Applications in the Automotive Sector of the Self-Sovereign Digital Identity Model on Permissioned Blockchain

Marta Lucrezia Alessandria[1]

[1]University of Rome Tor Vergata, Rome, Italy

Abstract

This paper develops a digital Driver Identification Certificate (CID) on a Multichain-based blockchain platform, aiming to provide a secure and decentralized solution for managing automotive identities. It enhances transparency and efficiency compared to traditional methods. The analysis covers benefits like reduced fraud and increased efficiency, while also addressing challenges such as complex key management and integration issues.

Keywords

Self Sovereign Identity, car's digital passport, Digital CID

1. Introduction

This paper examines how blockchain technology can address issues like inconsistent data and privacy in the automotive industry [1, 2, 3, 4]. This is due to the progress of electronic devices [5, 6, 7, 8, 9, 10]. It proposes a digital solution for car accident management, replacing the manual amicable accident statement (CID) with a smartphone application linked to a blockchain managed by insurance companies. This system automatically reports incidents and details damage, improving repair efficiency.

The paper also explores integrating Self-Sovereign Identity (SSI) and a digital car passport (PDA). SSI ensures driver identity authenticity, while the PDA, integrated with SSI, tracks car damages, repairs, and workshop details.

The work includes software design for a digital CID and demonstrates the PDA on the MultiChain blockchain. It is structured into five chapters covering blockchain fundamentals, project proposal, implementation on MultiChain, and conclusions. Overall, the paper highlights how blockchain and SSI can enhance car accident management by improving efficiency, transparency, and traceability.

2. Blockchain

Blockchain emerged in 2008 with the white paper "Bitcoin: A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto, proposing an electronic payment system without financial intermediaries, ensuring authenticity, confidentiality, non-repudiation, prevention of double spending, and reduction of intermediation costs [11]. The solution is a distributed ledger based on complex cryptographic exercises for adding new blocks, each containing transactions verified through peer-to-peer timestamps [12, 13]. The authenticity and confidentiality data are ensured by the use of asymmetric cryptographic keys.

2.1. Cryptography: Hash Functions and Asymmetric Keys

Cryptography uses algorithms and keys to encode messages, ensuring confidentiality, authenticity, integrity, and non-repudiation. Hash algorithms generate a unique string (digest) from any input, used to verify the integrity of information. However, they can present collisions, where two different texts produce the same hash.

Asymmetric cryptographic algorithms, such as RSA, use a pair of keys (public and private) to encrypt and decrypt data [14]. RSA, proposed by Diffie and Hellman and later by Rivest, Shamir, and Adleman, ensures that a private key remains secret despite the public key's knowledge.

2.2. Applications: Digital Signature

The digital signature uses asymmetric algorithms to ensure authenticity and integrity. The National Institute of Standards and Technology (NIST) proposed the Digital Signature Algorithm (DSA) as a standard. The digital signature includes the document's fingerprint, encoded with the sender's private key, and the public key accompanied by a certificate issued by a certification authority (CA), verifying the sender's identity. The recipient uses the public key to decrypt and verify the document's integrity.

2.3. Blockchain Architecture

Blockchain is a distributed ledger consisting of a chain of linked blocks, each containing data like transactions or smart contracts. Each participant in the network maintains a current copy of this chain [15]. When a block fills, it is sealed with a cryptographic hash, and the hash is included in the next block, ensuring security and immutability. Transactions use UTXO (unspent transaction output) to prevent double spending, and each transaction is timestamped and confirmed after being added to at least six subsequent blocks. Blockchain operates through a peer-to-peer network, with nodes validating transactions and miners solving Proof of Work (PoW) to add blocks, earning cryptocurrency rewards. For instance, Bitcoin miners receive rewards that halve every four years, controlling inflation and enhancing Bitcoin's value.

2.4. Operation: Consensus Algorithms

Consensus algorithms like Proof of Work (PoW) are crucial for blockchain. Nodes manage and record blocks, broadcasting transactions for network-wide validation. This includes checking syntax, block size, and fees. Valid transactions enter the Transaction Pool, awaiting block inclusion. In Bitcoin, miners solve PoW problems by finding hashes below

ICYRIME 2024: 9th International Conference of Yearly Reports on Informatics, Mathematics, and Engineering. Catania, July 29-August 1, 2024

martalucrezia1@gmail.com (M. L. Alessandria)

a set value, preventing Sybil attacks, and validating blocks for rewards.

