Institutional Pseudonymity in Decentralized Markets

Self-Custodied Trading, Public Settlement, and Identity Separation Across Layer-1 Blockchains

July 2026

Justin Belle

Abstract

The emergence of decentralized exchanges (DEXs) has introduced a fundamentally different model for participation in digital-asset markets. Unlike centralized exchanges, decentralized exchanges can permit market participants to trade directly from self-custodied blockchain addresses without maintaining a conventional custodial trading account with a centralized intermediary.

This architecture creates an important distinction between identity and activity.

A participant may have a legally identifiable institution, corporation, hedge fund, proprietary trading firm, family office or other organization in the real world while interacting with a decentralized exchange through blockchain addresses that do not inherently disclose the participant's legal identity.

This paper examines the concept of institutional pseudonymity in decentralized markets, particularly where institutions conduct substantial trading activity directly through decentralized exchanges without routing their trading accounts through centralized exchanges or custodial intermediaries.

The paper examines Bitcoin, Ethereum, Solana, Pecu Novus and comparable Layer-1 networks, and analyzes the relationship among:

- self-custody;
- decentralized exchanges;
- blockchain addresses;
- pseudonymous identities;
- institutional trading;
- high-frequency and algorithmic trading;
- public transaction records;
- blockchain analytics;
- identity attribution;

- centralized exchange exposure;
- decentralized settlement; and
- institutional privacy.

The paper argues that decentralized markets can provide a meaningful form of identity separation, the blockchain can publicly record what an address does without inherently revealing who controls that address.

However, this should be characterized as pseudonymity rather than anonymity. Blockchain transactions remain observable, traceable and potentially attributable. Once a real-world identity becomes associated with an address, historical activity associated with that address may also become attributable.

The resulting model is therefore not "anonymous finance." It is better described as:

> *Publicly verifiable financial activity conducted under a pseudonymous blockchain identity, without requiring continuous disclosure of the participant's legal identity to a centralized trading intermediary.*

1. Introduction

Traditional financial markets generally separate trading activity from public settlement through layers of regulated intermediaries.

An institutional trader typically establishes an account with:

- a bank;
- broker-dealer;
- prime broker;
- centralized exchange;
- custodian; or
- other financial intermediary.

The intermediary generally knows the identity of the customer and maintains records concerning:

- account ownership;
- beneficial ownership;
- trading activity;
- deposits and withdrawals;
- counterparties;
- compliance information;
- transaction history.

This structure provides important regulatory and operational functions, but it also creates a centralized repository of information about the participant.

Decentralized blockchain networks introduced a different architecture.

Bitcoin's original design proposed peer-to-peer transactions without requiring a trusted financial intermediary to maintain the transaction ledger. Transactions are publicly announced and recorded through network consensus.

The privacy model was not based on hiding transactions.

It was based on separating transactions from real-world identity.

That distinction remains foundational to decentralized financial markets.

2. The Difference Between Anonymity and Pseudonymity

This paper deliberately avoids using "anonymous" and "pseudonymous" interchangeably.

Anonymity

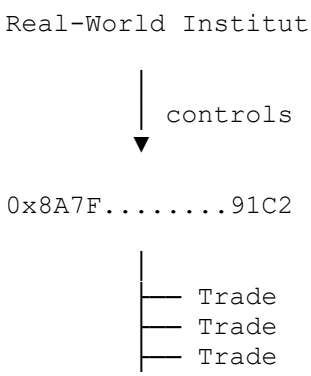
Anonymity implies that an individual's identity cannot reasonably be determined or associated with their activity.

Pseudonymity

Pseudonymity means that an individual or organization operates under an identifier that is different from its real-world identity.

Blockchain addresses are generally pseudonymous identifiers.

For example:



```
        ├── Liquidity provision
        └── Settlement
```

The blockchain can observe the address.

It does not inherently receive a field saying:

```
OWNER = BLACKROCK OR ABC CAPITAL MANAGEMENT, LLC
```

That separation is fundamental.

Bitcoin's original privacy discussion explicitly proposed keeping public keys anonymous while allowing transactions themselves to remain publicly observable.

3. The Centralized Exchange Identity Model

Consider a conventional digital-asset trading structure:

```
Institution
     │
     ▼
Centralized Exchange
     │
     ├── KYC
     ├── Legal Entity
     ├── Beneficial Owners
     ├── Trading Account
     ├── Deposit Records
     └── Withdrawal Records
              │
              ▼
         Blockchain
```

The centralized exchange establishes the identity relationship.

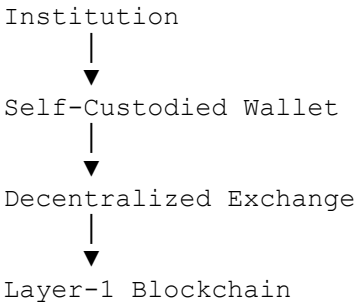
Consequently:

```
Blockchain Address
       ↓
Exchange Account
       ↓
Institution
```

can become a relatively straightforward attribution path.

