Computer Science and Information Systems 23(1):603–619 https://doi.org/10.2298/CSIS250410081B

Trustless Exchange for Personal Data: Adapting Intellectual Property Trading Security Protocols for Data Sovereignty*

Vijon Baraku[1], Simeon Veloudis[2,3], Iraklis Paraskakis[2,3], Poonam Yadav[1], and Rezon Baraku[3]

[1] Department of Computer Science, University of York, York, United Kingdom
vibaraku@seerc.org
poonam.yadav@york.ac.uk
[2] SEERC - South East European Research Centre, Thessaloniki, Greece
{iparaskakis, sveloudis}@seerc.org
[3] CITY College, University of York Europe Campus, Thessaloniki, Greece
rbaraku@york.citycollege.eu

Abstract. This paper presents an approach for adapting blockchain-based security protocols originally designed for intellectual property trading to support data sovereignty through secure exchange in personal data stores. As personal data becomes increasingly valuable in the digital economy, individuals need mechanisms to control and potentially monetise their information while ensuring its proper use. We examine how our existing multi-stage verification protocol can be applied to address the requirements of personal data exchange. The protocol uses symmetric and asymmetric encryption, smart contracts, and blockchain verification to create secure trading mechanisms. The proposed adaptation maintains the trustless verification and secure transfer mechanisms of the original protocol, creating a "meta-trust" layer, a higher level of confidence that extends beyond the foundational trust offered by blockchain technology alone. Through this conceptual adaptation, we explore a complementary framework that could enhance existing Personal Data Store (PDS) architectures. This framework enables individuals to selectively share their personal data with cryptographic guarantees about access and use, contributing to the advancement of data sovereignty in digital ecosystems.

Keywords: Data Sovereignty, Personal Data Stores, Blockchain technology, Smart contracts.

1. Introduction

In today's digital landscape, personal data has become a key enabler of economic and technological progress. Organisations collect and process vast amounts of personal information to drive decision-making, enhance services, and create new business opportunities, effectively transforming personal data into a commodity of extraordinary value [22, 11]. However, unlike other commodities, personal data is intrinsically linked to individuals,

* This is an extended version of the conference paper "Blockchain-Based Decentralised Marketplace for Secure Trading of Intellectual Property" presented at INISTA 2024 - The 18th International Conference on Innovations in Intelligent Systems and Applications/BCI 2024

raising significant ethical and legal concerns surrounding its use. In particular, the power asymmetry between data controllers, organisations that legally own and determine how personal data is processed, and individuals has led to growing concerns about privacy, transparency, and ethical data handling practices [19].

In response, the concept of *data sovereignty*, the principle that individuals should have ultimate control over their personal data, has emerged as a critical paradigm shift in data management [2, 10]. Data sovereignty encompasses both legal and technical dimensions. Legally, it is supported by regulatory frameworks such as the General Data Protection Regulation (GDPR), Data Governance Act (DGA), and the Data Act (DA), which aim to protect individuals' rights over their personal information. Technically, however, implementing data sovereignty requires innovative solutions that truly empower individuals within the digital ecosystem.

A promising approach to enabling data sovereignty involves Personal Data Stores (PDS) [6, 13, 15, 21, 9, 17], platforms that allow individuals to create and maintain private repositories of their personal data, and to define the terms under which this data can be accessed or shared. Moreover, many PDS incorporate mechanisms for data monetisation, enabling individuals to profit from personal data exchanges. However, for such digital asset trading to gain traction, a critical challenge must be addressed: establishing buyer trust in the quality and authenticity of the traded data, while preserving the individual's ultimate control over the data.

Contributions: This paper makes the following key contributions:

- We adapt a blockchain-based security protocol from intellectual property trading to personal data sovereignty contexts, addressing buyer-side trust challenges in existing PDS implementations.
- We present detailed algorithmic modifications that enable secure preview of personal data before purchase while maintaining individual control and data sovereignty.
- We provide a proof-of-concept implementation that validates the technical feasibility of the adapted protocol.

The paper explores how our previously developed blockchain-based security protocol for trading intellectual property [5] can be adapted specifically for personal data stores. Rather than proposing a new PDS architecture, our contribution lies in developing a protocol that enhances existing PDS operations by enabling the secure preview of personal data before purchase. The adapted protocol aims to establish a higher level of trust in personal data trading, a form of meta-trust that extends beyond the foundational trust offered by blockchain technology. It enables individuals to selectively share or trade their data with cryptographic assurances regarding access and use, thereby fostering broader participation in the data economy while maintaining data sovereignty.

To validate our approach, we have developed a proof-of-concept implementation that demonstrates the core mechanisms of the protocol adaptation. This technical demonstration confirms the feasibility of our approach while providing practical insights that complement our theoretical framework.

To illustrate the potential impact of this approach, consider Alice, who manages a chronic health condition and regularly generates valuable health data through monitoring devices. If Alice wanted to monetise this health data through a PDS, potential buyers (such as pharmaceutical researchers) currently have no way to verify the quality or relevance of her data without accessing it first, creating a trust paradox. Our protocol addresses this dilemma by allowing researchers to preview a cryptographically secured samples of the data before purchase, while ensuring that Alice maintains control over what is shared and that the complete dataset remains protected.