3. Self Sovereign Identity

Historically, digital identity management relied on centralized systems or third-party Identity Providers, where central authorities issued identifiers like driver's licenses or birth certificates, limiting user control. This approach had issues such as managing multiple accounts, corporate control over personal data, vulnerabilities to theft and privacy breaches, risks of service obsolescence, high costs and complexity, and increased cybersecurity threats.

The Self-Sovereign Identity (SSI) model offers a decentralized alternative, using blockchain and cryptography to provide users full control over their digital identities. With Verifiable Credentials (VCs) and Decentralized Identifiers (DIDs), SSI enhances security, privacy, and user control by allowing individuals to prove attributes like age without revealing sensitive information. This is particularly important in the case of video applications [16, 17, 18].

3.1. Involved Institutional Bodies

In Europe, blockchain technology is promoted and managed by several institutional bodies. The European Blockchain Partnership (EBP), formed in 2018 by 27 EU member states, Norway, and Liechtenstein, aids the European Commission in developing the European Blockchain Services Infrastructure (EBSI). EBSI, supported by the Connecting Europe Facility (CEF) and the Digital Europe Programme (DEP), aims to modernize digital public services and leverage the digital single market. EBSI provides cross-border public services through a network of blockchain nodes, ensuring transparency and security. The European regulation eIDAS (Regulation (EU) No 910/2014) standardizes electronic identification and trust services, enabling digital documents to replace paper with the same legal value across the EU.

3.2. Regulatory Framework

eIDAS requires that all member states recognize electronic signatures that comply with the standards set by the regulation, thereby facilitating cross-border digital transactions. It has been implemented in various digital authentication systems across Europe, such as SPID in Italy and Signaturgesetz in Austria.

On June 3, 2021, the European Commission proposed a revision of eIDAS to create a framework supporting a European Digital Identity, including the development of a pan-European "Digital Wallet." The proposal aims to promote a more decentralized governance model, also considering the adoption of digital identity systems based on the Self-Sovereign Identity (SSI) model.

3.3. SSI Architecture

Self-Sovereign Identity (SSI) empowers users to manage their own digital identities without intermediaries or central authorities. SSI emphasizes user autonomy, control over privacy, and direct access to personal data, ensuring transparency, portability, and protection [19, 20, 21]. The model aims to create secure digital identities while preventing unauthorized access. Influenced by historical events like the Holocaust, SSI prioritizes decentralization to avoid abuses of centralized information. Its architecture relies on Verifiable Credentials (VC) and Decentralized Identifiers (DID)[22, 23, 24]. VCs are digital proofs of identity attributes, and DIDs are unique, cryptographically verified identifiers. This system ensures that only authorized individuals can update identity information, preserving data integrity and security. The architecture of a DID is as follows: The Verifiable Data Registry (VDR), often based on blockchain, is where DIDs and DID Documents are registered. This distributed ledger ensures that all changes are traceable and immutable, providing an unprecedented level of transparency and security.

4. SSI and Blockchain Applications for the Automotive Sector: The Digital CID

The work aims to identify an efficient way to manage data and communications after a road accident, using blockchain to prevent fraud and improve the transfer of information to insurance companies. It analyzes current critical issues and proposes the use of SSI (Self-Sovereign Identity) credentials and a digital car passport, enabling the digital completion of the CID (Friendly Accident Statement) through a mobile app. The following table summarizes the scenarios and use cases we are going to analyze.

Table 1
Table summarizing the scenarios and their analyzed characteristics

Features	Scenarios		
	A	*B-1*	*B-2*
Both drivers have SSI credentials.	NO	YES	NO
Only one driver has SSI credentials.	NO	NO	YES
Both cars have a digital passport.	NO	YES	NO
Only one car has a digital passport.	NO	NO	YES
It is possible to complete the digital CID through the app and report the incident to both insurers, regardless of whether the two drivers cooperate.	NO	YES	YES

4.1. Problem Statement

The main issues after an accident include:

- The exchange of large amounts of personal and sensitive data.
- Fraud risks (e.g., false identity, falsification of accident details).
- Long times to obtain funds and repairs.
- Difficulties in tracking accidents and repairs.

