IOTPAY: A Decentralized Payment Architecture for Autonomous IoT Transactions

Benoît Maïsseu[1[0009-0006-5261-4647]] and François Chiron[1[0009-0008-7131-1080]]

[1] Werenode SAS, Montigny-le-Bretonneux 78180, France [17]
lncs@springer.com

Abstract. This article introduces IOTPAY, a decentralized autonomous payment system designed to address the growing need for secure, scalable, and low-cost microtransactions in the Internet of Things (IoT) ecosystem. IOTPAY leverages Web3.0 technologies to facilitate trustless, peer-to-peer payments between devices and stakeholders, with applications ranging from EV charging to energy sharing in decentralized communities. The system integrates smart contracts, embedded wallets, a layered public key infrastructure, and user-friendly Web/Mobile interfaces. We detail the system architecture, use cases, and core functionalities, along with ecosystem feedback from stakeholders. The approach is aligned with global sustainability, interoperability, and human-centric principles promoted by the NGI Sargasso initiative.

Keywords: Web3.0, Blockchain, IoT, Decentralized Payments, Smart Contracts, Microtransactions, EV Charging, Energy Communities, Autonomous Systems, Robot Vehicles.

1 Introduction

In the rapidly evolving Internet of Things (IoT) landscape [1] [2] [3], billions of devices increasingly need to autonomously transact value with minimal human intervention. Traditional payment systems, however, are ill-suited for machine-to-machine (M2M) microtransactions due to reliance on intermediaries, high fees, lack of automation, centralization risks and latency [5] [6].

These frictions impede scenarios like smart appliances buying energy or autonomous vehicles paying tolls on the fly. To address these challenges, IOTPAY is proposed as a decentralized, blockchain-based payment solution tailored for IoT devices. By integrating digital wallets directly into IoT endpoints, IOTPAY enables devices to send and receive payments securely, at high speed, and with negligible fees. This approach removes third-party payment processors, thereby reducing costs and delays while improving reliability.

IOTPAY leverages Web3.0 technologies – notably blockchain smart contracts and decentralized identity – to facilitate autonomous M2M payments. Each device in IOTPAY is provisioned with an embedded crypto wallet and a decentralized identifier (DID), allowing it to authenticate and transact without centralized oversight. Smart

contracts are employed to enforce transaction conditions and execute payments automatically once predefined criteria are met (for example, releasing funds only after a service is delivered). By providing a secure, feeless payment infrastructure, IOTPAY aims to unlock new IoT business models where devices routinely trade resources (energy, data, services) in real time.

Indeed, the potential applications span multiple domains. In smart energy networks [11], devices can buy and sell electricity dynamically, optimizing consumption. In supply chain [12] and mobility, connected vehicles [10] or drones can autonomously pay for tolls, parking, or refueling without human involvement.

2 System Architecture

2.1 Overall Design

The IOTPAY system is composed of blockchain-based smart contracts, embedded device wallets, and supporting off-chain infrastructure that together enable trustless, autonomous payments among IoT devices. **Figure 1** illustrates the high-level architecture, highlighting how IoT devices, users, and services interact. At its core, IOTPAY treats each IoT device as an independent economic agent with a cryptographic identity and wallet. This empowers devices to initiate or receive payments directly, without funneling transactions through centralized brokers or cloud platforms.

