BlockBaRT: Towards a Blockchain-based Battery Passport with Selective Disclosure of Verifiable Data

Julian Kanjere
Centre for Robotics and Future Production
Council for Scientific and Industrial Research
Pretoria, South Africa
jkanjere@csir.co.za

Merryl Ford
Centre for Robotics and Future Production
Council for Scientific and Industrial Research
Pretoria, South Africa
mford@csir.co.za

Murray Louw
Centre for Robotics and Future Production
Council for Scientific and Industrial Research
Pretoria, South Africa
mlouw2@csir.co.za

***Abstract*— The market for electric vehicles (EVs) is surging as automakers move towards decarbonisation, and consumer preferences towards environmentally friendly vehicles. In addition, technological advances are making EV production and operation cheaper, and EV performance comparable with that of traditional internal combustion engines. One of the core components of an EV is the lithium-ion battery, which has a multi-stakeholder and often siloed value chain. Given the nature of the EV battery supply chain, visibility into the end-to-end lifecycle of a battery is opaque. To address this limited visibility and the automotive decarbonisation agenda, governments are introducing battery passport legislation for the collection and sharing of EV battery-related data, throughout its lifetime, among supply chain actors.**

Drawing from available regulation and policy on EV battery passports, and literature on the use of blockchain and self-sovereign identity (SSI) to provide verifiable trust registries, we design and implement a blockchain-based Battery Registration and Tracking passport - BlockBaRT. BlockBaRT is a proof-of-concept EV battery lifecycle management system that allows registration of an EV battery at manufacture and selective disclosure of blockchain-verified data to a requestor (e.g. a government regulator) when in operation. BlockBaRT demonstrates the feasibility of combining a public blockchain together with SSI-inspired selective disclosure of product data for implementation of a battery passport. This lays the foundation for future advancements in EV battery information sharing, and lifecycle management based on this hybrid approach.

Keywords*— *battery passport, blockchain, selective disclosure, electric vehicle, battery lifecycle management

I. Introduction

The market for electric vehicles (EVs) is experiencing rapid growth, owing to environmental benefits from reduced emissions and noise pollution; technological advancements which make battery technology more efficient and production of EVs cheaper; cheaper operational costs of EVs compared to those of internal combustion engine vehicles; government policies and incentives to promote EV production and use; and shifting consumer preferences. The most important component of an EV is arguably the lithium-ion battery as it is the energy source.

However, visibility into the sourcing of raw materials, production, operation and end-of-life repurposing of EV batteries is limited – given the numerous stakeholders involved (and the resulting information silos), coupled with a lack of established production regulation and reporting requirements for this emerging sector, and the “notorious secretiveness” of the automotive industry [1]. This results in missed opportunities of data collection and sharing for policy making, optimization of EV battery manufacture, operation and ecosystems, and ensuring sustainable practices.

In response to this, governments across the world are beginning to mandate legislation for the collection and sharing of EV battery-related data among supply chain actors. To this end, blockchain technology has emerged as a potential solution for tracking and traceability of EV battery lifecycle data, from production, operation and end-of-life recycling, owing to its single source of truth and data integrity properties. The use of blockchain in this context is commonly referred to as a battery passport – a type of product passport.

There are two prevalent approaches to product passports and EV battery tracking, namely the use of self-sovereign identity (SSI) for issuance of decentralized identifiers (DIDs) and verifiable credentials, and the use of blockchain for decentralized and immutable data sharing. Whilst the former is privacy-preserving, it requires adherence to the same verifiable credential standards for interoperability and use of dedicated mobile applications as wallets. On the other hand, the use of blockchain technology for immutable EV battery data storage and sharing does not require use of specialised mobile wallet applications and adherence to the same verifiable credential standards for all supply chain stakeholder. That said, the blockchain typically used is a private or consortium based one, which requires infrastructure maintenance and coordination amongst the involved stakeholders; and if a public blockchain is used, there is then a lack of data privacy as the on-chain data, if stored in plain text, is available for all to see.

A. Objectives

The research objectives for this study are as follows:

1. **RO1** – Implement blockchain-based registration of a battery at manufacture.
2. **RO2** – Implement selective and privacy-preserving disclosure of granular-level blockchain-verified battery data.

B. Contribution

To address the gaps with existing the existing approaches for EV battery asset tracking - data collection, visibility and selective-sharing, we develop a proof-of-concept (POC) Blockchain-based Battery Registration and Tracking web application - BlockBaRT. BlockBaRT enables EV battery registration; and selective, privacy-preserving disclosure of attribute level battery data. The BlockBaRT POC showcases how leveraging blockchain technology, cryptographic techniques (hashing), and principles from both zero-knowledge proof (ZKP) techniques and SSI for verifiable data exchange, can address limitations in, and enhance asset tracking. This results in a decentralized and privacy-first approach to electric vehicle (EV) battery lifecycle management which may result in easier adoption of these technologies in emerging economies.

C. Paper Organisation

The rest of the paper is organised as follows: Section 2 introduces the background and motivation for the work; Section 3 and 4 details the design and implementation of the BlockBaRT battery passport platform, respectively; Section 5 evaluates the BlockBaRT solution; Section 6 discusses how BlockBaRT works and lists recommendations for future work; and Section 7 summarises our work.