The remainder of this paper is structured as follows. Section 2 provides background on blockchain technologies, data sovereignty, and personal data stores. Section 3 describes our blockchain-based security protocol for trading digital assets, with emphasis on the generic mechanisms that enable trustless transactions. Section 3.2 presents our main contribution: the adaptation of this protocol for personal data stores. Implementation considerations and use cases are discussed in Sections 3.3. Sections 3.5 and 4 conclude the paper with discussion and final remarks.

2. Background and Related Work

This section reviews relevant literature in three areas: blockchain technologies in digital asset trading, personal data sovereignty concepts, and existing personal data store implementations.

2.1. Blockchain Technologies for Digital Asset Trading

Blockchain technology has paved the way for secure digital asset exchange without centralised intermediaries. The foundational work of Nakamoto [16] introduced the blockchain as a distributed ledger for value transfer, while Buterin's Ethereum platform [8] expanded these capabilities through programmable smart contracts that enable complex trading logic and automated agreement enforcement.

Several researchers have explored blockchain applications for intellectual property and digital rights management, primarily focusing on ownership tracking and secure transfers. For instance, Savelyev [18] examined blockchain's role in managing intellectual property rights, analysing both technical and legal frameworks for tracking ownership and facilitating secure transfers. Ma et al. [14] presented a blockchain-based digital rights management system with cryptographic verification mechanisms for secure content transfer. Bodó et al. [7] proposed a blockchain-based licensing system for digital content that leverages smart contracts for automated enforcement.

While these works demonstrate blockchain's potential for managing digital rights and facilitating asset transfers, they overlook a fundamental trust paradox in personal data trading: buyers must be able to verify the quality of the data before purchase, while sellers must keep the traded data confidential until the transaction is complete.

2.2. Personal Data Sovereignty

Data sovereignty encompasses both legal considerations and individual control. Legally, data sovereignty refers to the principle that data is subject to the laws and governance structures of the country in which it is gathered or held [10]. This includes regulatory frameworks such as the EU's GDPR, the DGA, and the DA, which establish provisions for data protection, usage, and rights. This interpretation has gained relevance and prominence with the rise of cloud computing and global data flows.

Alongside this legal view, a more granular and individual-centric interpretation of data sovereignty has emerged, aided by the efforts of organisations such as the International Data Spaces Association (IDSA) and MyData.org. This interpretation emphasises individual agency, the ability to control how personal data is used, even across technological boundaries. This viewpoint defines data sovereignty as the ability of individuals to retain complete control over their data assets by determining how these may be used across technological boundaries [2]. This perspective shifts focus from legal frameworks to personal agency, emphasising that data sovereignty also involves technical methods that enable data subjects to:

- Specify and enforce usage conditions for personal data assets, regardless of storage location.
- Grant or revoke access rights dynamically, as needed.

However, despite these advancements, practical implementation remains a challenge, as individuals currently lack effective technical means to oversee how their personal information is collected, used, and shared across the digital ecosystem [12].

2.3. Personal Data Stores

PDS represent a paradigm shift in personal data management, placing individuals, rather than organisations, at the center of data control. Unlike traditional models where organisations retain custody of user data in siloed systems and dictate its use, PDS enable individuals to collect, store, manage, and selectively share their personal information from a repository under their direct control. This approach allows for sovereign personal data trading, where individuals determine how their data is accessed and exchanged.

Despite their advantages, PDS do not eliminate organisational data collection: businesses will continue to track user interactions, maintain customer records, and store legally required data. However, PDS introduce greater transparency and control, allowing individuals to negotiate access to their data, reduce excessive tracking, and align data-sharing with their privacy preferences. They also potentially reduce the amount of personal data traded directly between organisations. While challenges remain, PDS have the potential to reshape power dynamics in the digital economy by shifting the balance of control towards individuals.

The conceptual foundations of PDS emerged from early work on user-centric identity and data management, evolving through several generations of implementations to address increasing complexity in personal data governance. Early implementations focused primarily on secure storage and basic permission management. As the need for greater control and interoperability grew, later implementations incorporated more sophisticated features including granular access control, revocation mechanisms, data portability tools, and integration with emerging standards for consent and authentication [4, 3, 1].

Modern PDS architectures integrate several core technical components (see Figure 1) to address security, usability, and interoperability challenges. At their core, PDS feature a secure data repository capable of handling diverse data types while maintaining integrity and supporting efficient queries. This repository can be centralised (cloud-based), or distributed (content-addressable storage), each with implications for control and accessibility. Beyond storage, PDS incorporate identity and authentication mechanisms to verify both the individual's identity and those of potential data recipients. Access control systems enforce permissions at various levels of granularity, from entire datasets to specific attributes. Many implementations also include transparency logging to record all access events and data operations, consent management interfaces for capturing explicit data-sharing authorisations, and interoperability features that facilitate cross-system data exchange [20].

