DATAVAULT

FIN 4810-01 Final Report

Sabina Thai, Olivia Neunaber, Shruti Panda, Isabella Bretel, Sana Syed, and Gabby Flowers

Contents

Problem Identification 2

Proposed Solution 3

Why Blockchain? 4

Token Economics 5

Smart Contract and Execution Plan 6

Competitive Differentiation 11

Business Model 12

Challenges 13

References 15

Problem Identification

Every time users browse the web, download an app, or make a purchase online, companies collect personal data. In most cases, users have limited visibility into how that data is stored, shared, or monetized. As a result, trust in data handling practices has declined significantly.

The current system provides little ability for users to audit data usage, trace data sharing, or verify consent in a meaningful way. At the same time, companies face increasing regulatory pressure to demonstrate compliant data practices yet lack reliable infrastructure to prove consent was properly obtained.

Research indicates that 79% of users want greater control over their personal data (Pew Research Center, 2023). However, existing consent mechanisms are often limited to broad "accept all cookies" flows, which do not reflect meaningful user choice. This creates inefficiencies for both users and companies: users provide consent without understanding implications, while companies receive data that may not be fully verifiable or consent backed.

The data exchanged in this system typically includes browsing behavior, purchase history, location data, and app usage patterns. These data types are widely used in digital advertising and analytics (Interactive Advertising Bureau, 2024). However, because consent is often inferred or bundled into terms of service agreements, verification remains limited. This reduces confidence in data quality and creates compliance challenges for companies.

This creates a structural gap in the market. The advertising ecosystem is undergoing major disruption as third-party cookies are phased out and privacy-by-design systems become the default across major browsers (Google, 2025; Forrester Research, 2024). At the same time, regulatory pressure continues to increase under modern privacy frameworks such as GDPR enforcement expansion and updated compliance requirements across jurisdictions (European Data Protection Board, 2024; DLA Piper, 2024). The market is actively searching for a system that makes consent verifiable, data trustworthy, and exchange fair. DataVault is designed to address this gap by creating a system where user consent is verifiable, data access is permissioned, and participation is compensated.

Proposed Solution

Platform Overview

DataVault is a software platform that operates across three surfaces: a browser extension, a mobile application, and a desktop background service. These components work together to monitor and manage data collection activity across a user's digital environment. A blockchain layer records consent events, token transfers, and validator confirmations. Personal data itself remains encrypted and stored off chain. The system involves three participant groups: users who control and optionally monetize their data, companies that request permissioned data access, and validators who confirm transactions using a proof-of-history mechanism in exchange for monetary value coming from transaction fees. The platform is free for users. Revenue is generated from companies purchasing consent-based data access. This structure reduces adoption friction and aligns incentives toward user participation.

What Data is Collected and How

DataVault organizes user information into six separate data categories, each controlled through its own consent setting. Users can enable or revoke access to any category at any time. This approach addresses a major weakness in the current system, where users are often forced to accept broad data collection policies through a single cookie banner.

Data Category	What is Captured	Collection Mechanism
Browsing behavior	Pages visited, search queries, click patterns, scroll depth, time on page	Browser extension intercepting tracking activity
Purchase history	Transaction records, product categories, spending levels, retail preferences	Hashed metadata transmitted only when active consent exists
Location data	GPS coordinates, store visits, commute patterns, travel history	Mobile app with explicit GPS permission granted by the user
App usage patterns	Apps open, duration of use, interaction frequency, screen time by category	Mobile VPN layer with on-device traffic monitoring
Demographic signals	Estimated age bracket, income range, household composition, interest categories	Derived algorithmically from other consented data categories rather than directly surveyed

Table 1. *DataVault data categories and collection mechanisms*

How Data is Protected

All personal data is encrypted off-chain database partitioned by users. Access is controlled through encryption keys derived from the user's wallet address, meaning only the user, or a party they explicitly authorize through a smart contract consent agreement, can decrypt the information. DataVault's servers cannot directly read user data, and only hashed metadata is written on the blockchain.

DataVault does not combine user information into a single centralized database. Companies only receive access to data from users who have explicitly granted permission. The architecture reduces the risk of DataVault becoming a large-scale target for data brokers or cyberattacks while also limiting the possibility of a single catastrophic data breach.

Why Blockchain?

A traditional centralized database could reproduce some of DataVault's functionality, but it would also recreate the same trust issues the platform is meant to address. Centralized platforms such as major digital advertising ecosystems rely on internal verification systems without independent external validation (Forrester Research, 2024). Blockchain replaces this structure by distributing verification across a decentralized network, where system rules are enforced through smart contracts rather than a single company's internal policies (Ethereum Foundation, 2024; Solana Labs, 2025).