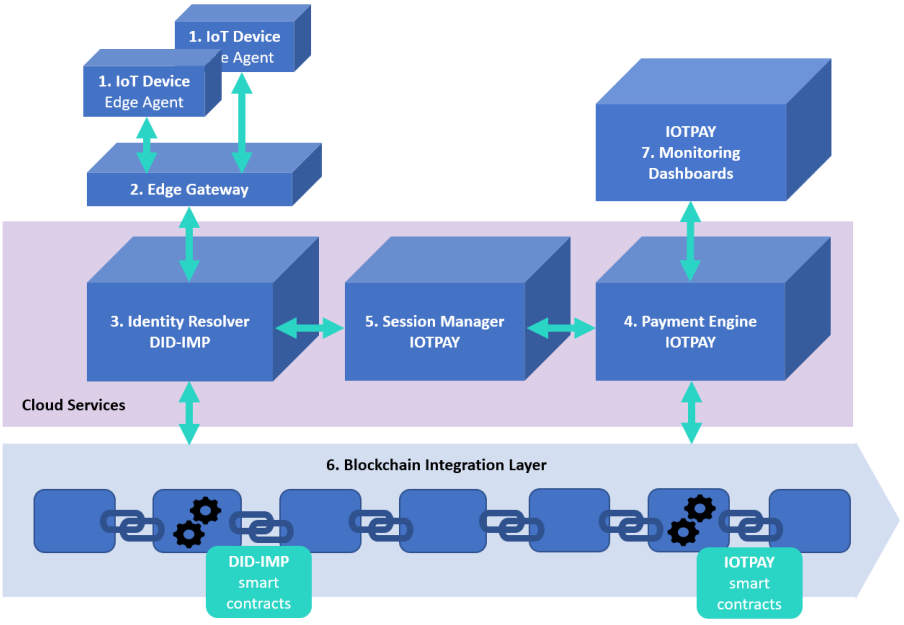

Figure 1- IOTPAY General Architecture

2.2 Key Components

The architecture consists of several functional components working in concert:

- **Embedded Wallets in IoT Devices:** Each device is equipped with an on-board digital wallet (software or secure hardware module) capable of generating cryptographic signatures and managing cryptocurrency or token balances. The wallet allows the device to *store, send, and receive* payments directly on the blockchain network. By integrating the wallet at the edge, devices can participate in transactions without relying on external payment gateways or user phones. This also enables devices to manage their own DIDs and associated credentials, as discussed later
- **Decentralized Public Key Infrastructure (DPKI):** To establish trust in device identities, IOTPAY implements a decentralized PKI tailored for IoT. Each device has a DID registered on-chain. The blockchain consensus serves as the source of truth for identity data, making device identity tamper-resistant and verifiable by any participant. This component ensures that only *authorized devices* can engage in transactions, mitigating spoofing or unauthorized access. This identity and credential layer is inspired by prior work developed within the DID-IMP project [14], which demonstrated the feasibility of trustless authentication and risk-based trust scoring in IoT ecosystems.
- **Smart Contracts (Payment and Credential Contracts):** IOTPAY uses a suite of Ethereum-based smart contracts to automate transactions and credential management. A central Payment Contract encodes the business logic between devices and services. For example, it can hold payment terms (price, conditions) and escrows funds until both a device and service provider fulfill their obligations. Smart contracts ensure that payments execute only when predefined conditions are met, eliminating the need for manual oversight or trusted intermediaries. In addition, an IoT Device Management contract handles creation and revocation of DIDs for devices and actors, and a Signature contract (implementing EIP-712 [15]) standardizes structured transaction signing and verification across heterogeneous wallets. These contracts collectively form IOTPAY's on-chain **Smart Contract Enforcement Layer (SCEL)** that governs device interactions and funds flow.
- **Feeless Transaction Protocol:** A critical requirement for IoT microtransactions is minimizing or eliminating transaction fees, which can otherwise dwarf the payment value. IOTPAY addresses this through a combination of design choices. First, it employs a blockchain network and token optimized for low fees; in our prototype we use an Ethereum-compatible network with batched transactions and sponsor-based fees. A dedicated *Transaction Server* in the architecture aggregates device requests and submits them on-chain in batches to amortize gas costs. Second, IOTPAY's off-chain protocols allow frequent interactions to occur off the main chain, recording only final settlement states on-chain. This approach is inspired by layer-2 scaling and DAG-based ledgers (e.g., Convex's lattice [16]) that achieve near-zero-cost transfers. Third, the execution of the payment transaction can be delegated to a specific account, thus preventing the risk of the IoT device's account running out of gas. By leveraging such techniques, IOTPAY enables *feeless or negligible-cost* payments, making even sub-cent micropayments economically viable. This is a significant improvement over traditional payment rails where fees render small transactions impractical.

- **User Interface Components:** While devices transact autonomously, human users (e.g. device owners or service managers) require interfaces for oversight and configuration. IOTPAY provides a web dashboard and a mobile dApp for users to register devices, configure payment rules, and monitor transactions in real time. Through these interfaces, an IoT devices fleet operator can, for instance, set spending limits for a device or view its payment history. The UI communicates with the smart contracts and off-chain database, presenting a coherent view of on-chain data (balances, credentials, DIDs) and off-chain logs. Robust user control and transparency are crucial to gain stakeholder trust in such autonomous systems.