4. The Decentralized Exchange Model

A decentralized exchange can remove that centralized identity bridge from the trading architecture:



There may be no centralized exchange account between the institution and the blockchain.

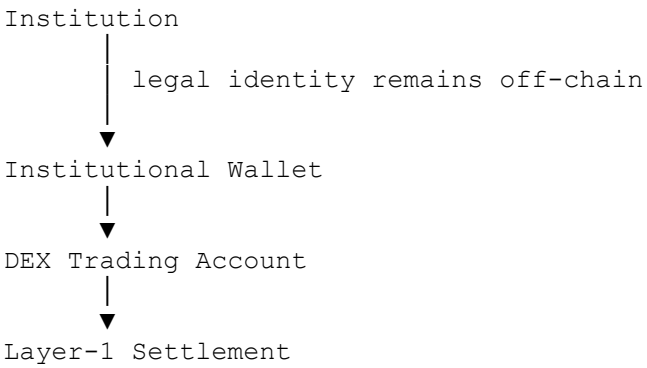
The DEX interacts with the blockchain address rather than necessarily requiring a conventional custodial account.

This is one of the fundamental architectural differences between centralized and decentralized markets.

The Bank for International Settlements has described DeFi as a form of financial intermediation based on blockchain protocols that seeks to reduce or eliminate traditional intermediaries.

5. The Institutional Pseudonymity Model

An institution could theoretically maintain:



The wallet address becomes the institution's market identity.

The blockchain knows:

> Wallet A traded Asset X against Asset Y.

It does not necessarily know:

> Wallet A belongs to Institution Z.

This distinction allows a decentralized market to maintain transparent market activity without necessarily publishing participant identity.

6. Bitcoin and Pseudonymity

Bitcoin established one of the foundational models for pseudonymous activity on a public blockchain. The Bitcoin protocol does not require the public ledger to contain the legal names of participants. Instead, transactions are associated with cryptographic addresses and publicly recorded on the blockchain.

The distinction between public transaction visibility and participant identity was explicitly contemplated in Bitcoin's original design. In its discussion of privacy, the Bitcoin white paper explains that while all transactions must be publicly announced, privacy can be maintained by separating public keys from real-world identities. Nakamoto compared this model to a securities-market "tape," where the public can observe the time and size of transactions without necessarily being told who the parties are.

The resulting architecture can be represented as:

```
Real-World Participant
        |
        | identity is not inherently encoded
        ▼
Public Key / Address
        |
        ▼
Bitcoin Transaction
        |
        ▼
Public Blockchain Ledger
```

The blockchain therefore records activity, rather than necessarily recording the identity behind that activity.

A Bitcoin transaction can reveal that a particular address transferred a particular amount to another

address at a particular point in time. It does not inherently contain a field identifying the beneficial owner as an individual, corporation, fund, institution, or other legal entity.

This creates the fundamental pseudonymous relationship:

> *The blockchain address is publicly identifiable; the person or organization controlling the address is not inherently identified by the protocol.*

This distinction was an important departure from traditional financial infrastructure. In a conventional banking environment, the account number is generally connected to a customer record maintained by a financial institution. In Bitcoin, the public ledger can expose the address and its transaction history without requiring the ledger itself to contain the corresponding legal identity.

Bitcoin therefore established an important principle for decentralized finance:

Public financial records do not necessarily require public disclosure of the identity of every participant.

6.1 Pseudonymity Rather Than Anonymity

Bitcoin's model should not, however, be characterized as absolute anonymity.

The Bitcoin white paper itself recognized that transactions could become linked when addresses or keys were reused and recommended the use of new key pairs to reduce the ability to associate transactions with a common owner.

Consequently, Bitcoin's privacy model is better described as **pseudonymity**.

A participant may operate through:

```
Address A
    │
    ├── Transaction 1
    ├── Transaction 2
    ├── Transaction 3
    └── Transaction 4
```

while the public may not initially know:

```
Address A = Institution X
```

However, if sufficient external information establishes that relationship, the activity associated with Address A can potentially become attributable to Institution X.

This creates a critical characteristic of blockchain pseudonymity:

The identity may be hidden from the ledger without the activity being hidden from the ledger.

That principle becomes increasingly important as blockchain networks evolve from simple payment systems into programmable financial markets.

7. Ethereum and Pseudonymous Programmable Finance

Ethereum expanded the concept of pseudonymous blockchain participation from peer-to-peer payments into programmable financial activity.

Where Bitcoin primarily established a decentralized transaction ledger, Ethereum introduced a general-purpose smart-contract environment in which programs and their associated state reside directly on the blockchain. Ethereum's documentation describes smart contracts as programs deployed to blockchain addresses that maintain code and data and can be interacted with by user accounts through transactions.