Decentralization and Transparency

Blockchain replaces centralized control with a distributed network of validators that collectively maintain the consent ledger. Because records are shared across many nodes, no single company can alter, suppress, or selectively enforce consent activity. This creates a more transparent system where users can independently verify how and when their data is shared.

Data Ownership and Control

Traditional digital platforms typically collect and monetize data with limited user oversight. DataVault instead gives users direct control over what data is shared, who can access it, and how long access remains active. Permission settings are managed through private-ley authorization and smart contracts, which allow users to revoke consent access at any time.

Immutability and Accountability

Once a consent event is recorded on chain, it becomes highly resistant to modification or deletion. This creates a permanent audit trail that improves accountability for both companies and the platform itself. Neither DataVault nor participating companies can quietly remove or alter consent records after the transaction has occurred.

Automated Smart Contracts

Smart contracts automatically execute payments and enforce access permissions when predefined conditions are met. This removes the need for manual oversight while reducing delays and opportunities for manipulation. For example, the platform's 85/10/5 payment split is enforced automatically through code rather than company policy, which ensures transactions are handled consistently across the network.

Token Economics

The Token Economics behind DataVault are designed to connect the value of the DVT token directly to real-world data usage rather than speculation. Instead of creating demand through hype or trading activity alone, the platform creates utility-based demand because companies must acquire DVT tokens to access user data. This structure gives the token a practical function within the ecosystem and ensures that usage of the platform naturally increases demand for the token over time.

While many cryptocurrency projects rely heavily on inflationary rewards or unrestricted token minting, DataVault limits how tokens enter circulation. DVT is primarily circulated through legitimate data transactions between companies and users. When a company wants access to specific consumer information, it must first purchase DVT and submit a request through the platform. The requested tokens are then placed into escrow by a smart contract until the user reviews and approves the request. This escrow system creates accountability because companies cannot gain access to data without verified user consent.

The consent process is one of the most important parts of the platform's design. Users always maintain ownership and control over their personal information, which reinforces the platform's emphasis on transparency and autonomy. Access to data is permission-based, temporary, and revocable, meaning users can withdraw consent at any time. By tying token release directly to verified consent, DataVault aligns economic incentives with ethical data practices.

Once consent is granted, validators confirm that the transaction and data transfer occurred correctly through a proof-of-history verification process. Validators play a key role in maintaining trust and reliability across the network because they ensure that data requests, permissions, and payments are accurately recorded on chain. After verification, the payment is automatically distributed through the smart contract system. Approximately 85% of the payment goes directly to the user providing the data, 10% is allocated to validators for maintaining and securing the network, and the remaining 5% is directed to the protocol treasury.

This payment structure is intended to align incentives across all participants in the ecosystem. Users are financially rewarded for sharing valuable data, companies gain access to verified and permissioned information, validators are compensated for maintaining trust within the system, and the treasury receives funding to sustain long-term platform growth. Because every participant benefits from honest participation, the model encourages cooperation while discouraging misuse of consumer data.

The token system helps reinforce scarcity and long-term value preservation. Since access requests require DVT to be temporarily locked in escrow, portions of the circulating supply are continuously removed from the active circulating supply during transactions. At the same time, the platform avoids unlimited token creation, helping reduce inflationary pressure that can weaken many digital assets over time.

Overall, DataVault's token economics is structured to support a transparent, decentralized marketplace for personal data. By combining permission-based access, escrow mechanisms, validator incentives, and utility-driven demand, the model attempts to create a more balanced relationship between consumers and companies. Rather than allowing corporations to collect and monetize user information without compensation, the platform gives users ownership, control, and direct participation in the value generated from their data.

Smart Contract and Execution Plan

The DataVault smart contract (DataVault.sol) serves as the core transaction and consent management system for the platform. Rather than storing personal data directly, the contract records agreements related to data access, including who granted consent, what data was approved, how long access remains active, and how much DVT was exchanged. All personal data itself remains encrypted and stored off chain. Only consent metadata and cryptographic proof hashes are written to the blockchain, helping maintain user privacy while still creating a transparent and verifiable audit trail.