2.3 Protocol

When an IoT device comes online in IOTPAY, it undergoes an *onboarding process*. The device (or its owner via the UI) generates a DID document containing the device's public keys, which is then registered on-chain. The device's embedded wallet is funded with an initial token balance (or given a channel for payments). To authorize a device to consume a paid service, a user (service manager) can create a **Payment Credential (PC)** via the IOTPAY dApp. This PC is essentially a verifiable credential that links the device, the service, and a payment policy (e.g., "Device X may spend up to 10 tokens on Service Y per day"). The creation of a PC triggers the Payment Contract to record this credential on-chain, optionally co-signed by the service provider for mutual consent. Devices can similarly obtain **Service Credentials (SC)** proving their supplier for a service. Both PCs and SCs are implemented as verifiable credentials anchored on-chain (with hashes or IDs recorded in the contracts for integrity).

Figure 2- IOTPAY Protocol below describes the protocol of operations. Once credentials are in place, an authorized device can initiate a payment transaction to a service device or provider. It does so by signing a transaction (off-chain) containing a reference to the relevant payment credential and the payment amount, then sending it (via the transaction server) to the IOTPAY Payment Contract. The contract verifies the device's signature and credential validity using the DID and credential registries. If the conditions are satisfied (e.g., the credential is valid, not expired or revoked, and the payment amount does not exceed allowed limits), the smart contract transfers the funds to the service provider's account in a *feeless* operation. Thanks to on-chain enforcement, the payment will only succeed if all criteria check out, providing assurances to all parties. IOTPAY thus serves as a trust intermediary replaced by code: it ensures *"autonomous payments happen correctly or not at all,"* which is essential in a machine-driven ecosystem.

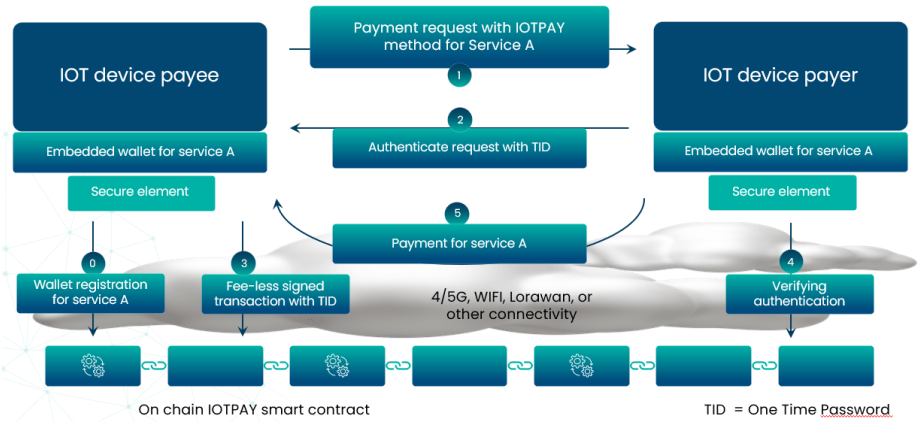

Figure 2- IOTPAY Protocol

Off-chain components complement this flow by handling data that is impractical or too costly to store on-chain. For example, detailed service-level logs, large sensor data related to a transaction, or audit trails are kept in a distributed storage (such as IPFS or a secure database) and referenced by hashes on-chain. This design maintains transparency and verifiability (through hash linking) while keeping blockchain transactions lightweight [7].

3 Security and Enforcement Mechanism

Ensuring security, trust, and compliance is paramount in a decentralized IoT payment system where there is no central authority to mediate disputes or fraud. IOTPAY addresses this through a combination of cryptographic techniques and an automated enforcement.

3.1 Decentralized Identity and Credentials

IOTPAY's use of W3C Decentralized Identifiers and Verifiable Credentials is central to its security model [8] [9]. Every actor (IoT device, service provider, IoT fleet manager) is assigned a DID, which is a globally unique identifier anchored on the blockchain. The benefit is twofold: (1) censorship resistance – no single authority can revoke or fake a device's identity; (2) uniform trust model – any participant can validate a DID's authenticity via blockchain consensus.

Building on DIDs, IOTPAY issues Verifiable Credentials to represent permissions and other claims. A Payment Credential (PC) as described earlier is a type of verifiable credential that authorizes an IoT device to make payments under certain terms. Likewise, a Service Credential proves a device's entitlement to supply a service. These credentials are digitally signed by the issuer (e.g., a fleet manager or service provider) and, when required, co-signed by a counterparty, making them tamper-evident and trustable. The smart contracts serve as **credential verifiers** – upon each transaction, the contract

checks the credential's signatures and status (valid or revoked) before proceeding. Credential revocation is also handled through the blockchain: an issuer can revoke a credential by updating its status in the contract (for example, if a device is compromised or a subscription ends).