II. BACKGROUND

A. Electronic Vehicles and Batteries

Demand for EVs is growing across the world, and the automotive industry is undergoing a shift from an internal combustion engine (ICE) based market to one that includes EVs [2]. This is due to several factors which include technological advancements that are making battery technology more efficient and production of EVs cheaper; cheaper operational costs of EVs compared to ICE vehicles; favourable government policies and incentives to promote EV production and use; and shifting consumer preferences towards more environmentally friendly, efficient and technology-enabled mobility solutions [3].

At the heart of an EV is the EV battery, a lithium-ion battery whose cost accounts for approximately 1/3 of the price of the EV [4]. Given that EV batteries gradually lose their efficiency and storage capacity over time, EV Original Equipment Manufacturer (OEM) typically suggest EV battery replacement when its capacity is reduced to about 70–80% of its rated capacity [2]. To reuse or recycle an EV battery, manufacturers need to refurbish the battery for other uses in a second life, which often is stationary storage [5]. The life of an EV battery, from the perspective of a circular economy (CE) value chain is comprised of multiple processes and stakeholders, from raw material sourcing, cell and battery pack manufacturing, EV battery manufacture, EV usage, EV battery end-of-life (EoL), collection of EV batteries, and recycle / reuse / disposal [1] [3]. However, one of the fundamental limiting factors to advancing the CE for EV batteries is insufficient data sharing along the value chain [1], which digital product passports (DPP), and more specifically digital battery passports (DBP) can remedy.

B. Digital Product Passports and Digital Battery Passports

DPPs are systems that contain detailed information on a product's provenance, use and EoL instructions [35]. DPPs are predicated on unique product identifiers and serve as a useful source of value chain life cycle data for value chain stakeholders and the CE efforts [6] [7]. DPPs are part of the "Circular Economy Action Plan" and promoted by the European Commission as a system of potential data-driven CE solutions, that are at the intersection of CE and digital technologies [8]. The primary objective of DPPs is the initiation and maintenance of communication among stakeholders, in the form of logs, containing relative information on materials and components used in products and services [9]. Put another way, DPPs are systems that enable asset tracking, which is the process of tracking a product or batch of products as they move in a value chain, with the goal of ensuring custodianship and modifications are noted for information sharing, audit trail and quality purposes [10].

DBPs are a specific type of DPP, specific to EV batteries, their identifier, and comprised of data that includes the make, composition, and operation, and the different data views accessible by different supply chain stakeholders, including regulators, supervisors, and consumers [11]. DBP has four main data categories, namely: (i) sustainability and circularity data; (ii) diagnostics, maintenance and performance data – which includes battery health, maintenance history and delivered performance; (iii) value chain data (general information and chain of custody); and (iv) battery specific information [7]. [12] suggest that DBP general information that should be publicly available to all stakeholders includes information on the manufacturer, the battery category, its capacity, material composition (such as hazardous substances and critical raw materials), carbon footprint declaration, responsible materials sourcing data, recycled content and share of renewables, management of waste batteries.

DBP initiatives have gained the most traction in the European market, either via consortia or commercial offerings. Examples of DBP consortia initiatives include the Global Battery Alliance [13] and German Battery Pass [14], and commercial offerings include Minespider [15], Circulor [16] and iPoint [17].

C. Blockchain and Data Sharing in Value Chains

Blockchain technology is often associated with asset tracking, and as noted by Organisation for Economic Co-operation and Development (OECD) Workshop on International Trade and Circular Economy [18], combining blockchain technology and DPPs may create pathways towards improved data, transparency and traceability of products, and in the process enable circular value chains globally.

Blockchain is a decentralized, peer-to-peer network, with a shared append-only (immutable) ledger, that contains securely recorded and timestamped transactions [19]. It makes use of asymmetric encryption to issue transactions that are recorded onto the blockchains state. Out of the box, transactions on blockchain networks are partially private using pseudonymous identities (addresses) between a sender and a receiver. However, in practice, this quasi-privacy falls away as any time two users transact as they each learn of the other's address.

Blockchain networks can be public or private. The former is open to anyone to participate in the network and maintain the state of the ledger, whilst the latter requires participants to be invited by the network starter (a central authority) who is also responsible for managing the ledger or setting its management rules. An example of a public blockchain is the Algorand Blockchain [20]. Similarly, an example of a private blockchain is the Hyperledger Fabric [38]. The downside with public blockchains is that they are open and therefore do not offer privacy for transactions, besides the pseudonymous identities of participants. That said, public blockchains have potential use in trustless, privacy-preserving and data provenance applications due to their native use of asymmetric cryptography and their distributed nature with no central authority [21] [22].

According to [23], blockchain architectures and protocols offer almost real-time decentralized sharing of information across organizations in mutually distrusting environments (e.g. automotive value chains). They also provide mechanisms in which the veracity of data can be trusted, and they create an immutable audit trail [19]. This positions blockchain as a foundational information sharing layer for DBPs, on top of which, other privacy-preserving technologies can be incorporated.

D. Data Sharing and Privacy-preserving Technologies

According to [29], privacy-enhancing technologies (PETs) are becoming increasingly foundational for fostering trust in data sharing and re-use. PETs are a system of ICT measures protecting informational privacy by eliminating or minimising unnecessary data disclosures without sacrificing utility in an information system [30]. In this section, we introduce PETs such as ZKPs and (SSI).

