

VALIDECK

Search with Confidence

Mission & Vision

Vision:

Build the world's **privacy-first data layer** for global loyalty and payments, where every transaction is customer-controlled, **secure, and interoperable**.

***Long-term:** Embed ValiDeck's patented tokenization layer into every Point of Sale (PoS), powering a global privacy-first commerce network and the world's first search engine built on pseudonymous customer transaction records and reviews.*

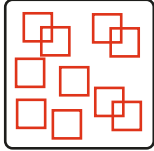
Mission:

Develop a privacy-first data layer that enables:

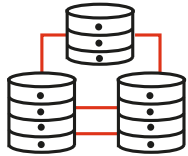
- **Customers** to capture and control their records in a secure cloud account, keyed to a customer-controlled pseudonym.
- **Businesses** to run privacy-compliant loyalty programs without collecting personal identifiers.
- **Enterprises** to access verified, privacy-protected data that improves decision-making and customer engagement.

***Current Focus:** building the reference implementation (a payment transaction simulator, PoS integration layer, and Loyalty Server) toward enterprise pilot readiness.*

Market / Problem



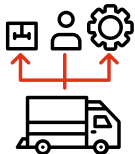
Customer transaction records are scattered and siloed. A few large merchants, such as Amazon, keep purchase histories in the customer's platform account; most businesses hand over a copy as an email or printed invoice. Every copy lives in a separate silo, tied to the customer's identity, in a format the customer cannot aggregate or reuse.



There is no practical infrastructure today for retaining and reusing transaction records without identity. Conventional anonymization of transaction data is easily re-identified, so in practice records are either deleted or kept in personally attributable form.



Customers cannot understand their spending habits, are unable to plan their purchases, and cannot profit from their own transaction data.

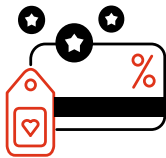


Businesses are unable to target customers efficiently, lack the necessary information to grow and expand their operations, and cannot run loyalty programs that encourage customers to pseudonymously share their transaction data.

Market / Problem



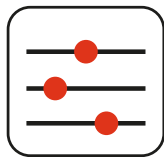
The loyalty management software market is estimated at USD 16.4 billion in 2026, projected to reach USD 32.5 billion by 2031 at a ~15% CAGR (Mordor Intelligence, 2026).



In the absence of a privacy-compliant model for reuse, merchants resort to identity-based loyalty programs to extract value from transaction data. These programs require customers to acquire a merchant-branded loyalty card or share their email/mobile number with the merchant during registration.



Existing merchant loyalty programs compromise the personal and confidential information of customers and expose them to security issues, such as identity theft.



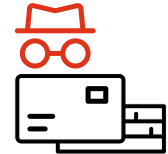
Loyalty programs also do not record crucial parameters about a product or service when they capture customer reviews.

Solution: PCX-based Loyalty Program



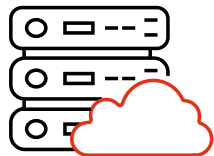
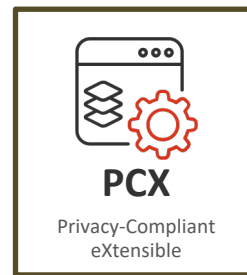
Protects