One challenge in a decentralized credential system is ensuring *issuers* of credentials remain honest. Since any authorized party can issue a PC or SC to a device (within their domain), there is a risk of mis-issuance or fraud (e.g., a malicious service provider issuing fake service credentials to siphon funds). The DID-IMP platform addresses analogous issues in digital identity by introducing the **DID Risk Assessment Model (DID-RAM)**. DID-RAM continuously monitors credential issuers' behavior (e.g., the rate of credential revocations, anomalies in issuance patterns) and computes a trust score for issuers, combined with anomaly detection to flag possible fraud. If an issuer's trust score falls below a threshold – for instance, an IoT service that is issuing an abnormally high number of credentials in a short time – automated enforcement can be triggered to restrict that issuer. IOTPAY can benefit from a similar model: as a future enhancement, the platform could integrate a reputation scoring mechanism for service providers and device owners [13]. For example, an *IoT service provider* with too many payment disputes or credential revocations could be temporarily blacklisted by the IOTPAY contracts.

3.2 Cryptographic Protocols

All transactions in IOTPAY require cryptographic signing by the initiating device or actor. We adopt the EIP-712 standard [15] for structured data hashing and signing, which prevents certain attacks like transaction replay or parameter tampering by ensuring the signed message explicitly encodes the transaction intent. IOTPAY verifies signatures on-chain, ensuring that only rightful transactions are authorized. This is crucial because IoT devices could be physically accessible to attackers – using strong signatures (with hardware-secured private keys where possible) provides non-repudiation and security even if network traffic is intercepted or the device firmware is compromised.

The privacy of transactions is also considered. By default, IOTPAY uses pseudonymous blockchain accounts for devices (their DIDs are not directly linked to real-world identities on-chain). However, IoT transactions could still potentially be analyzed via public blockchain data. To mitigate this, one could integrate privacy-preserving techniques such as zero-knowledge proofs or the use of privacy-focused sidechains so that, for example, energy trading between two devices does not reveal sensitive business information to competitors. Such additions are outside the initial scope of IOTPAY but are noted as future enhancements to align with privacy requirements.

3.3 Automated Enforcement

The final pillar of IOTPAY's security is the automated enforcement of payment conditions and constraints through smart contracts – essentially encoding the "rules of engagement" that all devices must follow. This includes enforcing rate limits (e.g., a device cannot spend more than X tokens per hour as per its credential), enforcing service-

level checks (e.g., payment is released only if a service confirmation is posted by the provider device), and preventing unauthorized entities from injecting transactions. All these are handled by contract logic, providing a **deterministic, real-time enforcement** of rules that would be difficult to achieve through manual or off-chain means. In IOTPAY, if any rule is violated or a credential is invalid, the contract will reject the transaction and emit an event for logging. Moreover, events from contracts (such as a device exceeding a usage quota) can trigger off-chain alerts via the middleware, notifying stakeholders or other systems to take action (for example, alert an operator or update a device's status in an ERP system). By blending on-chain enforcement with off-chain analytics and notifications, IOTPAY achieves a robust security posture: basic, quantifiable rules are enforced with the finality of blockchain transactions, while more complex analyses (e.g., fraud detection using AI on usage patterns) can be done off-chain and then fed back into on-chain controls.

4 Use Cases and Ecosystem Integration

To demonstrate IOTPAY's capabilities, we consider two representative use case scenarios. Each scenario involves IoT devices performing autonomous transactions in a decentralized fashion, highlighting different aspects of the system.

4.1 Electric Vehicle Battery Swaps

Electric vehicles (EVs) introduce new opportunities for IoT-based payments, particularly with innovative models like battery swapping and decentralized charging. In a **battery swapping** service, instead of waiting to charge, a driver can exchange a depleted battery for a charged one at an automated station. This service involves several IoT devices: the car, the battery and the swapping station. This could be an interesting use case for IOTPAY, making this exchange frictionless and secure.