According to [19], blockchain reduces the cost of state verification, interoperability and programmability. Blockchains enable multiple distributed agents to network with each other using pseudonymous identities, at reduced cost, whilst retaining custody of their private keys and maintaining provenance of transactions. Based on this capability, blockchain networks have the potential to be used as a base layer for privacy-preserving network applications, particularly when combined with cryptographic techniques such as hashing and ZKPs to enhance the privacy of transactions.

SSI asserts that individuals should have control over their own identities and how attributes relating to their identity are shared with others [26]. DID is an embodiment of SSI in which identifiers, such as usernames, can be replaced with IDs that are self-owned, independent, and enable data exchange using blockchain technology to protect privacy and secure transactions [24]. ZKPs on the other hand use cryptographic algorithms that enable a prover to mathematically demonstrate to a verifier that a statement is correct without revealing any data [25]. For example, an individual could prove they are over a minimum age limit to a requestor without revealing their actual age.

One approach to DBPs is using SSI, and the issuance of verifiable credentials for key battery data and events, for which an interested third-party can request attributes, and the battery owner can respond with a verifiable presentation [33]. The advantage with this approach is that there is inherent privacy preservation as only the requested information is presented, should the battery owner oblige. The challenge with this is the need to adopt SSI infrastructure and make use of SSI wallets which are typically in the form of a mobile application. In addition, there is a need for adherence to verifiable credential standards (e.g. W3C).

Another approach to battery tracking is using blockchain technology. This involves registering all EV battery data and events on the blockchain – this could be in plaintext, in hashed form or as a non-fungible token (NFT). An additional consideration when using the blockchain approach is whether to make use of a public blockchain, in which case the data is visible for all to see and therefore leaking unnecessary information, or a private blockchain which comes with the overhead of managing the network infrastructure.

BlockBaRT makes use of the latter approach, utilising a public blockchain, hashed data and selective disclosure of battery attributes using SSI-like principles. The selective disclosure is realised by allowing an EV battery data owner chooses to accept or decline an attribute-level data sharing request, and in the case of accepting, the resultant data shared may be a plaintext value or a Boolean response to an assertion.

III. DESIGN STRATEGY

A. BlockBaRT Overview

Recall that according to [7], a battery passport must have four key data points: (i) sustainability and circularity data; (ii) diagnostics, maintenance and performance (battery health, maintenance history and delivered performance); (iii) value chain data (general info and chain of custody); and (iv) battery specific information (manufacture metadata). For the BlockBaRT PoC, we initially consider the battery specific information, and the sustainability data. In addition, [9] posit three different data tiers for a digital product passport, namely: (i) Data Collection – IoT and digital twins; (ii) Data Curation and Sharing – artificial intelligence/machine learning, and data exchange protocols); and (iii) Data Leverage – information sharing via blockchain and data lakes. For the BlockBaRT design and implementation we focus on the Data Leverage via blockchain tier – which allows secure information sharing. The Data Collection is via forms, and the Data sharing utilises standard HTTP protocol.

The objective of BlockBaRT is to allow registration of an EV battery by an owner – typically the manufacturer – and allow privacy-preserving information exchanges of granular / attribute level battery information. The primary entities are the manufacturer and any value chain entity with an interest in this data, with a workflow that consists of registering an EV battery by the manufacturer, a request for EV battery attribute specific data from a value chain stakeholder, a response to the request by the EV battery manufacturer, and completes with the requestor viewing the information requested (if approved by the manufacturer). This is shown in Figure 1.

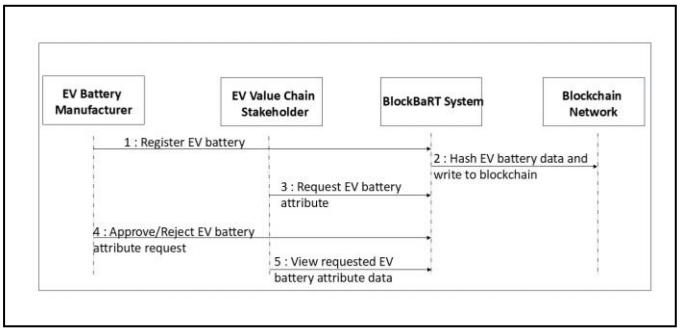

Fig. 1. Illustration of the BlockBaRT platform workflow (i) battery registration by the manufacturer; (ii) storage of the data on the blockchain; (iii) request for attribute specific data from a value chain stakeholder; (iv) response to the information request by the battery manufacturer; and (v) selective disclosure of the requested information if approved by the manufacturer.

B. Functional Requirements

Based on the BlockBaRT workflow, we derive the following functional requirements (FR) for the POC:

- **FR1** – Authenticate EV battery stakeholders – a battery manufacturer and other value chain stakeholders.
- **FR2** - Register a new battery with the battery specific metadata and sustainability information available at time of manufacture.
- **FR3** – Generate a unique identifier for the battery.
- **FR4** – Allow a value chain stakeholder to request attribute-level battery information from a battery owner (outgoing information request for a specific attribute).
- **FR5** – Allow a battery owner to respond (accept or reject) to an attribute-level battery information request (incoming information request).
- **FR6** – Display approved battery information in a privacy-preserving manner.