DataVault Function	Purpose
recordConsent	Company posts a data request and locks DVT into escrow.
grantConsent	User reviews and approves the request; access window opens
verifyDataDelivery	Validator confirms data was accessed; records a cryptographic evidence hash
releasePayment	DVT splits automatically: 85% to user, 10% to validators, 5% to treasury

Table 2. *DataVault smart contract functions and purpose*

Smart Contract Solidity Code

Function 1: recordConsent — called by the company

```
// Company posts a data request and locks DVT into escrow
function recordConsent(
    address user,           // Data owner's wallet address
    DataCategory category,    // Browsing, Location, Purchases, etc.
    uint256 dvtAmount,       // Payment offered to the user
    uint256 durationSeconds    // How long access lasts if granted
) external returns (uint256 consentId) {
    // Lock company DVT into this contract as escrow
    dvtToken.transferFrom(msg.sender, address(this), dvtAmount);
    // Write consent record on-chain — status: Pending
    consents[consentId] = ConsentRecord({
        user: user,  company: msg.sender,
        category: category,  dvtAmount: dvtAmount,
        status: ConsentStatus.Pending
    });
    emit ConsentRequested(consentId, msg.sender, category, dvtAmount);
}
```

Function 2: grantConsent — called by the user

```
// User approves the request — access window opens
function grantConsent(uint256 id) external {
    require(msg.sender == record.user, 'Only data owner can grant consent');
    require(record.status == Pending,  'Must be in Pending state');
    record.expiresAt = block.timestamp + durationSeconds;
    record.status    = ConsentStatus.Active;
    emit ConsentGranted(id, msg.sender, record.expiresAt);
}
```

Function 3: verifyDataDelivery — called by a validator

```
// Validator confirms access occurred — records hash, never the raw data
function verifyDataDelivery(uint256 id, bytes32 evidenceHash)
    external onlyValidator {
    require(record.status == Active,          'Consent must be Active');
    require(block.timestamp <= record.expiresAt, 'Access window has expired');
    record.evidenceHash = evidenceHash;  // Cryptographic fingerprint only
    record.status      = ConsentStatus.Delivered;
    emit DataDeliveryVerified(id, evidenceHash);
}
```

Function 4: releasePayment — DVT splits automatically

```
// Automatic three-way split — no human intervention required
function releasePayment(uint256 id) external onlyValidator {
    uint256 total     = record.dvtAmount;
    uint256 userShare  = (total * 8500) / 10000;  // 85% to data owner
    uint256 valShare   = (total * 1000) / 10000;  // 10% to validators
    uint256 protoShare = (total *  500) / 10000;  //  5% to treasury
    dvtToken.transfer(record.user, userShare);    // Pay user
    dvtToken.transfer(validators,  valShare);     // Pay validator network
    dvtToken.transfer(treasury,    protoShare);   // Protocol fee
    emit PaymentReleased(id, record.user, userShare, valShare, protoShare);
}
```

Development Roadmap

The execution plan is divided into four phases, with an emphasis on validating market demand before investing heavily in blockchain infrastructure. This approach helps reduce financial risk and ensures the platform is being developed around a proven market need rather than assumptions about user adoption.

Phase	Timeline	Key Deliverables & Targets
Phase 1	Months 1-4	Conduct demand validation interviews with performance marketers; develop a no-blockchain browser extension prototype with 500 beta users; deploy smart contracts on the Solana devnet; launch the DVT token on testnet; obtain a legal opinion on token classification
Phase 2	Months 5-9	Launch invite-only Chrome extension beta targeting 5,000 users; release the web dashboard; secure 5-10 pilot company integrations; enable live DVT payments; complete a third-party smart contract security audit; target USD $10,000 in protocol fees
Phase 3	Months 10-15	Launch iOS and Android mobile applications; release Firefox and Safari extensions, onboard 50+ external validators, target 100,000 users, 200 companies, and USD $500,000 in annualized protocol revenue
Phase 4	Months 16-18	Launch DAO governance; expand into the European Union with GDPR compliance certification; support additional data categories; target 500,000 users and 1,000 participating companies

Table 3. *Development roadmap*

Competitive Differentiation

One of DataVault's biggest competitors is Brave, which is a browser that locally stores user data. This ranges from passwords and login information, to cookies, cache, and browsing history. Local storage being used over cloud is in order to prioritize user privacy and limit targeting. Brave has features like "forgetful browsing," which lets users clear browsing data automatically, as well as the option to manually manage and remove site data. Despite many strengths in the data storage sector, Brave lacks superior decentralization, trustless verification, and censorship resistance that blockchain can provide for users.

True decentralization found with blockchain enables users to make peer-to-peer transactions without one or more intermediaries, whereas Brave is a company-controlled browser which means there will always be the possibility of policy changes or regulatory restrictions impacting which entities end up monitoring or interacting with user data.

Another important distinction is that with DataVault, users own their data and information completely, but with Brave, users can earn Basic Attention Token (BAT) which remains managed through a browser-specific wallet (Brave Software, 2023). This is another centralized layer on top of what could be an entirely decentralized chain.