The proposed solution involves a private blockchain managed by various insurance companies. This would allow for the digital completion of the CID, using the digital car passport to record accidents and repairs, and Verifiable Credentials (VC) to prevent fraud. Two main scenarios post-road accidents were analyzed: a traditional one and an innovative one utilizing digital technologies.

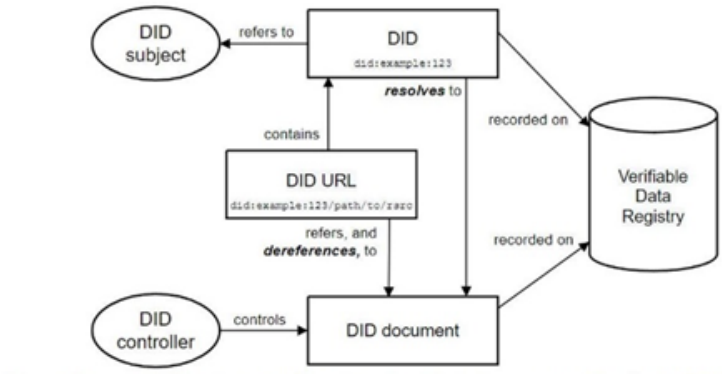

Figure 1: DID Architecture

4.2. Classical Scenario

In a typical accident, two drivers:

- **Exchange Information:** Verify identities and insurance, often on paper or via phone.
- **Determine Fault:** If no injuries, they establish fault and complete the CID. If cooperative, they submit the CID to insurers; if not, minimal details are shared.
- **Insurance Involvement:** Both insurers investigate the accident details to determine fault and assess damages.
- **Compensation:** The driver not at fault waits for insurance payout, often handling repairs independently due to delays.

4.3. Innovative Scenarios

Thanks to SSI and the car's digital passport the scenario changes. In fact, I take out an insurance policy with a certain insurance company; this company makes me install an app on my cell phone to use in case of a claim. Let's take a closer look at how this app works after the accident, referring to two possible situations 1) and 2):

Scenario 1

Assume that:

1. Both drivers possess SSI (VC) credentials approximately:

- their identity,
- their driver's license,
- their car's digital passport;

2. Both have installed the app related to incident management;

3. Both have installed the black box on their car (Same consequence of having the car's digital passport);

4. Both want to collaborate.

Steps:

a. Both drivers (who probably have insurance with different agencies) open their respective claims management app: digital CID compilation begins;

b. Both import their SSI credentials listed earlier;

c. Both enter the SSI credentials of the other driver (exchange of SSI between two holders);

d. Both of them, by mutual agreement, manually enter the description of the accident dynamics, the time, the type of damages reported by the vehicle and all the other info that are typically required in a paper CID and that are not contained in the VCs already imported before;

e. Photos or even a short video of the vehicles status are taken. The photos are somehow authenticated by the app itself, which then attaches them to the digital CID.

f. The digital CID has been completed:

o The APP is connected to an insurance company's own blockchain, so the digital CID (or its hash) is put on the blockchain, so that it is unambiguous and unrecoverable. In addition, all info related to damages reported by cars (including any photos and videos) are linked to the digital passport of the car to update it.

o The app automatically sends a copy of the digital CID to the certified email address of the relevant insurance company, saved by default;

At this point the accident report has been digitally submitted through the app provided: both insurance companies are aware of the accident and of the information recorded by the digital passport (certain) and by the individual drivers (to be verified)!

g. Once the complaint has been made, the engineers (the persons in charge) of each insurance company will be able as soon as possible to establish who is entitled to compensation both with the information they already have (digital CID), and with any information acquired following an inspection (personal or with drones) on the site of the accident, thanks to which they will verify the place of the accident: the horizontal and vertical road signs, the state of wear of the asphalt, potholes, etc.

h. After identifying the eligible motorist, the insurer that has contracted repair centers (garages) and that support SSI technologies will issue a VC to the driver to confirm the vehicle's eligibility for a repair paid for by the insurance company, so that the driver can directly present it to that garage and immediately receive the repairs he or she needs.

i. In addition, upon completion of the repair, the driver will receive a credential showing the repair, the warranty, and the fact that the garage was an authorized repairer for the car. This information would be useful to the driver when they sell the vehicle in the future, as they will have kept track of all the repairs done on their car. Therefore, all this info will go to update the SSI credentials referred to the car's digital passport.