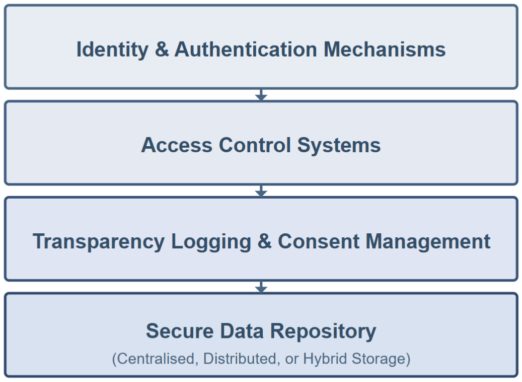
Identity & Authentication Mechanisms
Access Control Systems
Transparency Logging & Consent Management
Secure Data Repository
(Centralised, Distributed, or Hybrid Storage)

Fig. 1. Personal data store architecture with core components: data repository, identity management, access control, logging, consent interfaces, and interoperability features

Several implementations of PDS have been proposed, each emphasising different priorities including decentralisation, privacy, governance, or data economics. Below, we review key PDS platforms that illustrate these diverse approaches.

Solid (Social Linked Data), developed by Berners-Lee [6], prioritises decentralisation and interoperability through its pod-based architecture. Each pod functions as a personal web server hosting data in RDF format, with access managed via Web Access Control (WAC) and Access Control Policies (ACP). WAC enforces basic access permissions at the resource level, while ACP enables more complex, policy-driven controls. Solid offers both self-hosted deployment for technical users and managed hosting through providers like inrupt.com, balancing control with usability. The platform emphasises interoperability leveraging standard web protocols and linked data principles to facilitate seamless data portability across different Solid servers. While Solid has gained significant attention in academic and privacy advocacy communities, its real-world adoption remains limited primarily to research projects and early adopters. The platform currently lacks built-in monetisation mechanisms, focusing instead on data ownership and control rather than economic exchange.

Mydex [13] established one of the earliest operational PDS platforms, implementing a centralised "personal data account" model with strong governance provisions. As a Community Interest Company, Mydex operates under legally binding commitments that prevent exploitation of user data for corporate interests. Regarding deployment, Mydex uses a cloud-based infrastructure model where the organisation maintains the technical infrastructure while individuals maintain control of their data. The platform implements attribute exchange protocols that enable selective disclosure of validated information rather than sharing entire records. Their security architecture includes both symmetric and asymmetric encryption of data at rest and in transit, with keys controlled by the individual, and a verification framework that can authenticate the source and integrity of stored information. For interoperability, Mydex supports standardised data schemas and exchange protocols, though with less emphasis on open standards than Solid. The platform includes monetisation provisions through data exchange agreements where individuals can receive compensation for sharing validated attributes. In terms of adoption, Mydex has achieved limited but concrete implementation in several UK public sector projects.

Databox [15, 21, 9] takes a privacy-centric approach by implementing a localised deployment model based on edge computing. Databox processes data on users' own hardware, such as home routers, minimising external data movement and reducing exposure to third-party systems. Instead of focusing on secure sharing, Databox brings computation to the data through containerised "drivers" that perform specific processing tasks within the secure environment. This architecture implements the principle of data minimisation by enabling third parties to derive insights without accessing raw data, creating a strong privacy protection mechanism. The system includes a "store-first" model where data is captured from various sources before any processing occurs, an app platform for running containerised processing code, and an audit system that documents all data uses. Interoperability in Databox focuses on API-based integration with data sources and processing applications rather than direct data exchange with other systems. The platform includes potential for monetisation through an app marketplace model where users can selectively allow processing of their data in exchange for services or compensation. While technically sophisticated, Databox remains primarily in the academic research domain with limited commercial adoption.

The Hub-of-All-Things (HAT) platform [17] differentiates itself with a strong emphasis on data economics and value exchange. HAT implements "Microservers" as personal data repositories owned and controlled by individuals, with built-in capabilities for data transformation, combination, and analysis. Unlike Solid pods which focus primarily on storage and access control, HAT Microservers include built-in analytics capabilities to derive value from personal data. Regarding deployment, HAT offers a hybrid approach with distributed ownership but centralised technology provision through the HAT Community Foundation. The architecture includes "Data Debits" as structured exchange mechanisms that formalise the terms under which data can be shared, creating explicit value exchange relationships between individuals and data consumers. While similar in concept to smart contracts, Data Debits are specifically designed for personal data exchange with predefined duration and purpose limitations, compared to the more general computational capabilities of blockchain-based smart contracts. HAT's security model combines encryption, access control, and a market-based approach to data valuation. Interoperability is addressed through standardised APIs and data schemas. The platform has achieved moderate adoption through partnerships with commercial entities in the UK and Singapore, with working implementations in the retail and transportation sectors.