IV. IMPLEMENTATION

A. *BlockBaRT Architecture*

BlockBaRT is a web application, accessible to registered EV-battery value chain users, providing a structured interface for managing battery data. Users will navigate through dedicated pages for key functionalities, including authentication, viewing and creating battery records, requesting information from other users, and responding to incoming data requests.

The BlockBaRT high-level system architecture is illustrated in Figure 2. Client web browsers connect to the backend server, which in turn connects to the blockchain infrastructure over a network. Docker compose is used to deploy separate containers that run the backend business logic and to host the database. Furthermore, several other backend components run within the backend container and communicate with other components over the local network.

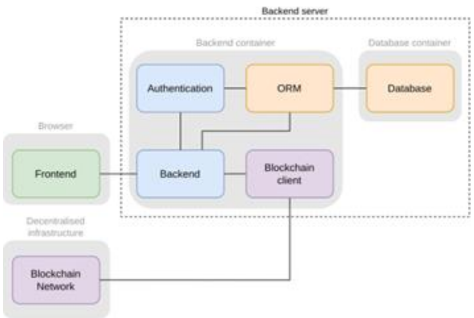

Fig. 2. High-level architecture diagram for the BlockBaRT platform, which allows registration of EV-batteries and privacy-preserving sharing of attribute-level battery data.

B. *System Features*

The BlockBaRT features are described below:

- **Authentication**. BlockBaRT makes use of username and password authentication. All pages except the home page are accessed by an authenticated user. The home page displays information about the application to all visitors and logged in users. An initial home page is display in the figure below. All other pages can be accessed from the navigation header which is presented on every page in the web application. However, these pages will redirect a visitor to the login screen if not yet logged in. See Figure 3.

Fig. 3. BlockBaRT home page.

The login screen is shown to visitors that are not yet logged in. Their email address and password can be used to login as expected. See Figure 4.

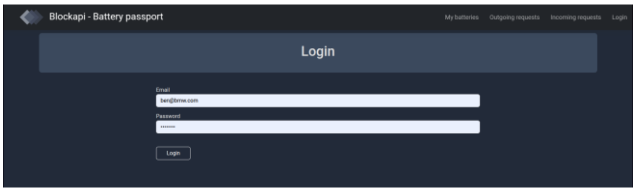

Fig. 4. BlockBaRT login.

After logging in, the user's email address will be displayed to them to indicate which account is currently active, as shown in the Figure 5. A logout button is also present for logged in users. This feature satisfies requirement **FR1**.

Fig. 5. BlockBaRT logged-in user identification.

- **Create New Battery**. The "Create new battery" button redirects users to a dedicated page for entering battery details, as shown in Figure 6. The data points required for a new battery registration are Serial Number, Model, Manufacturer, Manufacture Date, Percentage Recycled Materials, Number of Cells, Ethical Sourcing Score, Power Rating (W) and Energy Capacity (Wh).

  Upon submission, the form sends an HTTP POST request to trigger authentication, blockchain registration, and database record creation on the backend. All batteries are uniquely identified by an SSI-like decentralized identifier (DID). This is generated for each battery on the backend. This POST endpoint also functions as an API, enabling automated systems to generate new battery records or log lifecycle events programmatically.

Fig. 6. BlockBaRT create new battery.

When the battery creation request is received on the backend, the data is sent to the BlockAPI BaaS platform [27] which hashes and writes the data to the Algorand blockchain while the user waits for the transaction to complete, as shown in the Figure 7. The payload hash and blockchain transaction ID is then returned from the BlockAPI BaaS and stored in a database along with the battery data. After the transaction completes, the user is redirected to the pages that displays the battery information table. This feature satisfies requirements **FR2** and **FR3**.

Fig. 7. BlockBaRT create new battery – blockchain transaction pending view.

- **View Batteries**. As shown in Figure 8, a table is displayed with information about all batteries that belong to the current user. A column is included with a blockchain transaction ID that can be used to verify the information on the Algorand blockchain. A button is also displayed that redirects the user to a page to create a record for a new battery. This feature satisfies requirements **FR2** and **FR3**.

Fig. 8. BlockBaRT my batteries view.

- **Create Outgoing Request**. A “Create new information request” button on the outgoing requests page redirects the user to a form for submitting a new request. Each request is linked to a specific unique identifier that identifies the battery. A drop-down list allows the user to specify a data field to request information about, for example, the manufacturer, battery capacity, or ethical sourcing score. Depending on the field type, the request can be for a ZKP of equality, inequality, or the full value. The form submits a POST request, allowing automated systems to use the same API. Figure 9 shows the page used to submit a request. In this example, the ben@bmw.com user is making a request about a battery unique identifier managed by the rosendo@honda.com user. This feature satisfies requirements **FR4**.