Scenario 2

Assume that:

1. Only one driver has SSI credentials and digital car

passport.

2. One or both have black box installed on their car.

3. One does not want to cooperate or even runs away after the accident.

Steps:

In this case the previous steps are carried out by the single person who has SSI credentials and instead of step c) it will be enough to enter the license plate number of the uncooperative driver possibly attaching a photo.

The CID filled in by the individual driver on the app will be published on the blockchain and reported to the company via certified mail. At this point it will be up to the individual company to trace the data of the other driver from the license plate, identify his insurance company and get in touch to establish the true dynamics of the accident, establish whose fault it is and the damage caused by the cars.

Obviously, if the other car has the black box, the process of verifying the dynamics of the accident is much simplified! Therefore, the time is shortened.

4.4. Digital CID Structure

CID Information with SSI:

1. Date and time
2. Location (GPS, black box)
3. Injuries and authorities involved
4. Material damage to third-party property (optional photo upload)
5. Witnesses –> entry via SSI identification code
6. Insurance policyholder –> SSI
7. Vehicle –> SSI
8. Insurance company –> SSI
9. Driver –> SSI
10. Impact on own vehicle (drawing with clickable impact points)
11. List of visible damages (dropdown list)
12. List of accident circumstances (dropdown list)
13. Accident dynamics (drawing with 2D-3D options/photo/video upload)
14. Observations
15. Signature –> SSI-C (signature, fingerprint, etc.)

As we will see, the required information can be further reduced when items 10, 11, 12, and 13 are replaced with photos, videos, and pre-set responses based on known and listable accident dynamics. Next, we will delve into the dynamics of digital CID completion through a mobile app after an accident occurs.

5. Digital CID Compilation and Blockchain Entry

1. Personal Identification: The first information the application will require is the identity of the user using the app. This can be achieved through existing technologies like IMEI code, biometric factors, or two-factor authentication (2FA).
2. Association and Dialogue Between Individuals and App: The app will ask users to identify who they are filling out the CID with, i.e., the other party involved in the accident. This association can be created between the phones of the involved parties using GPS, NFC, or Bluetooth directly in the app, or by sharing a link if the other party doesn't have the app.
3. Creation of Chat Between Parties: The app then opens a chat where the participants, i.e., those involved in the accident, can fill out the digital CID, updating it with photos, videos, SSI credentials, etc.
4. Cross-Signing for CID Approval and Insurance Reporting: If the CID is completed in mutual agreement, users can digitally sign not only their version of the CID but also the other's. Once signed, these CIDs are automatically sent to the certified mail of the respective insurance companies, thus reporting the incident.
5. Incident Reporting: At this point, the incident is reported to all involved insurance companies. They will hash the received CIDs and record these hashes on the blockchain. Once the incident's dynamics are established, the insurance companies will:
6. Update the digital car passport for the involved vehicles. The digital car passport is managed by the insurance company the car is insured with.
7. Issue Verifiable Credentials (VC) for eligibility for repairs for the vehicle found not at fault.

5.1. Advantages and Disadvantages

Advantages: Avoids errors and delays in standard procedures, allowing quicker CID completion and avoiding traffic congestion. Prevents identity falsification through SSI credentials. Insurance companies are directly involved through the digital CID. Drivers cannot avoid reporting incidents as the black box records any impact. The app ensures incident reports are made to insurance companies, reducing fraud. Blockchain ensures accurate tracking of incidents and damages, preventing fraud. Drivers do not face delays in receiving repair funds and are directed to authorized repair shops.

Disadvantages: The effectiveness depends on at least one party using the technology. Current SSI applications communicate only from the service provider to the user, limiting transaction initiation. Coordination among insurers for a unified app format is challenging. Below is a summary table of the advantages and disadvantages of the proposed solutions:

6. The Project: Architecture

The Digital Vehicle Passport (DVP) will be created and managed through a private blockchain, with the vehicle's insurance company holding control. When a vehicle is first sold, the initial insurance company creates the DVP and inserts it into the blockchain, with visibility restricted to authorized parties. If the vehicle changes ownership and insurance providers, the control over the DVP is transferred to the new insurance company. The blockchain, using Multichain, stores information permanently, allowing only additions and no deletions.