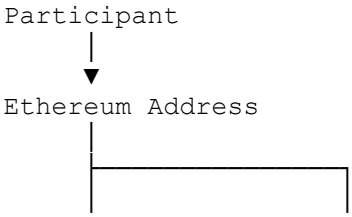
This creates a significantly broader pseudonymous activity surface.

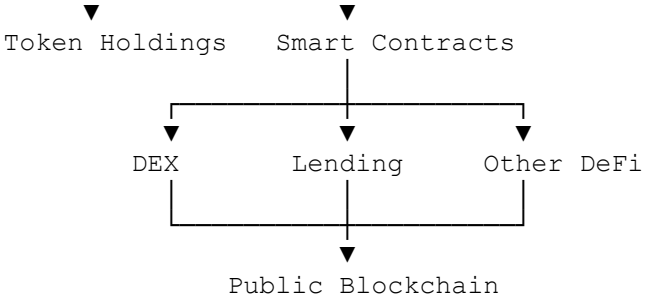
A participant can use a blockchain address to:

- hold digital assets;
- transfer assets;
- interact with smart contracts;
- provide liquidity;
- trade through decentralized exchanges;
- participate in decentralized applications;
- execute automated financial strategies;
- interact with tokenized assets;
- establish positions in decentralized financial protocols.

Ethereum transactions are cryptographically signed instructions initiated by accounts and used to change network state.

The resulting relationship can be represented as:





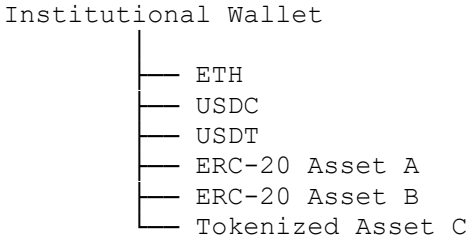
The address therefore becomes more than a payment identifier. It can function as a persistent pseudonymous financial identity.

7.1 ERC-20 Assets

The introduction and widespread adoption of ERC-20 token standards further expanded this model.

An Ethereum address can hold multiple assets without requiring the participant to establish a separate centralized account for every asset.

For example:



The public ledger can therefore reveal the address's holdings and interactions while the legal identity behind the address remains a separate question.

This is particularly relevant to institutional markets because the same pseudonymous address can participate in a broad range of financial activities without necessarily passing through a centralized exchange account.

7.2 Decentralized Exchanges

Ethereum's smart-contract architecture also enabled decentralized exchanges in which users can interact directly with trading contracts.

Instead of:

```
Institution
      ↓
Centralized Exchange
      ↓
Custodial Trading Account
      ↓
Blockchain
```

the participant can potentially use:

```
Institution
      ↓
Self-Custodied Wallet
      ↓
DEX Smart Contract
      ↓
Ethereum
```

The second model does not inherently provide anonymity. Rather, it changes the relationship between legal identity and trading identity.

The DEX can observe the wallet address and its activity. The blockchain can record the resulting transactions. The public can analyze those transactions. But neither the smart contract nor the blockchain protocol inherently requires the public ledger to contain the legal name of the institution controlling the address.

Ethereum itself now explicitly describes its public architecture in these terms: every address, balance, transaction, contract call and event is visible on-chain, while pseudonymity comes from activity being associated with public keys rather than directly with real-world identities. Ethereum also acknowledges that patterns of activity can potentially be analyzed to identify users.

This produces a fundamental characteristic of programmable blockchain finance:

> *Ethereum increases the amount and sophistication of activity that can be performed pseudonymously while simultaneously increasing the amount of information that can potentially be analyzed.*

8. Solana and Pseudonymous High-Throughput Activity

Solana extends the pseudonymous blockchain model into an architecture designed for high-performance decentralized execution.

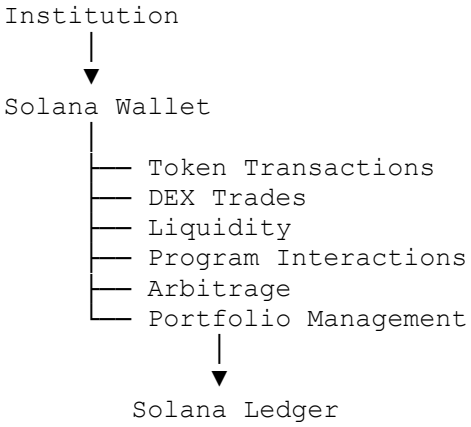
The significance of Solana to institutional pseudonymity is therefore not simply that participants can use blockchain addresses without publishing their legal identities. Bitcoin and Ethereum already established that principle.

Solana demonstrates how the same pseudonymous identity model can operate across a high-throughput execution environment capable of supporting substantial volumes of decentralized application activity.