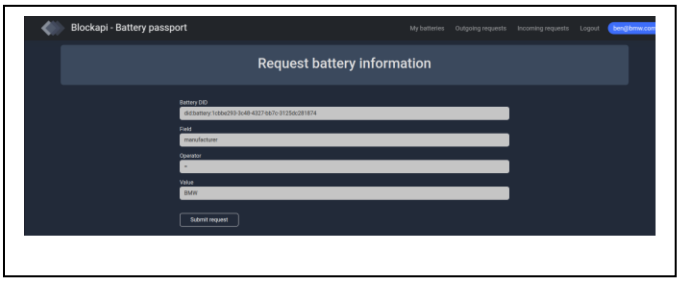

Fig. 9. BlockBaRT request battery information (outgoing request) view.

- **View Outgoing Requests**. An information exchange begins with a user creating an outgoing request, which the receiving user processes and responds to as an incoming request. A table on the page shown below displays the user's outgoing requests, including a status column indicating whether each request was granted or rejected. Another column details the information disclosed through the ZKP, whether it confirms an equality/inequality condition or reveals the full requested value. See Figure 10. This feature satisfies requirements **FR4** and **FR6**.

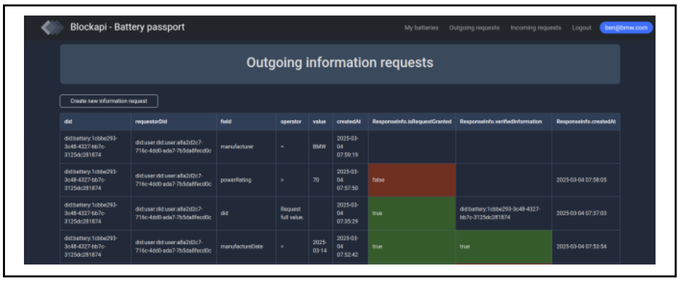

Fig. 10. BlockBaRT outgoing information requests view.

- **View Incoming Requests**. The incoming requests page, shown in Figure 11, allows the user to view requests about batteries owned by the current user. In this example the rosendo@honda.com is view information requests created by ben@bmw.com. The table on this page shows a history incoming requests and corresponding responses. The action column allows the user to approve or reject a request for information, which triggers the corresponding action on the backend to respond to the requesting user. This feature satisfies requirement **FR5.**

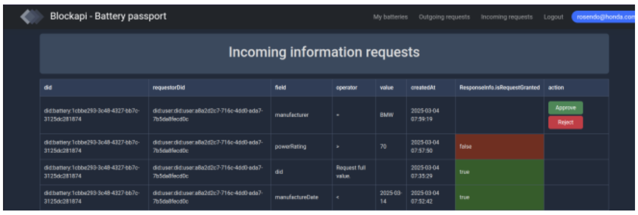

Fig. 11. BlockBaRT incoming information requests view.

V. EVALUATION

A. Simulation

To verify that BlockBaRT works as expected, we conduct a simulation with two users, (i) a battery manufacturer – rosendo@honda.com; and (ii) a value chain stakeholder - ben@bmw.com. The simulation is conducted on a server with the following specifications: *Ubuntu 22.04, 11th Gen Intel(R) Core(TM) i9-11950H @ 2.60GHz* and *32 GB RAM.*

The steps are as follows:

- **Battery manufacturer registers EV battery**. Battery manufacturer – rosendo@honda.com registers a battery with the following data: *Serial Number: FGH345TYH, Model: Bobson 2, Manufacturer: BMW, Manufacture Date: 27/01/2025, Percentage Recycled Materials - 34, Number of Cells: 24, Ethical Sourcing Score:95, Power Rating (W): 50000 and Energy Capacity (Wh): 120000*. The battery is successfully created with unique ID: *did:battery:1cbbe293-3c48-4327-bb7c-3125dc281874.* See Figure 6 and Figure 7.

- **Value chain stakeholder creates outgoing information request**. Value chain stakeholder - ben@bmw.com logs in and creates an outgoing information request - Requests to see whether the battery manufacturer = BMW. See Figure 12, which is extracted from Figure 10.

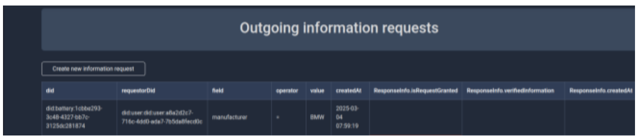

Fig. 12. Request by value chain stakeholder to see whether the battery manufacturer is BMW.

- **Battery manufacturer responds to incoming information request**. Battery manufacturer – rosendo@honda.com logs in, views the incoming information requests, and can approve or deny the request from the value chain stakeholder - ben@bmw.com. See Figure 13, which is extracted from Figure 11.

Fig. 13. Battery manufacturer can approve or reject the information request from the value chain stakeholder to see whether the battery manufacturer is BMW.

- **Value chain stakeholder views selective disclosure responses to outgoing information requests**. Refer to Figure 10 where value chain stakeholder - ben@bmw.com can see previous requests that have been approved including the request to the see the battery identifier in plaintext, and whether the battery manufacture date is before 14/03/2025 – the response is in the *Response.verifiedInformation* column.

B. BlockBaRT Test Cases

In addition to the simulation, the tests shown in Table 1 are carried out on the BlockBaRT system. All the test cases pass.