6.1. System Logical Architecture

The system uses a private blockchain with nodes representing insurance companies and possibly a regulatory body.

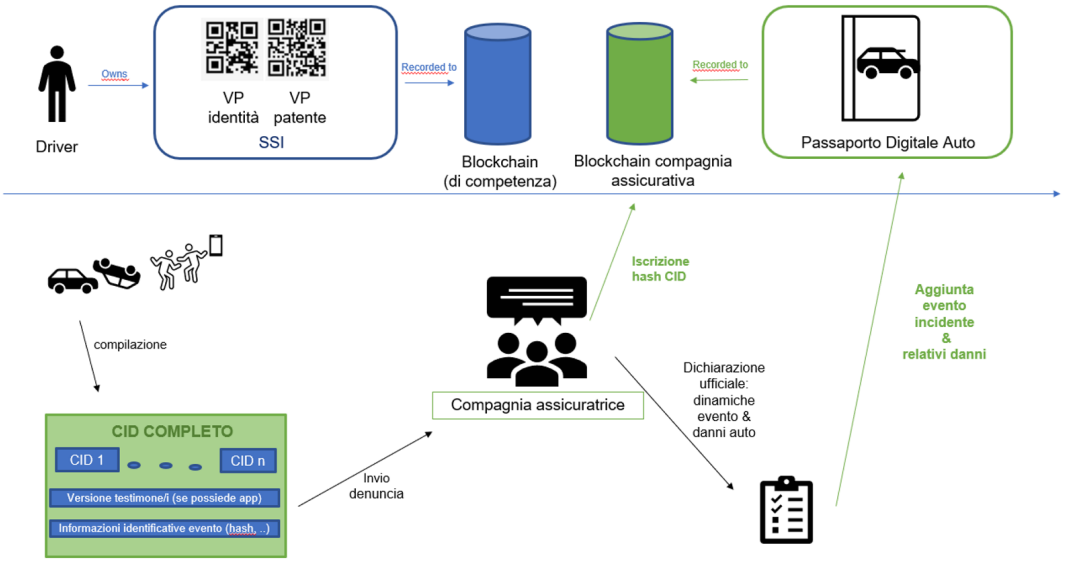

Figure 2: Digital Cid Architecture

Table 2
Summary table of the advantages and disadvantages of the proposed solutions

SCENARIOS	A	B-1	B-2
You can lie about the identity of the driver	yes	no	both
The entitled party always gets compensation, even if the two drivers do not cooperate	no	yes	yes
Both drivers are advised to fill in the CID after the accident.	no	yes	yes
The process of filling in the CID and reporting to the insurance company is quick and easy	no	yes	yes
You can lie about the car's past history, accidents, mileage, etc.	yes	no	yes
You can use the money received from the insurance company for purposes other than repairing the car	yes	no	no
If you are entitled to compensation, your car can be repaired quickly and by an authorised workshop without any possibility of fraud.	no	yes	yes
The police are also often involved in non-serious accidents	yes	no	no

In the case of an accident, the insurance company of the involved driver records the incident on the blockchain and notifies the other involved insurance company. The key transactions are:

TRANSACTION 0A: The driver reports the accident. TRANSACTION 1A-B: Insurance company A notifies insurance company B about the accident. TRANSACTION 2B: Insurance company B verifies the data and confirms or denies the accident. TRANSACTION 4: Consultation of the vehicle's history.

6.2. The Project Implementation: Blockchain Initialization and Granting Permissions

The private blockchain, named PDAChain1, is created and initialized on one node (Node1), with the node address shared with a second node (Node2). Node1 grants Node2 permission to connect and interact with the blockchain.

6.3. The Project Implementation:TRX 1A-B Accident Notification via Monetary Transaction

Node1 sends 10 PDACoin to Node2 to notify about the accident. Node2 confirms the accident by sending 1 PDACoin or denies it with 0 PDACoin.

6.4. The Project Implementation: TRX 2B-A: Accident Confirmation

Insurance company B verifies the data externally and confirms the accident by sending 1 PDACoin to Node1.