Solana organizes network state through accounts and programs. Accounts are identified by 32-byte addresses, while programs contain executable logic. Transactions contain signatures, account addresses and instructions, and multiple instructions can be composed into a single transaction.

This architecture allows a participant's blockchain address to become a persistent pseudonymous identifier across a broad range of decentralized activity.

For example:



The institution's legal identity does not inherently become part of each transaction simply because the institution is conducting a large number of transactions.

8.1 Scale Changes the Meaning of Pseudonymous Activity

High-throughput infrastructure changes the potential scale of pseudonymous activity.

A participant that conducts a small number of transactions creates a relatively limited observable footprint.

An algorithmic trader or market maker can generate a much larger footprint:

```
Wallet A
    │
    ├── Trade
    ├── Trade
    ├── Trade
    ├── Liquidity adjustment
    ├── Trade
    ├── Arbitrage
    ├── Trade
    └── Settlement
```

The blockchain may therefore contain a highly detailed record of an entity's trading behavior without necessarily containing the entity's legal name.

This creates an important paradox:

> *Greater transaction throughput can increase both the utility of pseudonymous decentralized markets and the quantity of information available for blockchain analysis.*

The public can potentially observe:

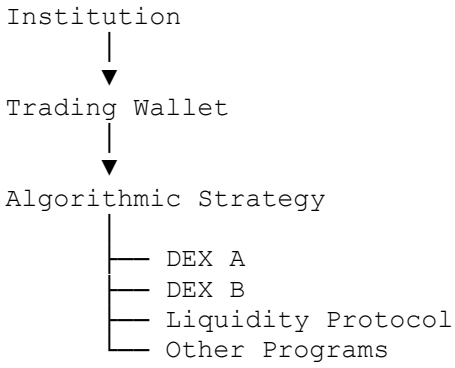
- transaction frequency;
- trading patterns;
- asset preferences;
- liquidity activity;
- timing;
- counterparties;
- program interactions;
- wallet balances;
- movement between addresses.

Yet the protocol does not inherently transform those observations into a legal identity.

8.2 Pseudonymity at Scale

For institutional markets, this distinction becomes particularly important.

An algorithmic trading organization may operate a dedicated wallet or set of wallets that function as its market identities:



The resulting activity is publicly observable and potentially analyzable, but the institution's legal identity remains a separate layer of information.

Solana's architecture therefore demonstrates how pseudonymity can extend beyond occasional transactions into continuous, high-volume decentralized financial activity.

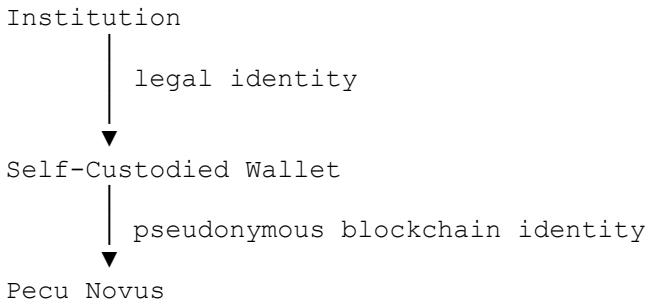
---

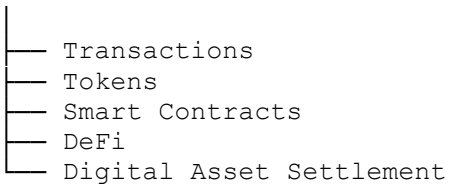
9. Pecu Novus and Pseudonymous Institutional Activity

Pecu Novus extends the public-blockchain pseudonymity model into a Layer-1 architecture designed to support high-volume digital-asset activity, smart contracts, tokenized assets and decentralized financial infrastructure.

As with Bitcoin, Ethereum and Solana, Pecu Novus transactions are associated with blockchain addresses rather than requiring the public ledger to contain the legal identity of the participant. Pecu Novus documentation describes transactions in terms of sender and recipient public addresses, with transactions cryptographically validated and subsequently recorded on the network ledger.

The resulting model is:





The significance of Pecu Novus in the context of institutional pseudonymity is its combination of a native Layer-1 network with modern interoperability and application infrastructure.

9.1 Native Layer-1 Identity

Pecu Novus maintains its own blockchain ledger and consensus infrastructure rather than functioning merely as an application deployed on another blockchain.

Its current Themis architecture uses a hybrid Proof-of-Time and Proof-of-Stake consensus mechanism. The Themis upgrade introduced this hybrid model, while subsequent development added broader interoperability with the Ethereum ecosystem.

This distinction is important because the pseudonymous identity exists at the Layer-1 level.

The participant is not simply anonymous to an application running on another blockchain.

The participant's blockchain address represents an identity directly within the Pecu Novus network.