Once the station confirms that a fresh battery was successfully installed and the old battery is received, it triggers the contract to finalize the payment to the station's account. If something goes wrong (e.g., the new battery fails to activate), the contract can cancel the payment, ensuring the driver isn't charged erroneously. This conditional payment flow is facilitated entirely by smart contracts reacting to IoT signals.

The entire battery swap and payment can be done in minutes. Integrating IOTPAY would allow the payment to happen in parallel with the physical swap, so the moment the new battery is in, the driver can just drive off, with payment settled. The immutability of the blockchain record gives both the station operator and the EV owner a trustworthy receipt of the transaction, which can be useful for audits or warranty claims on the battery.

From a security standpoint, IOTPAY ensures that only authorized swap stations and vehicles transact. The Decentralized PKI prevents a malicious device from impersonating a swap station to siphon payments, and the requirement for station authentication protects the vehicle owner from rogue actors. By using DIDs and VCs, a station proves it is certified by the network. The car verifies this credential on-chain before agreeing to any payment. This mutual authentication builds confidence in the automated system.

4.2 Smart Industry and Autonomous Service Procurement

In Industry 4.0 settings, machines equipped with AI may dynamically procure services from other machines or providers to optimize production. We consider a scenario of a *smart factory* with various IoT devices and services: robotic arms, sensor networks, and third-party service providers offering maintenance or data analytics. Using IOTPAY, these smart devices can **autonomously negotiate and pay for services** to minimize downtime and cost, essentially functioning as economic agents in a machine marketplace.

Imagine a robotic arm on a factory floor that needs a recalibration service. In a traditional setup, it would alert a human manager who then contracts a service. With IOTPAY, the robotic arm (or its controlling AI) can itself detect the need and initiate a search for calibration services listed on an IoT marketplace. Several service providers (perhaps other machines or cloud services, each with their own DID and IOTPAY account) advertise their offerings and prices. The robotic arm's system queries them automatically, maybe using predefined criteria (earliest availability, cost under a threshold, high reputation score). The IOTPAY contract then releases the payment from the robotic arm's wallet to the provider. All of this happens without human intervention, governed by the credentials and contracts set up by the machines themselves.

This *autonomous procurement* is facilitated by IOTPAY's ability to enforce multi-party agreements. If the service wasn't delivered satisfactorily, the robotic arm could contest the payment by not signing a completion confirmation, triggering a dispute resolution workflow (which could be automated or involve a human arbitrator who is another actor in the system). The important point is that routine services can be transacted by machines at machine-speed. This reduces delays — a machine doesn't have to sit idle waiting for a purchase order to be approved manually — and can lead to significant cost savings by optimizing resource use. It aligns with emerging *AIoT (AI + IoT)* paradigms where devices endowed with AI make decisions and interact with other systems intelligently [4].

5 Future Work

Future milestones include the deployment of pilots in the energy and mobility sectors, and deeper integration with advanced cryptographic techniques such as Zero-Knowledge Proofs (ZKPs). A key area of development involves enhancing the Smart Contract Enforcement Layer (SCEL) with comprehensive risk assessment capabilities derived from the DID-IMP platform, previously developed by Werenode as a foundational infrastructure for decentralized identity management. Further research will focus on optimizing transaction validation and batching, implementing complex multi-party transaction workflows, and ensuring alignment with emerging global standards for security and privacy.

6 Conclusion

We presented IOTPAY, a decentralized payment architecture enabling IoT devices to autonomously conduct secure, feeless transactions using blockchain and decentralized identity technologies. IOTPAY's design brings together embedded wallets in devices, DPKI-based identity management, verifiable credentials for permissions, and smart contracts that enforce transaction rules without human intervention. This combination addresses key challenges in IoT commerce: removing costly intermediaries, ensuring trust in a peer-to-peer environment, and handling micropayments efficiently. Through detailed use cases in energy, logistics, EV services, and industrial IoT, we demonstrated how IOTPAY can streamline processes (like a car paying a toll or machines trading services) that are cumbersome today. Each scenario highlighted not only the feasibility but also the tangible benefits – from reduced latency and admin overhead to new capabilities like dynamic service marketplaces for devices.

A recurring theme is the importance of trust and security in a fully decentralized setting. We showed how IOTPAY leverages and extends concepts from decentralized identity management (comparing with the DID-IMP platform) to maintain trust at scale. By using DIDs and VCs, devices can verify each other and the terms of engagement, while the blockchain provides an immutable log and self-enforcing contracts. The security mechanisms, including the proposed risk assessment model for IoT entities, ensure that the system can mitigate misbehavior and adapt to threats, much like analogous systems in the identity domain.