This analysis highlights the trade-offs between decentralisation, security, interoperability, and economic models in PDS implementations. While Solid emphasises decentralisation and web standards compatibility, Mydex focuses on governance and validated attribute exchange. Databox prioritises privacy-preservation through local computation,

Table 1. Comparison of Personal Data Store Implementations

PDS	Deployment	Security/Privacy	Interoperability	Monetisation	Adoption
Solid	Self-hosted or managed services; decentralised	WAC/ACP access control; encryption in transit	High: Web standards, RDF, linked data	None built-in	Limited: Research projects
Mydex	Cloud-based; centralised with individual control	Encryption at rest/transit; selective disclosure	Medium: Standard schemas and protocols	Attribute exchange agreements	Limited: UK public sector
Databox	Local hardware; edge computing; highly decentralised	Data minimisation; containerised processing; local computation	Medium: API integration with data sources	App marketplace model	Very limited: Academic only
HAT	Hybrid: distributed ownership, centralised technology	Encryption; Data Debits with time/purpose limits	Medium: Standard APIs and schemas	Data Debits as economic exchange	Moderate: Commercial partnerships

and HAT explores data monetisation possibilities with its Data Debits model. Each implementation represents different priorities within the personal data sovereignty space, with varying degrees of success in real-world adoption. However, none of these approaches make provisions to enhance buyer-side trust through mechanisms that would allow data consumers to verify data quality or authenticity before completing transactions.

These implementations demonstrate diverse approaches to personal data management, yet none fully leverage blockchain technology. Moreover, current PDS architectures lack robust mechanisms for buyers to verify data quality before committing to an exchange, creating significant challenges in personal data markets where trust is essential for enabling scalable data transactions between strangers. This trust deficit represents a key distinction between existing approaches and our blockchain-based framework. While current systems rely primarily on conventional access control mechanisms, our blockchain-based approach offers several unique advantages: transparent and immutable transaction records that create verifiable evidence of data exchanges and trustless verification through cryptographic techniques. These capabilities are particularly valuable in scenarios where individuals wish to exchange data with previously unknown parties or monetise their personal information while maintaining cryptographic guarantees about access. By exploring how these blockchain-based mechanisms could be applied to personal data contexts, our work highlights a complementary technical approach that could enhance the security and trust characteristics of future personal data exchange systems.

3. Blockchain-Based Protocol for Trading Intellectual Property and its Adaptation for Personal Data Stores

This section presents the blockchain-based security protocol for trading Intellectual Property originally introduced in [5]. The protocol enables buyers to preview digital assets before purchasing, thus establishing a higher level of trust, or meta-trust, that goes beyond the trust already provided by blockchains. This meta-trust is crucial in contexts where buyers require quality verification before committing to a purchase, which applies both to intellectual property trading [5] and personal data exchanges facilitated through PDS. Current PDS implementations lack robust mechanisms for such verification, making this protocol adaptation particularly valuable for advancing personal data sovereignty.

While describing each component of the protocol, we simultaneously discuss how it can be adapted to address the specific requirements of PDS and enable personal data sovereignty. By examining both the original application and potential adaptations, we demonstrate how specialised security mechanisms developed for intellectual property trading can be repurposed to enhance individual control over personal data.

3.1. Prerequisites and System Architecture

The protocol relies on several key components to facilitate secure trading without intermediaries. It is implemented as a web-based decentralised application (dApp), but differs from traditional web applications that separate frontend and backend functionalities. Instead, our dApp connects the frontend directly to blockchain networks via wallets, which store blockchain addresses and cryptographic keys to authenticate users and execute smart contract transactions.

Once users link their blockchain wallets, they can submit requests through the frontend, which are processed by smart contracts on the blockchain, stored in the InterPlanetary File System (IPFS)[4], or handled directly within the frontend. IPFS serves as a decentralised storage system for file retrieval, while smart contracts enforce business logic on-chain. To enhance security, critical operations such as file encryption and decryption occur locally on the frontend, minimising unnecessary data exposure.

The system supports two primary user roles:

- **Sellers**: Individuals who provide digital assets for sale, along with necessary metadata such as price and encrypted content location.
- **Buyers**: Users who wish to purchase digital assets, with mechanisms to verify quality through randomly selected samples before committing to purchase.

In the context of PDS, these roles would translate to:

- **Data Subjects**: Individuals who offer their personal data for sharing or monetisation through the PDS.
- **Data Recipients**: Entities interested in accessing or purchasing personal data, who need verification of data quality and relevance before commitment.

This direct correlation between roles in both contexts demonstrates the initial feasibility of adapting the protocol. However, personal data exchange presents specific requirements that necessitate adaptations to the original protocol, as discussed in the following subsections.

3.2. Protocol Design and Adaptation

The security protocol consists of four stages, each with specific adaptation considerations for personal data contexts.

[4] A peer-to-peer network for sharing data using a distributed hash table. `https://ipfs.tech/`

Stage 1: Preparing Digital Assets for Sale. In the initial stage, sellers prepare their digital assets for secure trading. The seller must ensure that only authorised users (buyers who have completed the purchase) can view the content, protecting the value of the digital assets until a transaction is complete. To achieve this, the seller proceeds as follows:

Algorithm 1 Asset Preparation Protocol

```
procedure PrepareAssets($assets[]$)
    for each $asset$ in $assets[]$ do
        $symmetricKey \leftarrow$ GenerateRandomKey()
        $encryptedAsset \leftarrow$ EncryptAES256($asset$, $symmetricKey$)
        Store $symmetricKey$ securely
        Store $encryptedAsset$ on IPFS
    end for
end procedure
```

As outlined in Algorithm 1 (Asset Preparation Protocol), the seller encrypts each digital asset using symmetric encryption (AES-256) and generates unique encryption keys. This encryption ensures that even if the assets themselves are accessible through IPFS, they remain confidential without the corresponding decryption keys.

