



Blockchain and SDMX: Immutable data sharing for trust

SDMX Global Conference

Edward Lambe, Glenn Tice, Rafael Schmidt, Christian Schmieder (BIS) and Mario Rusev (d-fine)

Agenda

- Blockchain for Statistical Data Exchange
- Why Blockchain & SDMX Solves Real Problems
- Why now?
- Two Use Cases with Clear Business Value
- Implementation proposal
- Pilot implementation
- Discussion and feedback

Blockchain for Statistical Data Exchange

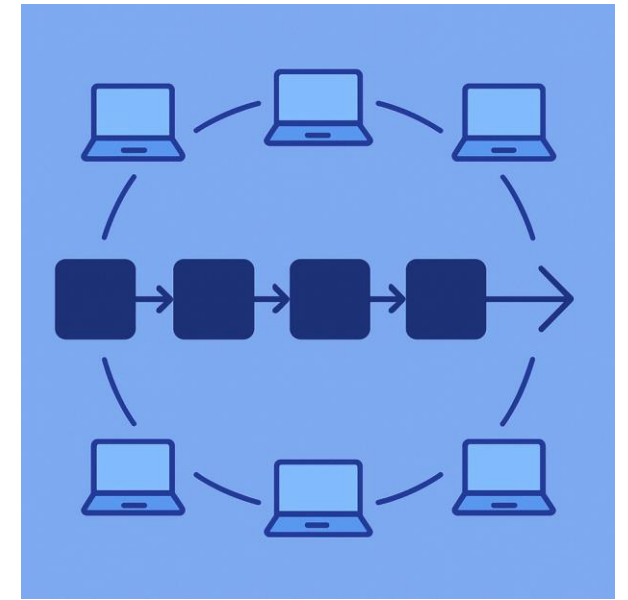
A blockchain is a decentralized, tamper-resistant digital ledger that chronologically records transactions in cryptographically linked “blocks” across a network of participants, ensuring security and transparency without relying on a central authority

Key Features:

- **Decentralization:** Eliminates single points of failure and control by distributing data
- **Transparency & Auditability:** Complete logged transaction history to participants, fostering trust
- **Security:** Data immutability and cryptographic hashing
- **Consensus Mechanisms:** Protocols like Proof-of-Work and Proof-of-Stake empower the network to validate new blocks collaboratively, ensuring unanimous agreement on a state without intermediaries
- **Common Use Cases:** Cryptocurrencies and Digital Assets, Smart Contracts, Supply Chain Management, Secure Record-Keeping

Benefits:

- Increased Trust, Enhanced Security, Traceability and Auditability, Greater Efficiency and Cost Reduction



Why Blockchain & SDMX Solves Real Problems

- **Builds Global Trust:**
 - Provides a ***transparent, cryptographically secure and verifiable record*** of official statistics, enhancing credibility globally
 - Strengthens international confidence through verifiably transparent data dissemination practices
- **Ensures Data Integrity:**
 - ***Guarantees immutability and reliability of statistics*** via cryptographic hashing and consensus mechanisms, establishing the foundation for **evidence-based policymaking**
 - Significantly mitigates risks of data manipulation and maintains high-quality standards
- **Promotes Interoperability via SDMX (*Verification Recommended*):**
 - Blockchain can inherently incorporate SDMX standards, facilitating effective, robust and standardized international data exchange.
 - Enhances **cross-system compatibility and data comparability** across global statistics
 - Allows **instant** data validation compared to legacy public key infrastructure



Why now?

- **Need for Evidence-Based Policy Making:**

- Policymakers depend critically on accurate, timely, and verifiably credible data to formulate robust and impactful decisions.
- Blockchain establishes an immutable chain of custody for data and metadata, guaranteeing authenticity and integrity and thereby creating a trusted foundation for mission-critical evidence-based policies.

- **Advances in AI and Machine Learning:**

- Modern AI/ML models can process and analyze massive, complex datasets faster than ever before.
- Blockchain serves as a critical enabler for trustworthy AI by providing a pipeline of high-fidelity, cryptographically assured data, significantly reducing the risks of bias, data poisoning and unreliable outputs in automated analysis.

- **Agent-Based Automation** (*Conceptual SDMX Integration Recommended*):

- The statistical ecosystem appears to be moving towards autonomous, agent-based systems for end-to-end data processing, validation, and dissemination.
- An SDMX-integrated blockchain architecture, could allow streamlining machine-executable workflows by natively embedding SDMX standards, ensuring efficiency, unwavering consistency, and verifiable reliability throughout the full data lifecycle.