Personal and confidential information of customers



Allows

Customers to join unlimited loyalty programs pseudonymously



Stores

Line-item customer transaction records without personal identifiers



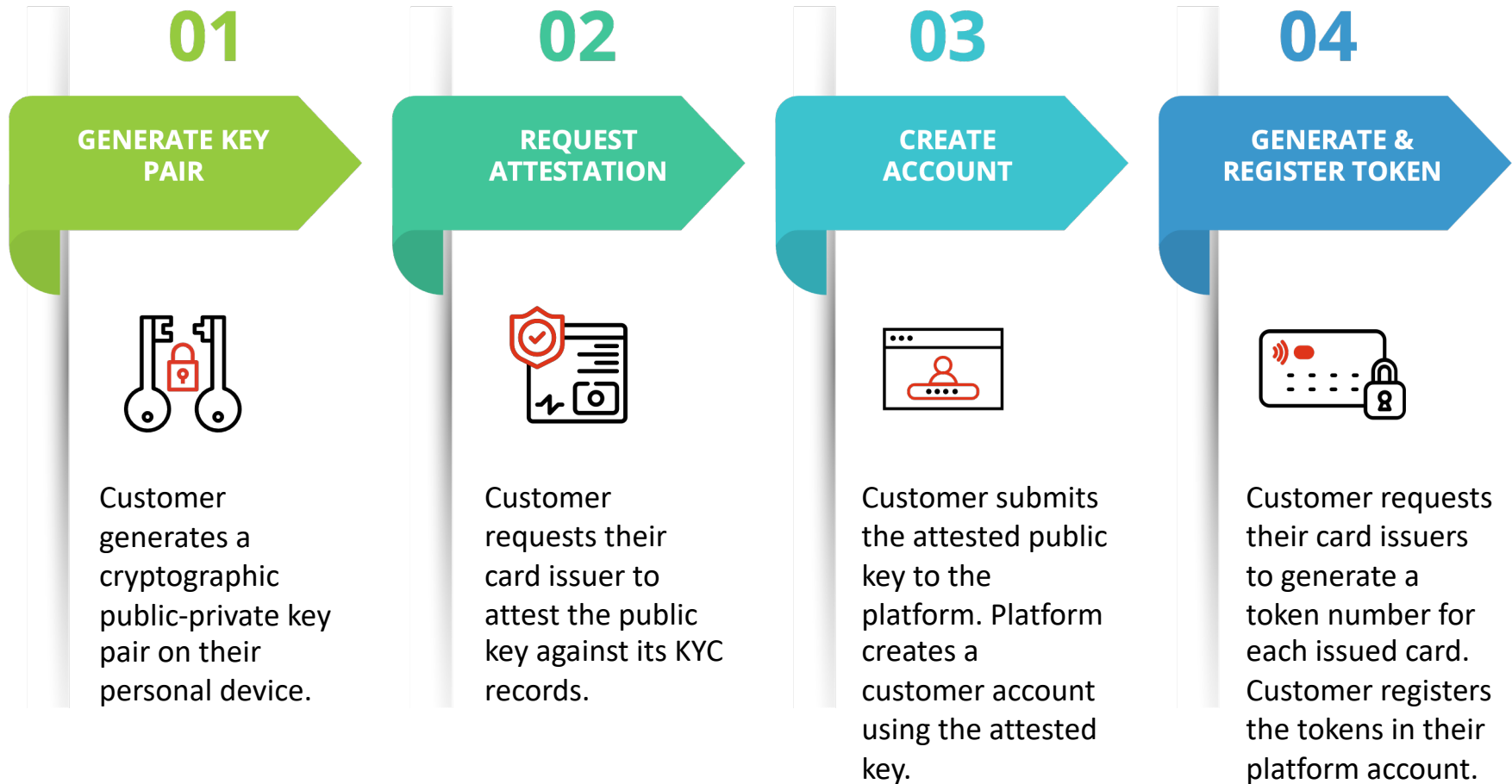
Unlocks

Cross-merchant spending insight (in development)

Note:

1. The PCX panel above links to the PCX White Paper, which describes the protocol in full. The underlying [tokenization technology](#) and the [PCX-based loyalty program](#) are documented in more detail on the ValiDeck website.
2. The core token pipeline is protected by a granted patent family: [US12125054B2](#), with corresponding grants in [Australia](#) and [India](#), and national-phase prosecution continuing in Canada, Europe, and China. The privacy-preserving record architecture built on that pipeline (pseudonymous enrollment, domain-separated records, and cross-merchant spend analytics) is covered by new applications filed in the US in 2026, currently pending.

Joining the PCX-based Loyalty Program



Note: The platform does not require the customer to disclose their personal and confidential information during account creation. No email ids, phone numbers, or payment card details are shared with the platform.