Lastly, blockchain is nearly impervious to censorship; a key reason behind why DataVault uses blockchain technology. However, the Brave Browser could be banned from app stores or forced to adapt to regional regulations, which would then affect the extent of autonomy users to have with their data.

Business Model

Revenue Streams

DataVault operates in a two-sided marketplace where the privacy and data management service is free for users, while revenue is generated from companies purchasing permission-based access to data. This model lowers barriers to user adoption and allows the platform to compete more effectively with free privacy tools already on the market. By keeping the service free, DataVault can grow its user base more quickly, which in turn increases the platform's value to companies and expands the volume of transactions from which the protocol earns fees.

- Data access protocol fees – DataVault retains 5% of every DVT transaction through an automatic smart contract deduction, eliminating the need for manual payment processing.
- Enterprise compliance application programming interface (API) – companies can subscribe to a monthly SaaS plan that provides GDPR audit reporting, compliance documentation, and high-volume API access, with pricing ranging from approximately USD $2,000 to $15,000 per month depending on usage tier.
- Validator staking fees – a portion of validator staking rewards is directed to the platform treasury to help support long-term network operations and development.

- Premium user tier – users may optionally subscribe for USD $4.99 per month to access enhanced earning analytics, priority consent matching, and early access to additional platform features and data categories.

Financial Projections

Year	Active Users	Companies	Avg Revenue per User (via DVT flow)	Protocol Fees	Enterprise API	Total Revenue (USD)
Year 1	5,000	5-10 pilot	$0.10 - $0.25	$10,000	$0	$15,000
Year 2	100,000	200	$0.40	$150,000	$200,000	$350,000
Year 3	500,000	1,000	$0.60	$600,000	$900,000	$1,500,000

Table 4. *Financial projections*

Challenges

Token Regulatory Risk

One of the biggest risks for DataVault is how the DVT token would be classified under U.S. securities law. Under the Howey Test, a token can be considered a security if people buy it expecting to profit from others' work. Because of this, DataVault would need to position DVT primarily as a utility token used within the platform rather than as an investment asset. To reduce legal risk, the company would work with a crypto-focused law firm early in development to get formal legal guidance.

Chicken-and-Egg Adoption

Like many marketplace platforms, DataVault faces the challenge of attracting both users and companies at the same time. Users will not want to join if there are no companies buying data, while companies will not be interested if there are not enough users on the platform. The address this issue, DataVault would try to secure pilot company partnerships before launching so that users can immediately begin earning DVT rewards. Referral programs, privacy-focused communities, and beta testing would also attract early users and build interest before the full launch.

Transaction Scale and Cost

DataVault could eventually process billions of consent transactions each year. If every transaction were written directly to the blockchain, the costs and processing requirements would become exceptionally large over time. To make the system more efficient, DataVault would use a method called batch hashing, where multiple consent events are grouped together before being recorded on chain. Individual transaction details would still be stored securely off chain, while the blockchain keeps a verifiable audit trail. This approach significantly reduces costs while still maintaining transparency and security.

User Experience Complexity

One major challenge is making the platform easy for average users to understand. Most people are not familiar with crypto wallets or blockchain technology, so the system needs to feel simple and user-friendly. DataVault's goal is to hide most of the technical blockchain processes behind a familiar interface that looks more like a regular banking or finance app. Users would simply see their earnings, consent settings, and account activity without needing advanced crypto knowledge. Creating this simple experience would be one of the most important parts of the platform's design.

Company Adoption Incentives

Another challenge is convincing companies to pay for data they currently collect for free through traditional tracking methods. However, increasing privacy regulations, restrictions on third-party cookies, and Apple's App Tracking Transparency policies are making older tracking systems less effective. DataVault would try to position itself as a compliant and transparent alternative that gives companies access to higher-quality, consent-based data. The platform would also use pilot campaigns and testing data to demonstrate that verified user data can improve advertising performance and customer targeting.

References

Brave Software. (2023). *Basic Attention Token ecosystem overview*. https://brave.com/bat

DLA Piper. (2024). *GDPR fines and enforcement tracker*. https://www.dlapiper.com

European Data Protection Board. (2024). *GDPR enforcement updates*. https://edpb.europa.eu

Ethereum Foundation. (2024). *Ethereum documentation and protocol updates*. https://ethereum.org

Forrester Research. (2024). *State of data deprecation report*. https://www.forrester.com

Google. (2025). *Privacy Sandbox updates*. https://privacysandbox.com

Interactive Advertising Bureau. (2024). *State of data report*. https://www.iab.com

Solana Labs. (2025). *Network and ecosystem documentation*. https://solana.com

Pew Research Center. (2023). *Americans and privacy: Concerned, confused and feeling lack of control over their personal data*. https://www.pewresearch.org