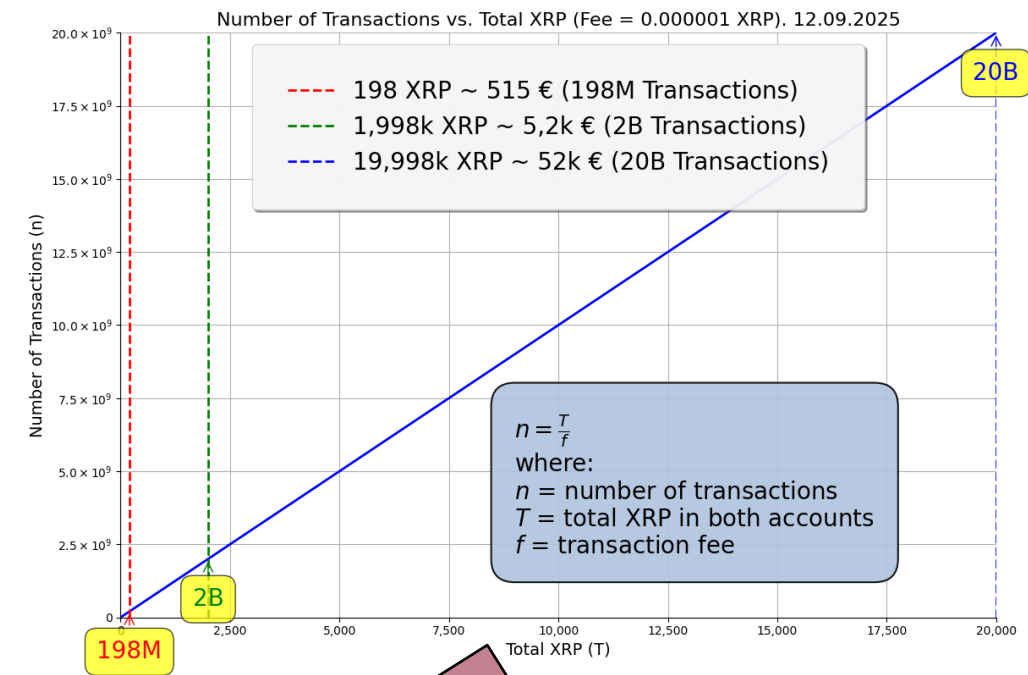
Two Use Cases with Clear Business Value

Two **sample** use cases to prevent the misuse of official statistics on unverified commercial or third-party platforms by cryptographically binding datasets to their origin:

- Use Case 1: **Immutable Version Authentication**
 - *Cryptographic Provenance*: Trace datasets unambiguously back to the official producer
 - *Immutable Audit Trail*: Record every version and modification with tamper-proof proofs
 - *Digital Signature Authentication*: Producers sign each dataset release, proving origin and integrity
 - *Real-Time Validation*: Enable end users to instantly verify the authenticity via lightweight cryptographic proofs
 - *Standards Alignment*: Support SDMX schemas and ensure GDPR compliance
- Use Case 2: **Redistribution Trust Framework**
 - *Portable Proofs*: Third-party platforms can bundle data with tamper-proof credentials
 - *Selective Disclosure*: Producers reveal only authorized fields via zero-knowledge proofs
 - *Blockchain Anchoring*: Immutable fingerprints of each dataset version are anchored to public blockchains
 - *Privacy-Preserving Revocation*: Manage credential revocations without revealing user identities

Associated costs – holdings and transaction capacity for our XRPL DevNet PoC

- Metainformation is written as a *memo*.
- Costs are kept at *minimum* by using two blockchain accounts, rotating sender/receiver if required, referencing only transaction fee (assuming full control of seeds).
- Possibilities to extend the PoC for smart contracts (*conditional transactions*) or NFTs (e.g. *ownership*), **inflation-linked products**, real-time markets, **transparent dashboards powered by immutable data**, perpetual futures markets, issuance of new types of digital assets etc.



Personal Measurements

Feature	Our Implementation	Chainlink Approach	Ethereum Approach	Legacy Public Key Infrastructure
Verification Time	Fixed < 5s (ts validation), < 2s (query)	seconds to minutes (ts validation) < 2s (query)	several minutes (ts validation) < 4s (query)	Hours to days
Transaction fee	~\$0.0000028	~\$2 to \$50	~\$0.50	~\$5.00 (Cert Authority cert)
Integration Complexity	Low (API-based)	Low (API-based)	Medium (custom integration required)	High (infrastructure)
Real-time Verification	Yes	Yes	Limited	No
SDMX Compliance	Full	Full (via metadata)	Variable	Variable

Local Tests + DevNet

Feature	Timing
Compute SHA3-512	~ 4 ms
Canonicalize XML bytes (C14N)	~15 ms
Total End-To-End Publication Time and GUI Response	~5-7 s
Total Processing Time for a validation	~1 s

Pilot implementation demo

Navigation

Publish SDMX

Validate SDMX

View Wallets

Manage Wallets

Login to Manage Wallets

Username

Password

Login

SDMX Publisher & Validator PoC on XRPL DevNet

Publish SDMX

Upload an SDMX file to publish (will anchor a hash on XRPL DevNet memo). We canonicalize the XML (C14N) and compute SHA3-512 then anchor it on the XRPL memo.