TABLE I. BLOCKBART TEST CASES

Test Category	**Test Case Detail**		
	Test case description	***Expected result***	***Pass / Fail?***
Authentication	Login by EV battery manufacturer.	EV battery manufacturer can login and access their profile.	Pass
	Login by EV battery value chain stakeholder.	EV battery value chain stakeholder can login and access their profile.	Pass
EV battery registration	EV battery registration by manufacturer. Register battery and create record on the blockchain.	EV battery created and corresponding entry on the blockchain.	Pass
	Generate unique identifier for EV battery by system.	Unique identifier created for battery.	Pass
EV battery information request	Request battery attribute information request by EV value chain stakeholder.	Outgoing information request created.	Pass
	Respond to request for battery attribute information by EV battery manufacturer.	Incoming information request approved or rejected.	Pass
	Display battery information attribute with appropriate privacy based on the request. Response to information request either displays a Boolean result (true / false) or the full plaintext value.	Information requestor can see information if the request is granted.	Pass

C. Overview of Digital Product Passport Solutions

Table 2 provides an overview of various DPP solutions – which are either purely blockchain-based, or a hybrid of decentralized identity and blockchain-based.

TABLE II. OVERVIEW OF DIGITAL PRODUCT PASSPORT IMPLEMENTATIONS

Study	*Key Contribution*	*Gap Addressed*
P. Emmenegger [34]	PermaPass implementation based on a React-native mobile app, Ethereum smart contracts for managing product identifiers, and QR codes and NFTS for accessing product passport data.	Use of NFTs and smart contract based decentralized identifiers to create a product passport, accessible via a mobile phone. Uses QR codes and NFC chips as data carriers.
M. Hulea et al. [35]	Digital product passport using multi-blockchain approach and decentralized identifier provider.	Product passport using the Hyperledger Fabric blockchain (consortium based) and product identities managed via an external decentralized identifier platform (cheqd.io).
H. Abreu et al. [36]	Blockchain-based DPP based on the Hyperledger Fabric blockchain, without any decentralized identifiers.	A pure-blockchain-based DPP on a consortium blockchain – Hyperledger Fabric.
L. Navarro et al. [37]	DPP system that utilises Ethereum smart contracts accessible via a REST API to register devices; register and verify proofs; generate and verify DPPs; generate and verify verifiable reports;	Verifiable registry using decentralized identifiers, a permissioned blockchain and Ethereum smart contracts. Supported on Ethereum and IOTA blockchain.
BlockBaRT	Blockchain-based DBP with SSI-inspired selective disclosure of verifiable data.	An EV battery DPP based on a public blockchain (Algorand), with privacy-preservation and selective disclosure of EV battery attributes.

The purely blockchain-based solutions are based on private blockchain networks or permissioned / consortium based blockchain networks e.g. Hyperledger Fabric. The use of a consortium blockchain is to alleviate concerns with data privacy that are otherwise associated with public blockchains. The hybrid solutions which make use of SSI and blockchain technology typically make use of Ethereum smart contracts or external providers (e.g. cheqd.io) for the decentralized identifier component and do not implement a custom mobile wallet solution to store the credentials. This speaks to the complexity with pure SSI-based solutions.

BlockBaRT is different from these existing implementations as it makes use of a public blockchain, but with privacy considerations as the data is hashed before writing to the blockchain. In addition, whilst it does not make use of decentralized identifiers, the ability for an information requestor to request specific attribute information and the ability of an EV battery custodian to respond provides the SSI-inspired selective disclosure of data. In its current form, to access data about a battery, an information requester needs to have the unique battery identifier, which can in future be encoded as a QR code, which is the data carrier mechanism used in [34] and [37]. Further, BlockBaRT is accessible via a web browser and not a mobile application, for ease of access.

VI. DISCUSSION

A. Final Remarks

Recall that the research objectives for this study are as follows:

1. **RO1** – Implement blockchain-based registration of a battery at manufacture.

2. **RO2** – Implement selective and privacy-preserving disclosure of granular-level blockchain-verified battery data.

In Chapter 4 and 5, we have demonstrated how BlockBaRT enables registration of an EV battery by a manufacturer, and subsequent attribute-level information requests by EV value chain stakeholders to the EV battery manufacturer, which can be approved or rejected.

The blockchain based registration of the battery is via the BlockAPI BaaS platform [27] which abstracts the blockchain integration by means of a REST API interface that writes to the public Algorand blockchain, satisfying **RO1**.

Further, the selective disclosure/ZKP aspect of the system is achieved by only allowing requests for a single attribute value, - either the full requested value, or a Boolean response - for which the data owner must approve or reject the request. The mechanism for a data owner to approve or reject a information request is based on SSI principles. In addition, this data is cross-checked on the blockchain before being returned to the requestor, which provides the verification aspect. This satisfies **RO2**.

DBPs provide a traceability tool for every stakeholder in the battery supply chain, ensuring that custodianship, and modifications are noted for audit trail and quality purposes [10]. Therefore, with enhanced traceability, the use of a system such as BlockBaRT is key to not only providing more visibility into the EV battery supply chain, but a mechanism for tracing batteries and also identifying fake batteries before owners of EVs can even buy them, as they will not be found in the blockchain-based battery registry - assuming that only authentic EV batteries are captured on the system. The increased visibility and traceability capability is of benefit, both to the consumers and to ensure the competitiveness of local industry manufacturing the EV batteries.