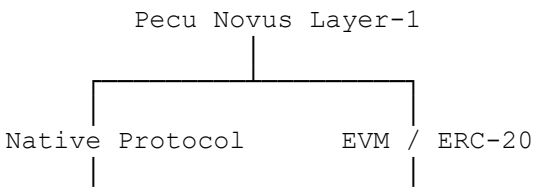
9.2 EVM and ERC-20 Compatibility

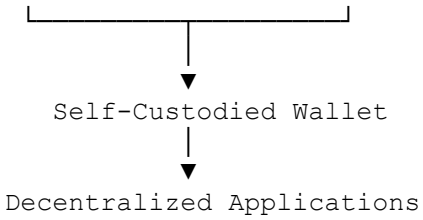
Pecu Novus has also introduced protocol-level EVM and ERC-20 compatibility. Its publicly documented RPC infrastructure allows Ethereum-compatible wallets, developer tools and decentralized applications to communicate with the network, while the network maintains its own underlying blockchain architecture.

This creates an important extension of the pseudonymity model.

A participant can interact with Pecu Novus using blockchain infrastructure familiar to the broader EVM ecosystem while maintaining a wallet identity within the Pecu Novus network.

The architecture can therefore be represented as:





The compatibility layer expands access to the network without changing the underlying principle:

> *The public blockchain address represents the participant's on-chain identity, while the legal identity behind that address remains a separate layer of information.*

9.3 Public RPC and Direct Network Participation

Pecu Novus' public RPC infrastructure is particularly relevant to this model.

Public RPC endpoints allow applications, wallets and other blockchain infrastructure to communicate directly with the Pecu Novus network. The network describes its RPC infrastructure as supporting its EVM-compatible environment and allowing standard Ethereum ecosystem infrastructure to connect to Pecu Novus.

This is important for pseudonymous institutional participation because it reduces the conceptual necessity of routing every interaction through a centralized portal.

The architecture can therefore be:

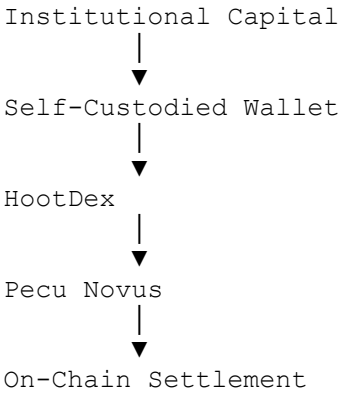
```
Institution
     |
     ▼
Self-Custodied Wallet
     |
     ▼
RPC / Decentralized Application
     |
     ▼
Pecu Novus Layer-1
     |
     ▼
Public Ledger
```

The participant can interact directly with decentralized infrastructure while maintaining control of the private keys associated with the wallet.

9.4 Institutional Trading Activity

This becomes particularly relevant when decentralized exchanges operate directly on Pecu Novus.

An institution can potentially maintain:



Under this model, the institution does not necessarily need to maintain a conventional custodial trading account at a centralized exchange.

The public blockchain can observe the wallet's:

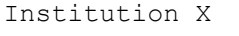
- trades;
- transfers;
- liquidity activity;
- smart-contract interactions;
- token balances;
- settlement activity;

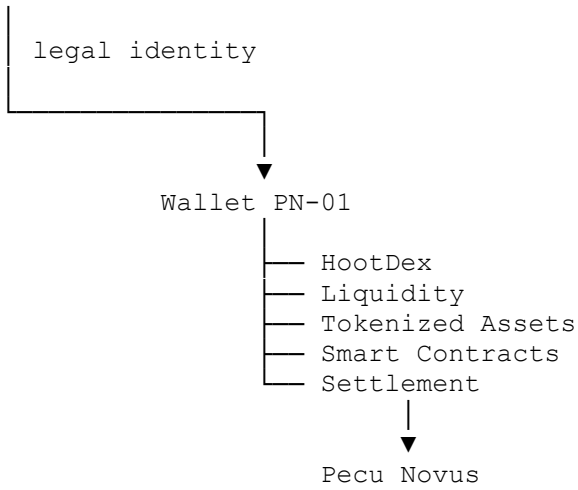
while the legal identity of the institution remains separate from the public blockchain address unless an external relationship establishes that identity.

9.5 Pseudonymous Institutional Market Identity

This creates the possibility of a persistent **institutional market identity** that is pseudonymous at the blockchain layer.

For example:





The public ledger can establish that `PN-01` performed those activities.

It does not inherently establish that:

```
PN-01 = Institution X
```

unless information outside the basic transaction record establishes that connection.

This is the central concept of institutional pseudonymity.

9.6 Public Transparency and Institutional Identity Separation

Pecu Novus therefore illustrates the same fundamental principle established by Bitcoin and subsequently expanded by Ethereum and Solana:

> *A public blockchain can provide transparent and independently verifiable financial activity without requiring the public ledger to directly publish the legal identity of every participant.*

The difference lies in the type and scale of activity supported by each network.

