2021)
9. Stiehle, F., Weber, I.: Blockchain for business process enactment: A taxonomy and systematic literature review. In: BPM (Blockchain and RPA Forum). vol. 459, pp. 5–20 (2022)
10. Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., Mendling, J.: Untrusted business process monitoring and execution using blockchain. In: BPM. vol. 9850, pp. 329–347 (2016)
11. Wu, A., Zhang, Y., Zheng, X., Guo, R., Zhao, Q., Zheng, D.: Efficient and privacy-preserving traceable attribute-based encryption in blockchain. Ann. des Télécommunications **74**(7-8), 401–411 (2019)
12. Yan, L., Ge, L., Wang, Z., Zhang, G., Xu, J., Hu, Z.: Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment. J. Cloud Comput. **12**(1), 61 (2023)
13. Zhang, R., Xue, R., Liu, L.: Security and privacy on blockchain. ACM Comput. Surv. **52**(3), 51:1–51:34 (2019)
14. Zou, R., Lv, X., Zhao, J.: SPChain: Blockchain-based medical data sharing and privacy-preserving ehealth system. Inf. Process. Manag. **58**(4), 102604 (2021)

This document is a pre-print copy of the manuscript
(Kryston et al. 2025)
published by Springer (available at link.springer.com).

The final version of the paper is identified by DOI: 10.1007/978-3-031-94590-8_21

References

Kryston, Michele, Edoardo Marangone, Claudio Di Ciccio, Daniele Friolo, Eugenio Nerio Nemmi, Mattia Samory, Michele Spina, Daniele Venturi, and Ingo Weber (2025). "MARTSIA: A Tool for Confidential Data Exchange via Public Blockchain". In: *CAiSE Forum*. Ed. by Luise Pufahl, Kristina Rosenthal, Sergio España, and Selmin Nurcan. Vol. 557. Lecture Notes in Business Information Processing. Springer, pp. 173–180. ISBN: 978-3-031-94589-2. DOI: 10.1007/978-3-031-94590-8_21.

BibTeX

```
@InProceedings{   Kryston.etal/CAiSEForum2025:MARTSIAToolConfidential,
  author        = {Kryston, Michele and Marangone, Edoardo and Di Ciccio,
                   Claudio and Friolo, Daniele and Nemmi, Eugenio Nerio and
                   Samory, Mattia and Spina, Michele and Venturi, Daniele and
                   Weber, Ingo},
  booktitle     = {CAiSE Forum},
  title         = {{MARTSIA:} {A} Tool for Confidential Data Exchange via
                   Public Blockchain},
  year          = {2025},
  pages         = {173--180},
  crossref      = {CAiSE2025Forum},
  doi           = {10.1007/978-3-031-94590-8_21},
  keywords      = {Business Process Management; Blockchain Technology;
                   Multi-Authority Attribute Based Encryption; InterPlanetary
                   File System; Ciphertext Policy}
}
@Proceedings{     CAiSE2025Forum,
  title         = {Intelligent Information Systems - CAiSE 2025 Forum and
                   Doctoral Consortium, Vienna, Austria, June 16-20, 2025,
                   Proceedings},
  year          = {2025},
  editor        = {Luise Pufahl and Kristina Rosenthal and Sergio
                   Espa{\~{n}}a and Selmin Nurcan},
  isbn          = {978-3-031-94589-2},
  publisher     = {Springer},
  series        = {Lecture Notes in Business Information Processing},
  volume        = {557}
}
```