Running the PCX-based Loyalty Program

01

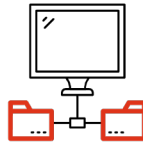
SHOP NORMALLY



Customer makes payment using any tokenized card. No loyalty card, app, or personal identifier is required at the point of sale.

02

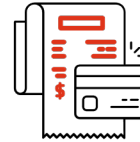
TRANSFORM CUSTOMER TRANSACTION



Merchant PoS links token with the transaction record and transmits both to the platform. The platform is built to transform the package into domain-specific records.

03

RECORD CUSTOMER TRANSACTION



Platform stores each domain record separately. No single database holds a complete transaction. Card tokens map to platform pseudonyms: the platform receives no direct identifier.

04

EARN REWARDS

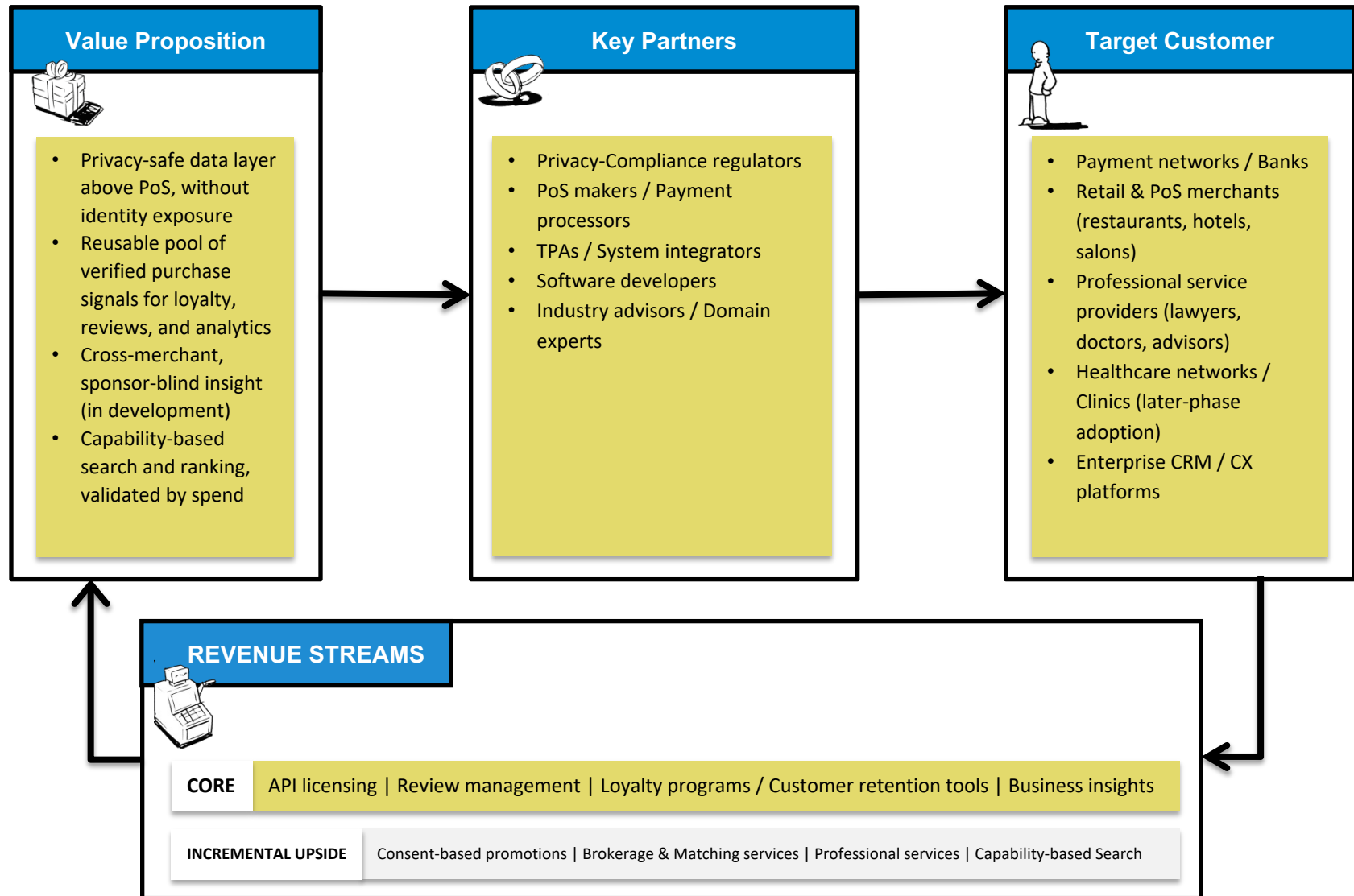


Enrolled merchants reward on their own and partner-network sales. Cross-merchant, sponsor-blind rewards run on synthetic records (in development).

Competitive Advantage

Feature	Fetch Rewards	Ibotta	Fidel API	ValiDeck (in development)
Pseudonymous Enrollment Note: A platform qualifies for the pseudonymous enrollment label if a customer can enroll and transact without disclosing personal identifiers (name, email, phone, or card number) with records linked to a customer-controlled pseudonym that persists across merchants rather than to a real-world identity.	No	No	No	Yes
Customer-controlled Data Aggregation Note: When a customer joins a merchant loyalty program, the transaction records are stored on the merchant's platform. A platform qualifies for this label only if the customer's copy of the record is under their control: portable, deletable, and not monetized without consent. Receipt-scanning apps that hold and monetize the customer's copy without that control do not qualify.	No	No	No	Yes
Sponsor-Blind Cross-Merchant Rewards Note: A merchant in a loyalty program sees a customer's spending only at its own store, or within a partner network. A platform qualifies for the sponsor-blind cross-merchant rewards label if a sponsor can reward purchases made at unaffiliated merchants, without ever seeing or singling out the customer.	No	No	No	Yes