Adaptation for PDS: For personal data contexts, the algorithm implementation organises data into structured records based on distinct categories, including demographic information, transaction history, and preference data, rather than treating each asset as a unique creative work. The PDS implementation maintains the same encryption approach while extending it with an authenticity metadata layer.

Unlike intellectual property, where value is largely subjective, personal data often requires verification of source and accuracy. The protocol extension incorporates authenticity indicators such as digital signatures from original data sources and verification timestamps into the metadata structure. This authentication mechanism directly addresses the verification requirements in personal data exchanges while preserving the security foundation of the original protocol.

Stage 2: Sample Request and Selection. To ensure buyers can verify product quality without gaining access to the complete collection, the protocol implements a secure sampling mechanism:

Algorithm 2 (Sample Request Protocol) implements a verifiable random selection process that is crucial for fair sample verification. This process prevents sellers from deliberately choosing high-quality samples that might not represent the overall collection quality. The smart contract randomly selects one encrypted key hash from all submitted hashes, and the blockchain's transparency ensures this selection process cannot be manipulated by either party.

Adaptation for PDS: For personal data exchange, the algorithm implementation provides meaningful sampling capabilities while preserving the critical randomness mechanism that prevents selective presentation. Personal data requires contextual understanding for effective evaluation, a feature missing from current PDS architectures that creates significant friction in personal data markets.

Algorithm 2 Sample Request Protocol

```
procedure RequestSample($symmetricKeys[]$)
    Buyer → Seller: Sample request with $buyerPublicKey$
    $encryptedKeys[] \leftarrow \emptyset$
    for each $key$ in $symmetricKeys[]$ do
        $encryptedKey \leftarrow$ AsymmetricEncrypt($key$, $buyerPublicKey$)
        $hashedKey \leftarrow$ Hash($encryptedKey$)
        Add $hashedKey$ to $encryptedKeys[]$
    end for
    Seller → Blockchain: Upload $encryptedKeys[]$
    $randomIndex \leftarrow$ SmartContract.SelectRandom(0, length($encryptedKeys[]$)-1)
    $selectedHash \leftarrow encryptedKeys[randomIndex]$
    return $selectedHash$
end procedure
```

The protocol implementation enhances the sample selection process with contextual metadata that characterises the selected data without compromising confidentiality. This contextual layer enables data recipients to properly interpret and evaluate the sample data within its broader framework. The implementation also supports multiple sample selection across different data categories, delivering a comprehensive cross-sectional view of data quality across various personal information types.

Stage 3: Sample Delivery. Once a sample has been selected, the seller must provide the corresponding key to the buyer:

Algorithm 3 Sample Delivery Protocol

```
procedure DeliverSample($selectedHash$)
    SmartContract → Seller: Notification of selected hash
    Seller → SmartContract: $encryptedKey$ corresponding to $selectedHash$
    SmartContract: Verify $hash(encryptedKey) = selectedHash$
    if verification succeeds then
        SmartContract → Buyer: $encryptedKey$
        Buyer: $symmetricKey \leftarrow decrypt(encryptedKey, buyerPrivateKey)$
        Buyer: Access sample using $symmetricKey$
    else
        Transaction fails
    end if
end procedure
```

Algorithm 3 (Sample Delivery Protocol) manages the secure delivery of the selected sample to the potential buyer. Once a hash is randomly selected, the protocol verifies the corresponding encrypted key through hash comparison before delivery, ensuring that only the specific sample chosen by the smart contract is provided to the buyer.

Adaptation for PDS: The sample delivery mechanism translates directly to personal data contexts with minimal architectural changes. The core verification process maintains the same cryptographic integrity while integrating the contextual metadata layer that positions each sample within the broader data collection framework.

This implementation preserves the security architecture of the original protocol while specifically addressing the challenges of evaluating personal data quality. The transparent verification process builds recipient confidence that they are examining representative samples of the actual data they may acquire, addressing a critical trust gap in current personal data exchange systems.

Stage 4: Purchase and Complete Delivery. If the buyer is satisfied with the sample quality, they can proceed with the purchase:

Algorithm 4 Purchase Completion Protocol

```
procedure COMPLETEPURCHASE($hashedKeys[]$)
    Buyer → SmartContract: Purchase request with payment
    SmartContract: Hold payment in escrow
    SmartContract → Seller: Purchase notification
    Seller → SmartContract: All $encryptedKeys[]$
    $verified$ ← TRUE
    for each $encryptedKey$ in $encryptedKeys[]$ do
        $hashedKey$ ← Hash($encryptedKey$)
        if $hashedKey$ not in $hashedKeys[]$ then
            $verified$ ← FALSE
            break
        end if
    end for
    if $verified$ then
        SmartContract → Seller: Release payment
        SmartContract → Buyer: All $encryptedKeys[]$
        Buyer: Decrypt and access all assets
    else
        Transaction fails
    end if
end procedure
```

Algorithm 4 (Purchase Completion Protocol) finalises the transaction while ensuring both parties fulfil their obligations. The smart contract holds payment in escrow until the seller provides all remaining encrypted keys, which are then verified against their previously stored hashes. This verification ensures the buyer receives all necessary keys to access their purchased content while the seller receives payment only after providing valid keys.