6.5. The Project Implementation:Stream Creation for TRX 3A Update PDA

A stream is created to record the accident. Both nodes publish JSON data with details of the accident for the respective involved vehicles in the stream. Each stream key contains information about the accident and reported damages.

6.6. The Project Implementation: PDA Consultation

Interested parties must request the vehicle's history from the insurance company, which can consult the streams associated with the vehicle's license plate to obtain accident data. Consultation is done through MultiChain commands

that allow searching and viewing streams and associated details.

7. Conclusion

In conclusion, the document proposes a solution to the main issues in pre- and post-accident scenarios, which are often marked by uncertainty about procedures, driver cooperation, and the accuracy and reliability of exchanged information. The Digital Accident Report (DAR) system, leveraging SSI credentials and the Digital Vehicle Passport (DVP), enhances transparency, security, and efficiency. Key benefits include:

1. Transparency of information flow.
2. SSI credentials prevent identity fraud.
3. DAR completion ensures immediate and fraud-proof reporting to insurance companies.
4. The affected party can receive compensation even if drivers do not cooperate.
5. Compensation and vehicle repairs are expedited and fraud-proof.
6. Insurance payouts are restricted to repair purposes using SSI credentials.
7. The DVP eliminates vehicle history fraud.

The success of this project relies on widespread adoption of these technologies, including the DAR app and connected black box, along with SSI credentials. One challenge is the need for high technology adoption and the integration of diverse data systems. Future steps involve insurance companies convincing their clients of the benefits of the DVP and SSI credential. In future works, the artificial intelligence will be applied to optimize the procedure discussed in this paper. In fact, the artificial intelligence has proven to be effective in different contexts but which present problems similar to those addressed in this paper [25, 26, 27].

References

[1] L. Cotugno, F. Mazzenga, A. Vizzarri, R. Giuliano, The major opportunities of blockchain for automotive industry: a review, in: 2021 AEIT International Conference on Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE), IEEE, 2021, pp. 1–6.

[2] E. Iacobelli, V. Ponzi, S. Russo, C. Napoli, Eye-tracking system with low-end hardware: Development and evaluation, Information (Switzerland) 14 (2023). doi:10.3390/info14120644.

[3] I. E. Tibermacine, A. Tibermacine, W. Guettala, C. Napoli, S. Russo, Enhancing sentiment analysis on seed-iv dataset with vision transformers: A comparative study, in: ACM International Conference Proceeding Series, 2023, p. 238 – 246. doi:10.1145/3638985.3639024.

[4] F. Fiani, V. Ponzi, S. Russo, Keeping eyes on the road: Understanding driver attention and its role in safe driving, in: CEUR Workshop Proceedings, volume 3695, 2023, p. 85 – 95.

[5] G. C. Cardarilli, L. Di Nunzio, R. Fazzolari, D. Giardino, M. Re, A. Ricci, S. Spano, An fpga-based multi-agent reinforcement learning timing synchronizer, Computers and Electrical Engineering 99 (2022) 107749.

[6] F. Fiani, S. Russo, C. Napoli, A fully automatic visual attention estimation support system for a safer driving experience, in: CEUR Workshop Proceedings, volume 3695, 2023, p. 40 – 50.

[7] D. Giardino, G. C. Cardarilli, L. Di Nunzio, R. Fazzolari, A. Nannarelli, M. Re, S. Spanò, M-psk demodulator with joint carrier and timing recovery, IEEE Transactions on Circuits and Systems II: Express Briefs 68 (2020) 1912–1916.

[8] F. Fiani, S. Russo, C. Napoli, An advanced solution based on machine learning for remote emdr therapy, Technologies 11 (2023). doi:10.3390/technologies11060172.

[9] G. C. Cardarilli, L. Di Nunzio, R. Fazzolari, M. Panella, M. Re, A. Rosato, S. Span, A parallel hardware implementation for 2-d hierarchical clustering based on fuzzy logic, IEEE Transactions on Circuits and Systems II: Express Briefs 68 (2020) 1428–1432.

[10] N. Brandizzi, A. Fanti, R. Gallotta, S. Russo, L. Iocchi, D. Nardi, C. Napoli, Unsupervised pose estimation by means of an innovative vision transformer, in: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), volume 13589 LNAI, 2023, p. 3 – 20. doi:10.1007/978-3-031-23480-4_1.