Line-item Transaction Details Captured at the Payment Rail Note: To understand the exact spending behavior of the customer (e.g., \$100 on Nike sneakers), it is necessary to have access to line-item transaction details. A platform that allows customers to aggregate granular transaction details without using additional tools or methods has the line-item transaction details at the payment rail feature.	No	No	No	Yes

Business Model



Note: Information on revenue streams is described in more detail in the [product development strategy](#).

Team & Ask

Founder

Alok Narula – Product, IP, and System Architecture

LinkedIn: <https://www.linkedin.com/in/aloknarula>

Support

- IP Education and Funding: [Intellectual Property Ontario \(IPON\)](#)
- Talent Search, Networking Events, and IP Strategy: [Communitech](#)

Seeking: US\$1M Pre-Seed Round, deployed in staged tranches over 24 months to validate ValiDeck's granted and patent-pending architecture:

- \$700K – Engineering & Product Build
- \$200K – Partner Integration & Testing
- \$100K – Compliance & Operations

Outcome: PoC designed for PIPEDA/GDPR compliance and validated by independent privacy audit within 24 months → ready for enterprise pilots and seed scaling.

Non-Dilutive Funding: IPON Tier 2 client, eligible for up to **CAD \$300K lifetime** in cost-shared IP funding for patent prosecution, approved per statement of work.

SR&ED Eligibility: Development activities in Canada are expected to qualify for [federal reimbursement of eligible R&D expenses](#) (salary, equipment, subcontractors).

Phase I Roadmap & Milestones

1-6 Months

Platform Design

- Design encryption and tokenization architecture
- Build a virtual PoS Simulator for multi-merchant testing
- Implement secure enclave for privacy-preserving transaction processing



6-9 Months

Backend Development

- Implement Loyalty Server backend linking tokens with transaction records
- Automate encryption validation and performance benchmarking
- Prepare SR&ED technical narrative and evidence documentation



9-12 Months

Analytics & Compliance

- Deploy BI dashboard (Metabase/Superset) for cross-merchant analytics
- Complete PIPEDA / GDPR privacy audit and finalize SR&ED submission



12-24 Months

Reference Integration

- Finalize UI/UX and investor demo environment
- Build hardware-agnostic PoS SDK, validated against the transaction simulator
- Demonstrate GDPR-compliant tokenized transactions in a reference integration