Adaptation for PDS: For personal data exchange, this stage implements expanded transaction terms while maintaining the core key delivery mechanisms. The smart contract extension incorporates detailed usage agreement parameters including permitted purposes, access duration rights, processing restrictions, and attribution requirements.

The implementation stores hashed representations of these agreement terms and requires explicit cryptographic acceptance via digital signatures. This architecture produces an immutable record that the recipient acknowledged specific conditions prior to receiving access. While the smart contract cannot directly monitor post-delivery data usage, the blockchain record serves as definitive evidence of the agreed-upon terms for dispute resolution.

This implementation bridges a critical gap in current personal data exchange systems that lack robust mechanisms for formalising and recording usage agreements. The protocol extension gives individuals precise control mechanisms over how their personal data is used after sharing.

Public Key Recovery. Supporting all stages of the protocol, a critical technical component is the ability to recover a user's public key from their blockchain address:

Algorithm 5 Public Key Recovery Protocol

```
procedure RecoverPublicKey($ethereumAddress$)
    $addressHash$ ← Keccak256($ethereumAddress$)
    $signature$ ← Sign($addressHash$, $userPrivateKey$)
    Extract $r, s$ values from $signature$
    $publicKey$ ← ECDSARecover($addressHash$, $r$, $s$)
    return $publicKey$
end procedure
```

Algorithm 5 (Public Key Recovery Protocol) enables secure asymmetric encryption by recovering a user's public key from their Ethereum address. This recovery process allows for secure key exchange without requiring users to manually manage cryptographic keys.

Adaptation for PDS: This component functions identically in personal data contexts, as the cryptographic requirements for secure key exchange remain consistent across domains. The public key recovery mechanism operates in the PDS implementation with the same security architecture, maintaining consistent user experience and cryptographic protections.

3.3. Technical Implementation

These algorithms have been implemented in Solidity, the primary programming language for Ethereum smart contracts. The smart contract implementation oversees the entire transaction process, ensuring security without requiring trust between participants. The contract handles four critical functions: recording sample requests from potential buyers, implementing verifiable random sample selection, verifying the authenticity of provided keys via hash comparison, and securing the exchange of payment and keys.

In the Solidity implementation, we've incorporated important safeguards for both parties. For buyers, the contract includes an escrow mechanism that holds payments until valid keys are delivered and verified through hash comparison. If the seller fails to provide valid keys within a specified timeframe (24 hours in our implementation), the buyer can execute a function to retrieve their deposited funds. For sellers, the contract includes ownership verification that prevents unauthorised modifications and ensures only legitimate buyers can access the encrypted keys. Additionally, the contract implements gas-efficient verification procedures that balance thorough validation with reasonable transaction costs.

This design creates a self-enforcing agreement that protects both intellectual property rights and buyer interests without the need for centralised intermediaries. Readers should refer to our previous work [5] for full implementation details.

Adaptation for PDS: The PDS implementation extends the smart contract with additional state variables and functions that handle the complex data usage agreements. The contract extension includes structured data types for agreement terms storage, cryptographic functions for verifying recipient acceptance signatures, and time-bound access control mechanisms that enforce specified duration limits.

The extended implementation maintains the core security architecture while incorporating the specific functionalities required for personal data contexts. The contract optimises these extensions for gas efficiency to ensure practical usability on public blockchains without compromising the enhanced functionality.

3.4. Security Analysis and Benefits

The security protocol provides several important guarantees that apply to both intellectual property trading and personal data exchange:

- **Seller/Data Subject Protection:** Complete confidentiality of digital assets or personal data is maintained, as all content is encrypted before being made available. Only authorised entities who have completed the transaction receive decryption keys.
- **Buyer/Recipient Protection:** The ability to verify quality through randomly selected samples before purchase prevents misrepresentation of assets or data. The blockchain enforced randomness ensures this verification is trustworthy.
- **Transaction Integrity:** The smart contract ensures that both parties fulfil their obligations, with buyers/recipients receiving valid keys only after payment and sellers/data subjects receiving payment only after providing valid keys.
- **No Trust Requirements:** The protocol eliminates the need for trust between parties. The cryptographic verification and blockchain-based enforcement ensure compliance without requiring trust in either the counterparty or a central authority.
- **Non-repudiation:** All transactions are recorded on the blockchain, providing an immutable record that neither party can later deny.

Additional Benefits for PDS: Adapting this protocol for PDS creates several important capabilities for personal data sovereignty that aren’t present in existing PDS implementations:

- **Reduced Information Asymmetry:** Both parties can verify aspects of the exchange before commitment, addressing a critical weakness in current data marketplaces.
- **Enhanced Transparency:** The blockchain-based record creates transparency and accountability not typically found in conventional data sharing mechanisms.
- **Expanded Exchange Opportunities:** By minimising trust requirements through cryptographic verification and blockchain-based enforcement, the protocol potentially enables secure personal data exchange between individuals and organisations without established relationships.