Bitcoin demonstrated pseudonymous peer-to-peer value transfer.

Ethereum expanded pseudonymity into programmable finance and smart-contract-based markets.

Solana demonstrated pseudonymous activity within a high-performance execution environment.

Pecu Novus extends the model through a Layer-1 architecture combining its hybrid Proof-of-

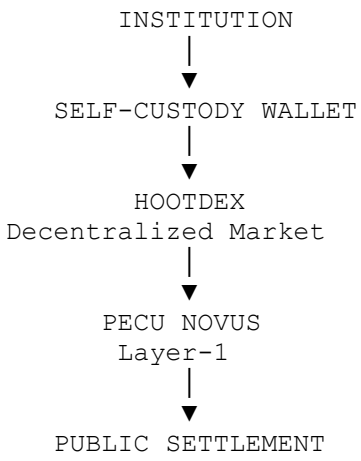
Time/Proof-of-Stake consensus, smart-contract infrastructure, public RPC access, and protocol-level EVM/ERC-20 compatibility.

In this context, Pecu Novus provides an additional example of how institutional financial activity can remain publicly verifiable at the blockchain level while the legal identity of the participant remains separate from the pseudonymous address used to conduct that activity.

9.7 The Role of HootDex

HootDex provides a practical decentralized-market application of this model.

The relationship is therefore deliberately hierarchical:



HootDex does not create the underlying pseudonymity.

The blockchain provides the pseudonymous identity layer.

HootDex provides the marketplace through which that pseudonymous identity can participate in decentralized trading.

Pecu Novus provides the Layer-1 settlement and consensus infrastructure on which those transactions are recorded.

This distinction is important to the overall thesis of the paper:

> *Pseudonymity is a property of the relationship between blockchain identity and real-world identity; decentralized exchanges are one of the principal financial applications through which that relationship can be utilized.*

10. Eliminating the Centralized Exchange Link

One of the most significant privacy benefits of this architecture is the elimination of unnecessary identity bridges.

Compare:

Centralized route

```
Institution
 ↓
KYC Exchange
 ↓
Custodial Account
 ↓
Withdrawal
 ↓
Blockchain
 ↓
DEX
```

with:

Decentralized route

```
Institution
 ↓
Self-Custody Wallet
 ↓
DEX
 ↓
Blockchain
```

The second model contains fewer centralized identity repositories.

That does not mean the participant is invisible.

It means fewer entities automatically possess the participant's complete identity-and-trading relationship.

11. Institutional High-Frequency Trading

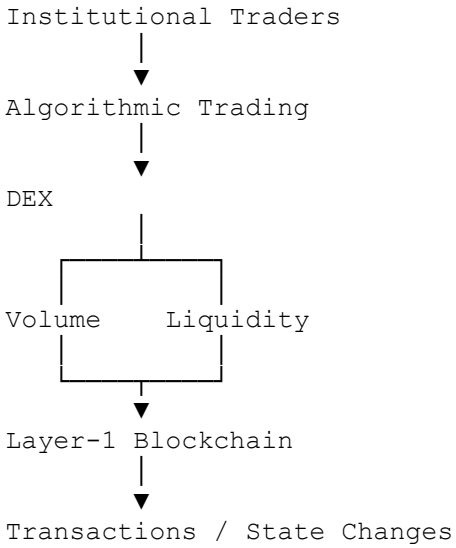
This becomes particularly interesting when applied to algorithmic and high-frequency trading.

An institutional trading operation may execute:

- thousands of orders;
- thousands of cancellations;
- arbitrage strategies;
- market-making transactions;
- liquidity adjustments;
- portfolio rebalancing;
- cross-asset trades.

If these activities settle on a public blockchain, they contribute to the economic activity of the underlying network and DEX.

Conceptually:



This can create a substantial increase in:

- DEX trading volume;
- liquidity;
- transaction activity;
- smart-contract interactions;
- settlement activity;
- on-chain asset movements.

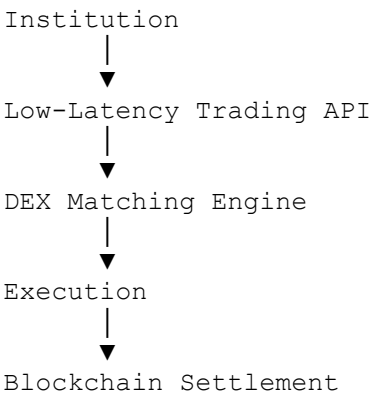
However, DEX volume should not be equated directly with Layer-1 transaction count. A trading venue

can batch operations, match orders off-chain and settle them on-chain, or otherwise structure execution so that one transaction represents multiple economic actions.