However, it must be mentioned though, that the success or failure of adopting DBPs is based on the willingness of the OEMs to subscribe to them, which is anticipated to be a challenge given the previously alluded to siloed nature of automotive value chains. OEMs are also known to be hesitant to invest in technology where the benefit is realised by other OEMs who have not invested the same. To this end, policy makers in emerging economies need to prioritise policy development and enforcement, firstly for production and adoption of EVs, followed by the corresponding process changes, one of which being EV battery tracking [31]. In addition, government can offer supply side incentives to

OEMs that adopt these technologies (e.g. tax rebates), as this contributes towards decarbonisation efforts for the automotive industry [32].

BlockBaRT validates the feasibility of a decentralized, privacy-preserving asset tracking application on a public blockchain, with selective disclosure of battery attribute data. The BlockBaRT implementation removes the need for downloading of mobile applications / credential wallets and the setup of private blockchain infrastructure. This hybrid approach makes adoption of DBP technology easier – especially in emerging economies, as it becomes cheaper to adopt and supply chain stakeholders only need to access this via a web application, a process they are already familiar with.

Lastly, the BlockBaRT implementation can be modified with minor changes to serve as a generic asset tracking application.

B. Limitations

BlockBaRT has been restricted to only record and provide information captured at the time of manufacture – the battery information and sustainability information to simplify development and demonstrate the critical aspects of the passport – registration of data and selective disclosure of verifiable data, in a privacy-preserving manner as needed. This falls short of the EU Strategy for Data [28] which notes that DPPs will provide information at inception, operation and EoL of a product. There is therefore a need to extend the functionality to incorporate the use phase of an EV battery, and its EoL / reuse / repurpose phase.

Further this study has focused on the feasibility and functionality of a blockchain-based EV battery tracking approach with SSI-like selective disclosure of EV battery data, and as such, a robust performance, cost and security evaluation has not been carried out.

C. Future Work

BlockBaRT is envisioned to evolve into a comprehensive lifecycle management platform, integrating cradle-to-grave supply chain stakeholders (and processes) including manufacturers, regulators, consumers and service providers, to establish a decentralized, trust-based ecosystem where battery data is securely shared and verified, enhancing transparency and accountability across the supply chain. As such, future work will focus on expanding the system's capabilities to support full lifecycle management of batteries, including during their operation phase, and incorporating additional stakeholders.

Enhancements may include improved user interfaces; adding zero-knowledge proof implementations; data analytics; extended API functionality for automated data management, operational data capture and recycle data capture; performance benchmarking; security evaluation / threat model assessment and evaluation against blockchain-based DPP design frameworks such as the one by [36].

VII. CONCLUSION

This paper presents the POC BlockBaRT web application that demonstrates how blockchain, ZKPs, and SSI principles can be integrated into a battery passport system to enable secure and private data exchange. BlockBaRT allows EV battery manufacturers to create a battery with key data points such as date of manufacture, ethical sourcing score and energy capacity, and pin it to the blockchain. The blockchain capability is provided by integrating with the BlockAPI BaaS platform which provides an API for writing to the blockchain and verifying data. In addition, BlockBaRT allows EV value chain stakeholders to request, share and verify battery data while maintaining confidentiality. Leveraging ZKPs, the system verifies data authenticity without exposing sensitive information, ensuring compliance with privacy and security requirements; and enables attribute-level selective disclosure that is SSI-inspired.

ACKNOWLEDGMENT

The authors acknowledge funding for this project provided by the South Africa National Blockchain Alliance (SANBA), an initiative supported by the South African Department of Science, Technology and Innovation.

REFERENCES

[1] E. R. da Silva, J. Lohmer, M. Rohla, and J. Angelis, Unleashing the circular economy in the electric vehicle battery supply chain: A case study on data sharing and blockchain potential. Resources, Conservation and Recycling, 193, 106969. Chicago, 2023.

[2] C. A. Rufino Júnior, E. Riva Sanseverino, P. Gallo, D. Koch, S. Diel, G. Walter, and H. Zanin, Towards to battery digital passport: reviewing regulations and standards for second-life batteries, Batteries, 10(4), 115, 2024.

[3] S. Jagani, E. Marsillac, and P. Hong, The electric vehicle supply chain ecosystem: changing roles of automotive suppliers. Sustainability, 16(4), 1570, 2024.

[4] P. Barman, L. Dutta, and B. Azzopardi, Electric vehicle battery supply chain and critical materials: a brief survey of state of the art. Energies, 16(8), 3369, 2023.

[5] L. Ahmadi, S. B. Young, M. Fowler, R. A. Fraser, and M. A. Achachlouei, A cascaded life cycle: Reuse of electric vehicle lithium-ion battery packs in energy storage systems, Int. J. Life Cycle Assess, 22, 111–124, 2017.

[6] European Commission, 2020a. Proposal For A Regulation of the European Parliament and of the Council Concerning Batteries And Waste Batteries, Repealing Directive 2006/66/EC and Amending Regulation (EU) No 2019/1020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0798. Accessed on May 08, 2025.

[7] K. Berger, J. P. Schöggl, and R. J. Baumgartner, Digital battery passports to enable circular and sustainable value chains: Conceptualization and use cases. Journal of Cleaner Production, 353, 131492, 2022.