[11] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Satoshi Nakamoto (2008).

[12] P. K. Kaushal, A. Bagga, R. Sobti, Evolution of bitcoin and security risk in bitcoin wallets, in: 2017 International Conference on Computer, Communications and Electronics (Comptelix), IEEE, 2017, pp. 172–177.

[13] B. A. Nowak, R. K. Nowicki, M. Woźniak, C. Napoli, Multi-class nearest neighbour classifier for incomplete data handling, in: Lecture Notes in Artificial Intelligence (Subseries of Lecture Notes in Computer Science), volume 9119, 2015, p. 469 – 480. doi:10.1007/978-3-319-19324-3_42.

[14] Wikipedia, Algoritmo rsa, ???? URL: https://en.wikipedia.org/wiki/RSA_(cryptosystem).

[15] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in: 2017 IEEE international congress on big data (BigData congress), Ieee, 2017, pp. 557–564.

[16] R. Giuliano, F. Mazzenga, E. Innocenti, A. Vizzarri, Integration of video and radio technologies for social distancing, IEEE Communications Magazine 59 (2021) 30–35.

[17] M. Woźniak, D. Połap, C. Napoli, E. Tramontana, Graphic object feature extraction system based on cuckoo search algorithm, Expert Systems with Applications 66 (2016) 20 – 31. doi:10.1016/j.eswa.2016.08.068.

[18] M. Wozniak, C. Napoli, E. Tramontana, G. Capizzi, G. Lo Sciuto, R. K. Nowicki, J. T. Starczewski, A multiscale image compressor with rbfnn and discrete wavelet decomposition, in: Proceedings of the International Joint Conference on Neural Networks, volume 2015-September, 2015. doi:10.1109/IJCNN.2015.7280461.

[19] G. Capizzi, G. L. Sciuto, P. Monforte, C. Napoli, Cascade feed forward neural network-based model for air pollutants evaluation of single monitoring stations in urban areas, International Journal of Electronics and Telecommunications 61 (2015) 327 – 332.

doi:10.1515/eletel-2015-0042.

[20] A. Alfarano, G. De Magistris, L. Mongelli, S. Russo, J. Starczewski, C. Napoli, A novel convmixer transformer based architecture for violent behavior detection, in: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), volume 14126 LNAI, 2023, p. 3 – 16. doi:10.1007/978-3-031-42508-0_1.

[21] N. Brandizzi, S. Russo, G. Galati, C. Napoli, Addressing vehicle sharing through behavioral analysis: A solution to user clustering using recency-frequency-monetary and vehicle relocation based on neighborhood splits, Information (Switzerland) 13 (2022). doi:10.3390/info13110511.

[22] N. Genise, B. David, Cryptography review of w3c verifiable credentials data model (vcdm) and decentralized identifiers (dids) standards and cryptography implementation recommendations (2021).

[23] C. Napoli, G. Pappalardo, E. Tramontana, R. K. Nowicki, J. T. Starczewski, M. Woźniak, Toward work groups classification based on probabilistic neural network approach, in: Lecture Notes in Artificial Intelligence (Subseries of Lecture Notes in Computer Science), volume 9119, 2015, p. 79 – 89. doi:10.1007/978-3-319-19324-3_8.

[24] D. Kilroy, A decentralised website login system using 'decentralized identifiers' (2021).

[25] G. Lo Sciuto, G. Capizzi, S. Coco, R. Shikler, Geometric shape optimization of organic solar cells for efficiency enhancement by neural networks, in: Advances on Mechanics, Design Engineering and Manufacturing: Proceedings of the International Joint Conference on Mechanics, Design Engineering & Advanced Manufacturing (JCM 2016), 14-16 September, 2016, Catania, Italy, Springer, 2017, pp. 789–796.

[26] G. Lo Sciuto, G. Capizzi, R. Shikler, C. Napoli, Organic solar cells defects classification by using a new feature extraction algorithm and an ebnn with an innovative pruning algorithm, International Journal of Intelligent Systems 36 (2021) 2443–2464.

[27] G. L. Sciuto, G. Susi, G. Cammarata, G. Capizzi, A spiking neural network-based model for anaerobic digestion process, in: 2016 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM), IEEE, 2016, pp. 996–1003.