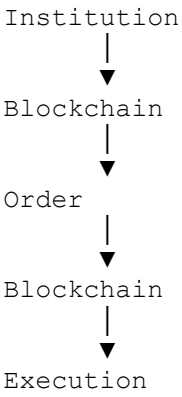
12. The Importance of the Trading Architecture

For genuine institutional HFT, putting every order event directly onto an L1 can be inefficient.

A more sophisticated architecture may be:



Rather than:



The first architecture can preserve decentralized custody and blockchain settlement while allowing the trading system to operate at much higher speeds.

This distinction is especially important when discussing HFT.

13. The Blockchain Becomes the Settlement Layer

Under this model, the Layer-1 blockchain does not necessarily need to function as the entire trading engine.

Instead, it provides:

Final settlement and verifiability.

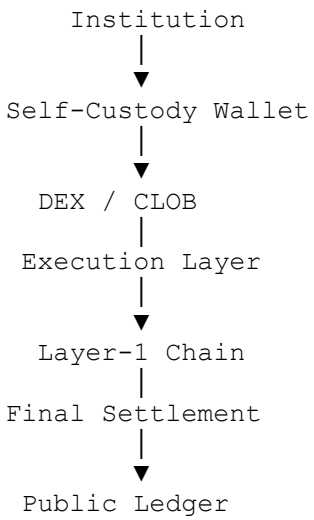
The DEX provides:

Market structure and execution.

The institution provides:

Capital and trading strategy.

The resulting architecture becomes:



14. The Institutional Privacy Trade-Off

The model produces an interesting balance:

Attribute	Centralized Exchange	Decentralized Exchange
Custody	Typically centralized	Self-custody possible
Legal identity	Known to exchange	Not inherently encoded in wallet
Trading history	Exchange-controlled	Publicly observable

Attribute	Centralized Exchange	Decentralized Exchange
Blockchain activity	May begin at withdrawal	Directly originates from wallet
Identity exposure	Direct to exchange	Potentially separated
Transparency	Exchange-dependent	Blockchain-dependent
Attribution risk	High once account identified	Possible through analytics
Counterparty transparency	Exchange controlled	Protocol/on-chain
Intermediary dependence	Higher	Lower

The DEX therefore does not eliminate surveillance or analysis.

It changes where identity information resides and how it becomes associated with trading activity.

15. The Deanonymization Problem

Institutional pseudonymity is only as strong as the separation between the wallet and the institution's identity.

Potential attribution mechanisms include:

Centralized exchange interaction

```
Wallet → KYC Exchange
```

Public disclosure

```
Institution announces:
"Our trading wallet is..."
```

Counterparty identification

```
Known Institution
        ↓
Known Wallet
        ↓
Related Wallets
```

Behavioral analysis

Repeated trading patterns can reveal relationships among addresses.

Academic research has specifically examined address clustering and the possibility of inferring relationships between Ethereum addresses and entities.

Therefore, a sophisticated institutional privacy architecture must treat wallet management itself as part of the identity boundary.

16. Pseudonymity Is Not a Compliance Exemption

This distinction should be explicit in the white paper.

Self-custody and pseudonymity do not eliminate:

- securities laws;
- commodities laws;
- AML obligations;
- sanctions requirements;
- tax obligations;
- beneficial ownership requirements;
- market-abuse restrictions;
- reporting requirements.

A blockchain address not containing a legal name does not mean an institution is legally entitled to conceal its identity from regulators or counterparties where disclosure is required.

The purpose of pseudonymity is better understood as:

> *Minimizing unnecessary public disclosure of identity while preserving cryptographic accountability and transaction verifiability.*

That is a much stronger institutional argument than claiming "anonymous trading."

17. A New Market Structure

The ultimate implication is that decentralized markets can create a third model between traditional anonymous trading and fully identified centralized accounts.

Traditional finance

```
Known participant
+
Private trading records
+
Centralized intermediary
```

Public blockchain

```
Unknown/pseudonymous participant
+
Public trading records
+
Decentralized settlement
```

Institutional decentralized market

```
Known legal participant
+
Pseudonymous market identity
+
Publicly verifiable settlement
+
Private legal identity
+
Regulated disclosure when required
```

This third model may be particularly relevant to institutional digital-asset markets.

18. The "Public Tape, Private Identity" Model

One of the most compelling concepts for this paper comes directly from Bitcoin's original privacy discussion.

The Bitcoin white paper compares its privacy model to securities-market disclosure where the time and size of trades can be public without necessarily identifying the parties.

That gives us a useful conceptual framework:

> Public tape. Private identity.