- **Individual Empowerment:** The protocol provides individuals with greater agency in deciding how their personal data is shared and used, advancing the broader goal of data sovereignty.

The combination of symmetric encryption for content protection, asymmetric encryption for secure key exchange, and blockchain-based verification creates a comprehensive security framework that addresses the key challenges in both intellectual property trading and personal data exchange.

3.5. Key Requirements Addressed by Protocol Adaptation

To summarise, the protocol adaptation described in this section effectively addresses several critical requirements for secure personal data exchange:

- **Data Quality Verification:** By implementing the sample selection and delivery mechanisms (Algorithms 2 and 3), the protocol enables recipients to evaluate personal data before commitment, solving a key limitation of current PDS architectures.
- **Formal Usage Agreements:** The extended smart contract functionality creates cryptographically signed records of data usage terms, providing a foundation for accountability in personal data exchanges.
- **Secure Exchange Mechanism:** The trustless escrow system ensures fair exchange without requiring third-party intermediaries, protecting both data subjects and recipients.
- **Transparency and Non-repudiation:** The blockchain-based implementation provides an immutable record of all transactions, creating transparency that's often lacking in conventional data sharing approaches.

The theoretical protocol adaptation described in this paper has been complemented by a technical demonstration implementing key components of the system. This implementation successfully validates the sample selection and verification mechanisms in a personal data context, confirming that the cryptographic and blockchain-based verification approaches translate effectively from intellectual property to personal data sovereignty applications. The implementation particularly demonstrates the technical viability of trustless sample verification.

4. Conclusion and future works

This paper demonstrates how the blockchain-based security protocol developed for intellectual property trading could be utilised to address challenges in personal data sovereignty. The exploration of adapting a multi-stage verification protocol built on symmetric and asymmetric encryption, smart contracts, and blockchain verification reveals a practical framework for personal data exchange that preserves individual control while enabling participation in the data economy. The protocol creates a level of meta-trust that goes beyond the basic trust provided by blockchain technology alone, by allowing data buyers to verify quality before purchase while still protecting sellers' data sovereignty.

Rather than proposing a new PDS architecture, our research offers a complementary security protocol that addresses a critical gap in existing PDS implementations: the lack of buyer-side trust mechanisms. The proposed adaptation maintains the core security mechanisms of the original protocol while introducing specific modifications to address the unique requirements of personal data contexts. By implementing structured data organisation, enhanced authenticity verification, and expanded usage agreements, the protocol creates a trustless environment where individuals can confidently share their personal information.

This research, including our technical demonstration, provides a foundation for further exploration. The implementation has validated our theoretical adaptations, particularly the critical sample selection and verification mechanisms. Building on this foundation, future work can focus on extending the implementation to more complex usage scenarios and evaluating its performance at scale.

Another promising direction for future work is exploring how smart contracts could be extended to enforce post-sharing obligations in personal data exchanges. While current PDS implementations typically focus on access control before sharing rather than enforcement after access is granted, our blockchain-based approach creates a foundation for implementing enforceable usage terms. Future research could investigate mechanisms for monitoring compliance with data usage agreements, implementing automated penalties for violations, and creating auditable records of data usage that extend beyond the initial exchange.

Additionally, future work should look at the legal and regulatory implications of the proposed approach, specifically how the protocol complies with GDPR standards and other data protection frameworks. This analysis would help identify any potential compliance gaps and determine how the protocol should evolve to fulfil regulatory standards.

The practical implementation faces certain technical challenges, particularly regarding smart contract extensions for complex usage agreements and robust authenticity verification. Nevertheless, the conceptual framework demonstrates significant promise in repurposing specialised security mechanisms to shift power dynamics in the digital data economy. This proposed adaptation represents a meaningful step toward enabling individuals to participate in and benefit from the value of their personal data while maintaining complete sovereignty over its access and use.

References

1. Abiteboul, S., André, B., Kaplan, D.: Managing your digital life. Communications of the ACM 58(5), 32–35 (2015)
2. Bader, S., Pullmann, J., Mader, C., Tramp, S., Quix, C., Müller, A.W., Akyürek, H., Böckmann, M., Imbusch, B.T., Lipp, J., et al.: The international data spaces information model–an ontology for sovereign exchange of digital content. In: International Semantic Web Conference. pp. 176–192. Springer (2020)
3. Baraku, V., Paraskakis, I., Veloudis, S., Yadav, P.: Personal data sovereignty in virtual enterprises: Implementing data capsules for enhanced privacy and compliance. In: Working Conference on Virtual Enterprises. pp. 447–461. Springer (2024)
4. Baraku, V., Paraskakis, I., Veloudis, S., Yadav, P.: Responsible information sharing in the era of big data analytics facilitating digital economy through the use of blockchain technology and observing gdpr. In: CLOSER. pp. 257–264 (2024)
5. Baraku, V., Veloudis, S., Paraskakis, I., Yadav, P.: Blockchain-based decentralised marketplace for secure trading of intellectual property. In: Bădică, C., Gušev, M., Iftene, A., Ivanović, M.,