[8] European Commission (2020b), A new circular economy action plan: For a cleaner and more competitive Europe, COM(2020) 98 final, Brussels.

[9] K. Voulgaridis, T. Lagkas, C. M. Angelopoulos, A. A. A. Boulogeorgos, V. Argyriou, and P. Sarigiannidis, Digital product passports as enablers of digital circular economy: a framework based on technological perspective, Telecommunication Systems, 85(4), 699-715, 2024.

[10] J. Mehta, D. Mehta, J. Jain, and S. Dholay, Asset tracking system using blockchain, 2021 Asian Conference on Innovation in Technology (ASIANCON) (pp. 1-7), IEEE, August 2021.

[11] V. Rizos, and P. Urban, Implementing the EU digital battery passport: Opportunities and challenges for battery circularity, CEPS Papers 42379, Centre for European Policy Studies, 2024.

[12] European Parliament and Council, Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC, 2023.

[13] Global Battery Alliance, 2022 Annual Impact Report, Brussels, 2022.

[14] Battery Pass consortium, Battery passport content guidance: Achieving compliance with the EU Battery Regulation and increasing sustainability and circularity, Version 1.0, April 2023.

[15] Battery Passports. [Online]. Available: https://www.minespider.com/battery-passports. Accessed on May 08, 2025.

[16] Mandated Digital Battery Passports. [Online]. Available: https://circulor.com/battery-passport. Accessed on May 08, 2025.

[17] The Digital Product Passport Solution. [Online]. Available: https://www.ipoint-systems.com/solutions/digital-product-passport. Accessed on May 08, 2025.

[18] S. Yamaguchi, International trade and circular economy - Policy alignment, OECD Trade and Environment Working Papers 2021/02, 2021. [Online]. Available: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/02/international-trade-and-circular-economy-policy-alignment_fee7d5b0/ae4a2176-en.pdf. Accessed on May 08, 2025.

[19] C. Catalini, and J.S. Gans, Some simple economics of the blockchain, Communications of the ACM, 63(7), 80-90, 2020

[20] J. Chen, and S. Micali, Algorand, arXiv preprint arXiv:1607.01341, 2016.

[21] G. Zyskind, and O. Nathan, Decentralizing privacy: Using blockchain to protect personal data, 2015 IEEE security and privacy workshops, pp. 180-184, IEEE, May 2015.

[22] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), pp. 468-477, IEEE, May 2017.

[23] D. Gozman, J. Liebenau, and T. Aste, A case study of using blockchain technology in regulatory technology, MIS Quarterly Executive, 19(1), 19-37, 2020.

[24] Microsoft Entra Verified ID. [Online]. Available: https://www.microsoft.com/en-za/security/business/identity-access-management/decentralized-identity-blockchain. Accessed on May 08, 2025.

[25] U. Fiege, A. Fiat, and A. Shamir, Zero knowledge proofs of identity, Proceedings of the nineteenth annual ACM symposium on Theory of computing, pp. 210-217, January 1987.

[26] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, A survey on essential components of a self-sovereign identity, Computer Science Review, 30, 80-86, 2018.

[27] J. Kanjere, and M. Ford, Design and Implementation of BlockAPI - a Blockchain-as-a-Service Platform, IST-Africa 2025 Conference Proceedings, ISBN:978-1-905824-74-8, 2025.

[28] A European strategy for data. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/strategy-data. Accessed on May 08, 2025.

[29] C. Reimsbach-Kounatz, T. Reynolds, and C. Girot, Emerging Privacy Enhancing Technologies - Current regulatory and policy approach, 2023.

[30] G. W. Van Blarkom, J. Balking, and H. Verhaar, PET, Handbook of Privacy and Privacy-Enhancing Technologies - The case of Intelligent Software Agents. 33–54, 2003.

[31] G. Mittal, A. Garg, and K. Pareek, A review of the technologies, challenges and policies implications of electric vehicles and their future development in India, Energy Storage, 6(1), e562, 2024.

[32] R.Y. Kupa, Original equipment manufacturers' perspectives of barriers to the adoption of electric vehicles in South Africa, Master's thesis, University of the Witwatersrand, 2023.

[33] I. I. García, F. D. Muñoz-Escoí, J. A. Aroca, & F. Peñuela, Digital product passport management with decentralised identifiers and verifiable credentials. arXiv preprint arXiv:2410.15758, 2024.

[34] P. Emmenegger, Design, Implementation, and Analysis of Decentralized Product Passport Systems for Circular Construction, Master's thesis, University of Zurich, 2024.

[35] M. Hulea, R. Miron, & V. Muresan, Digital product passport implementation based on multi-blockchain approach with decentralized identifier provider, Applied Sciences, 14(11), 4874, 2024.

[36] H. Abreu, V. Pereira, and J. Barata, Blockchain-based digital product passport: design principles and demonstration. International Journal of Production Research, 1–20, 2025.

[37] L. Navarro, J. C. Esteban, M. F. Miralles, and D. F. Griso, Digital transformation of the circular economy: Digital product passports for transparency, verifiability, accountability. Manuscript submitted for publication, 2022.

[38] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, and J. Yellick, Hyperledger fabric: a distributed operating system for permissioned blockchains, Proceedings of the thirteenth EuroSys conference, pp. 1-15, April 2018.