The blockchain can publish:

```
13:42:17
Asset: X
Quantity: 250,000
Price: $1.024
Wallet: 0x....
```

without publishing:

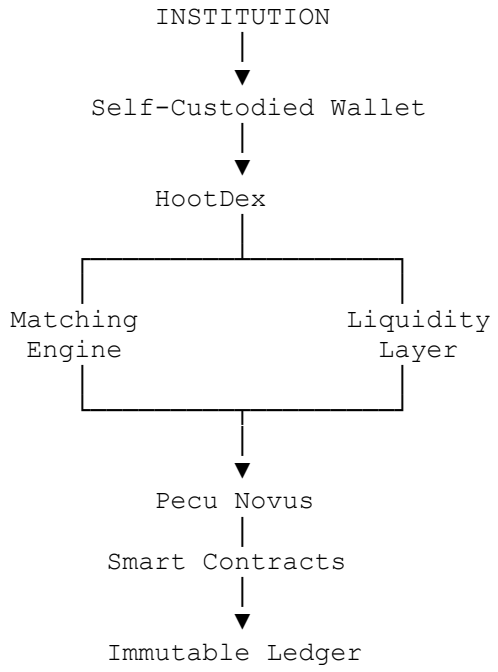
```
Beneficial Owner:
XYZ Capital Management
```

That is potentially a powerful design principle for decentralized institutional markets.

19. The HootDex / Pecu Novus Extension

This concept becomes particularly interesting when applied to the architecture for HootDex and Pecu Novus.

A model is:



The institution does not necessarily need:

```
Institution
    ↓
Centralized Exchange
    ↓
Withdrawal
```

```
    ↓
HootDex
```

Instead:

```
Institution
    ↓
Self-Custody
    ↓
HootDex
    ↓
Pecu Novus
```

This produces a fundamentally different institutional market structure.

20. The Data Consequence

There is another important consequence.

If institutional traders operate directly on a DEX, their economic activity becomes part of the DEX's observable market data.

For example:

```
Institution A
    ↓
Wallet A
    ↓
10,000 executions

Institution B
    ↓
Wallet B
    ↓
25,000 executions

Institution C
    ↓
Wallet C
    ↓
50,000 executions
```

The DEX can consequently experience substantial:

- volume;
- liquidity;
- order-book depth;
- transaction activity;
- price discovery;
- arbitrage;
- market-making;
- settlement.

And the underlying Layer-1 can experience increased smart-contract utilization and settlement activity.

This creates a feedback loop:

```
Institutional Participation
          ↓
Greater Liquidity
          ↓
Better Market Quality
          ↓
More Traders
          ↓
More Volume
          ↓
Greater Blockchain Utilization
          ↓
More Institutional Interest
```

21. Conclusion

Decentralized exchanges introduce a fundamentally different relationship between identity, trading activity and settlement.

An institution can possess a fully identifiable legal existence while interacting with a decentralized market through one or more pseudonymous blockchain addresses.

The blockchain can maintain an immutable record of:

- transactions;
- balances;
- execution;
- liquidity;
- smart-contract interactions;

- settlement;

without inherently storing the legal identity of the controlling institution.

This architecture does not create absolute anonymity.

Instead, it creates institutional pseudonymity.

The distinction is fundamental:

> *The blockchain can know what the wallet did without necessarily knowing who the wallet is.*

The absence of a centralized exchange can further reduce the number of points at which a legal identity is directly connected to a trading address. Nevertheless, blockchain analytics, wallet reuse, funding relationships, public disclosures, centralized counterparties and other forms of external information can potentially establish attribution.

Accordingly, the future of institutional decentralized markets should not be characterized as anonymous finance.

It should be characterized as:

> *transparent markets with pseudonymous participants, self-custodied capital, decentralized execution and publicly verifiable settlement.*

Selected References

1. **Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008)** — particularly the Transactions and Privacy sections. The original privacy model explicitly discusses keeping public keys anonymous while transactions remain publicly observable.
2. **Ethereum Foundation, "How to build privacy apps on Ethereum with zero-knowledge proofs" (2026)** — discusses Ethereum's intentionally public architecture and the visibility of addresses, balances, transactions, contract calls and events.
3. **Solana Foundation, "Core Concepts"** — documents Solana's account, program, instruction and transaction architecture and its public RPC infrastructure.
4. **Bank for International Settlements, "Cryptocurrencies and Decentralised Finance (DeFi)," BIS Working Paper No. 1061 (2022)** — examines decentralized finance, blockchain-based intermediation and the role of intermediaries in crypto markets.
5. **Reid & Harrigan, "An Analysis of Anonymity in the Bitcoin System"** — examines Bitcoin's public transaction graph and the implications for anonymity and address attribution.
6. **Biryukov, Khovratovich & Pustogarov, "Deanonymisation of Clients in Bitcoin P2P Network"** — examines network-level techniques that can potentially associate transactions with users.

7. **Wu et al., "Tutela: An Open-Source Tool for Assessing User-Privacy on Ethereum and Tornado Cash"** — examines Ethereum address clustering and the difference between pseudonymity and actual privacy.