The feedback from initial deployments has been encouraging, confirming that such a system can work in practice and deliver value. It has also kept us grounded in real-world needs – usability, interoperability, and compliance cannot be afterthoughts. As we refine IOTPAY, we are incorporating these lessons: simplifying the user experience, providing governance tools, and adhering to emerging standards. The next steps include scaling up testing, and integrating with other blockchain-based IoT frameworks to leverage synergies. We see a strong synergy with initiatives aiming to create Machine Economic Infrastructures, where protocols like IOTPAY would handle the financial transactions layer while others handle data or communication layers.

Acknowledgments. This project has received funding from the European Union's Horizon Europe research and innovation programme NGI Sargasso (Grant Agreements No. 101092887).

Disclosure of Interests. The authors declare no competing interests.

References

1. "IoT devices 'to generate nearly 80 zettabytes of data' by 2025," 2023. [Online]. Available: https://aro.tech/iot-devices-to-generatenearly-80-zettabytes-of-data-by-2025/

2. "Big Data Market Worth $229.4 Billion by 2025," MarketsandMarkets™, 2020. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/big-data-market-1068.html

3. "Internet of Things (IoT) Market," Allied Market Research™, 2023. [Online]. Available: https://www.alliedmarketresearch.com/internet-of-things-IoT-market/

4. "Artificial Intelligence of Things (AIoT) Market Report," Grand View Research, 2023. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-of-things-aiot-market-report

5. V. Gugueoth, S. Safavat, S. Shetty, and D. Rawat, "A review of IoT security and privacy using decentralized blockchain techniques," *Comput. Sci. Rev.*, vol. 50, p. 100585, 2023. DOI: 10.1016/j.cosrev.2023.100585

6. A. Abdulhamid, S. Kabir, I. Ghafir, and C. Lei, "An Overview of Safety and Security Analysis Frameworks for the Internet of Things," *Electronics*, vol. 12, no. 14, p. 3086, 2023. DOI: 10.3390/electronics12143086

7. Z. Rahman, X. Yi, I. Khalil, and A. Kelarev, "Blockchain for IoT: A Critical Analysis Concerning Performance and Scalability," *arXiv*, 2023. [Online]. Available: https://arxiv.org/abs/2111.11158

8. "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, 2022. [Online]. Available: https://www.w3.org/TR/did-core/

9. "Verifiable Credentials Data Model v2.0," W3C Working Draft, 2024. [Online]. Available: https://www.w3.org/TR/vc-data-model/

10. A. Mykola and A. Anastasiia, "Internet of Things in the Automotive Industry: Solutions for Vehicles, Smart, and Connected Cars," 2023. [Online]. Available: https://www.aimprosoft.com/blog/automotive-iot-usecases-for-cars-vehicles/

11. K. Oliynyk, "How IoT Can Help with Energy Management Systems?" 2024. [Online]. Available: https://webbylab.com/blog/how-iot-can-help-with-energymanagement/

12. M. Baig, D. Sunny, A. Alqahtani, S. Alsubai, A. Binbusayyis, and M. Muzammal, "A Study on the Adoption of Blockchain for IoT Devices in Supply Chain," *Comput. Intell. Neurosci.*, vol. 2022, Art. ID 9228982, 25 pages, 2022. DOI: 10.1155/2022/9228982

13. O. Dogan and H. Karacan, "A Blockchain-Based E-Commerce Reputation System Built with Verifiable Credentials," *IEEE Access*, vol. 11, pp. 47080–47097, 2023.

14. Zhdarkin, E., Chiron, F., Maïsseu, B.: DID-IMP: Decentralized Public Key Infrastructure for Defended IoT Data Management and Procurement. Werenode SAS, 2025.

15. Reitwiessner, C., Remor, R., Johnson, N.: *EIP-712: Ethereum Typed Structured Data Hashing and Signing* (2017). Ethereum Improvement Proposals. Available : https://eips.ethereum.org/EIPS/eip-712

16. Convex Team. (2024). *Convex: An Open Decentralised Platform for the Internet of Value*. Available : https://raw.githubusercontent.com/Convex-Dev/design/main/papers/convex-whitepaper.pdf

17. Werenode SAS.: Werenode - Decentralized EV Charging and Energy Community Solutions. Available online: https://werenode.com