Manolopoulos, Y., Xinogalos, S. (eds.) Advances in ICT Research in the Balkans, pp. 208–219. Springer Nature Switzerland, Cham (2025)

6. Berners-Lee, T., Sambra, A., Capadisli, S., Verborgh, R., Mansour, E., Hawke, S., Hess, C., Eling, N.: Solid: A platform for decentralized social applications based on linked data. Technical report, MIT CSAIL & Qatar Computing Research Institute (2018)
7. Bodó, B., Gervais, D., Quintais, J.: Blockchain and smart contracts: the missing link in copyright licensing? International Journal of Law and Information Technology 26(4), 311–336 (2018)
8. Buterin, V.: Ethereum white paper: A next-generation smart contract and decentralized application platform. Ethereum Foundation (2014), [Online]. Available: https://ethereum.org/en/whitepaper/
9. Crabtree, A., Lodge, T., Colley, J., et al.: Building accountability into the internet of things: the iot databox model. Journal of Reliable Intelligent Environments 4, 39–55 (2018)
10. De Hert, P., Papakonstantinou, V.: The new general data protection regulation: Still a sound system for the protection of individuals? Computer Law & Security Review 32(2), 179–194 (2016)
11. Fathullah, M.A., Subbarao, A., Muthaiyah, S.: A review of data breach cost in cloud computing. In: Proceedings of the International Conference on Technology and Innovation Management (ICTIM 2022). pp. 199–209. Atlantis Press (2022)
12. Janssen, M., Brous, P., Estevez, E., Barbosa, L., Janowski, T.: Data governance: Organizing data for trustworthy artificial intelligence. Government Information Quarterly 37(3), 101493 (2020)
13. Kirkham, T., Winfield, S., Ravet, S., Kellomäki, S.: The personal data store approach to personal data security. IEEE Security & Privacy 11(5), 12–19 (2013)
14. Ma, Z., Jiang, M., Gao, H., Wang, Z.: Blockchain for digital rights management. Future Generation Computer Systems 89, 746–764 (2018)
15. Mortier, R., Zhao, J., Crowcroft, J., Wang, L., Li, Q., Haddadi, H., Amar, Y., Crabtree, A., Colley, J., Lodge, T., Brown, A.: Personal data management with the databox: What's inside the box? In: Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking. pp. 49–54 (2016)
16. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review (2008)
17. Ng, I., Holtby, J., Ma, X., Alahmadi, A., Turoczy, S.: White paper on the hat (hub-of-all-things) and hatdex personal data exchange ecosystem. Working paper series, WMG Service Systems Research Group (2017)
18. Savelyev, A.: Copyright in the blockchain era: Promises and challenges. Computer Law & Security Review 34(3), 550–561 (2018)
19. Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwaider, M.: Iot privacy and security: Challenges and solutions. Applied Sciences 10(12), 4102 (2020)
20. Van Kleek, M., Liccardi, I., Binns, R., Zhao, J., Weitzner, D., Shadbolt, N.: Better the devil you know: Exposing the data sharing practices of smartphone apps. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. pp. 5208–5220 (2018)
21. Yadav, P., Moore, J., Li, Q., Mortier, R., Brown, A., Crabtree, A., Greenhalgh, C., McAuley, D., Amar, Y., Shamsabadi, A.S., Haddadi, H.: Providing occupancy as a service with databox. In: Proceedings of the 1st ACM International Workshop on Smart Cities and Fog Computing (CitiFog'18). pp. 29–34. Association for Computing Machinery, New York, NY, USA (2018)
22. Zuboff, S., Schwandt, K.: The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Profile Books (2019)

Vijon Baraku is a PhD student in the Department of Computer Science at the University of York, UK. His research interests focus on data sovereignty, data ownership, blockchain technology, and knowledge representation.

Simeon Veloudis is an Associate Professor in the Department of Computer Science at CITY College and a Senior Researcher at the South East European Research Centre (SEERC). He holds a PhD in Computer Science from the University of Reading. His research interests include Cloud Computing, Semantic Modelling, Knowledge Representation, Security, and Formal Methods.

Iraklis Paraskakis is a Professor of Information Systems in the Department of Computer Science at CITY College, Greece, and a Senior Research Officer at the South East European Research Centre (SEERC), where he coordinates the Information & Knowledge Management Research Group. He holds a PhD in Information Technology and Education from the Open University (UK) and an MSc from London School of Economics. His research focuses on Cloud Computing, Service Oriented Computing, Educational Informatics, and Knowledge Management.

Poonam Yadav is a Senior Lecturer in the Computer Science Department at the University of York, UK, and a visiting research fellow at Computer Lab, Cambridge University. Her research focuses on making IoT and edge computing-based distributed systems resilient, reliable, and robust, with particular emphasis on coordination and collaboration in resource-constrained environments. She leads the System and Network Interoperability (SYSTRON) Lab.

Rezon Baraku holds a BSc from CITY College, University of York. His research focuses on blockchain technology.

Received: April 10, 2025; Accepted: July 17, 2025.