Upload SDMX file to publish

Drag and drop file here

Limit 200MB per file • XML

Browse files

TestMario1.xml

4.4KB

×

Publish

Required XRP to send (1.2 * 1e-05): 1.2e-05

Balances:

rKcFwICGQyZGvWDJRnZYRVWJyzRt6k45VZ: 100.00021 XRP

rBvesVLvcuZASmZCnyGkESYaypewjRF3Pr: 99.999769 XRP

Using source address: rBvesVLvcuZASmZCnyGkESYaypewjRF3Pr

Published — transaction hash: 05D31CAF6B3D0FC245E099225FAC044B1B6B3557FAC7677B2F0342D82BCE48EA

Navigation

Publish SDMX

Validate SDMX

View Wallets

Manage Wallets

Login to Manage Wallets

Username

Password

Login

SDMX Publisher & Validator PoC on XRPL DevNet

Published file (result from server)

Using source address: rBvesVLvcuZASmZCnyGkESYaypewjRF3Pr

Published — transaction hash: CAC5ECDAF24BDA16DF506CBC52E0261E34C582C02D5DDFEB34A8B745B25C858

Published file (result from server)

```
5 <ns0:Test>false</ns0:Test>
6 <ns0:Prepared>2025-07-31T11:36:52Z</ns0:Prepared>
7 <ns0:Sender id="UNKNOWN"/>
8 <ns0:Receiver id="guest"/>
9 <ns0:Structure structureID="BIS_WS_CBPOL_1_0" namespace="urn:sdmx:org.sdmx.infomodel.datastructure.Dataflow-BIS_WS_CBPOL(1.0):ObsLevel
10 <ns1:StructureUsage>
11 <Ref agencyID="BIS" id="WS_CBPOL" version="1.0"/>
12 </ns1:StructureUsage>
13 </ns0:Structure>
14 <ns0:DataSetAction>Information</ns0:DataSetAction>
15 <ns0:DataSetID>0efcb1b9-bfb2-4581-b993-858668c94cd2</ns0:DataSetID>
16 <ns0:Extracted>2025-07-31T11:36:52</ns0:Extracted>
17 <ns0:ReportingBegin>1945-01-01T00:00:00</ns0:ReportingBegin>
18 <ns0:ReportingEnd>2025-06-01T23:59:59</ns0:ReportingEnd>
19 <ns0:Source>Transaction Hash:CAC5ECDAF24BDA16DF506CBC52E0261E34C582C02D5DDFEB34A8B745B25C858</ns0:Source>
20 </ns0:DataSet>
21 <ns0:DataSet UNIT="0" UNIT_MEASURE="368" ns2:dataScope="DataStructure" xs1:type="ns1:DataSetType" ns2:structureRef="BIS_WS_CBPOL_1_0"/>
```

Download published XML

Navigation

Publish SDMX

Validate SDMX

View Wallets

Manage Wallets

Login to Manage Wallets

Username

Password

Login

SDMX Publisher & Validator PoC on XRPL DevNet

Validate SDMX

Upload a file to validate (canonicalize + SHA-3-512) against an on-chain transaction.

Upload an SDMX file to validate

Drag and drop file here

Limit 200MB per file • XML

Browse files

published_TestMario1 (3).xml

4.1KB

×

Validate

Validation result:

The file is valid.

Details: Transaction memo matches dataset hash (valid).

Navigation

Publish SDMX

Validate SDMX

View Wallets

Manage Wallets

Login to Manage Wallets

Username

Password

Login

SDMX Publisher & Validator PoC on XRPL DevNet

Validate SDMX

Upload a file to validate (canonicalize + SHA-3-512) against an on-chain transaction.

Upload an SDMX file to validate

Drag and drop file here

Limit 200MB per file • XML

Browse files

published_TestMario1 (2).xml

3.2KB

×

Validate

Validation result:

The file is NOT valid.

Details: Memo mismatch: on-chain memo
11A82815C05B2213973C801D56C498C2D58FC4E8EFF1CC2034237D564E127933E8E440E077D6891F871821A3668294C96F893A574369092551F8672C5825AA3 != computed dataset
hash CB85287294D2F4EB765722444DE477D88AD6D365F74A382290495B8322A49702E0EBD85B08944148D781C9EAB0697790313C42DEF707B6266243D253080D7

8

Discussion and feedback

- **Relevance and Priority**

- Do you see a real need for authenticating SDMX data through blockchain in your institutional context?
- Where do you rank this use case compared to other SDMX innovations?

- **Feasibility and Adoption**

- What technical or organizational barriers would your institution face in adopting blockchain for data dissemination?
- Would a decentralized validation model improve your trust in redistributed data?

- **Collaboration and Governance**

- Which actors (e.g., NGOs, international organizations, private vendors) should maintain and govern the blockchain infrastructure or use a public blockchain?
- Would embedding digital signatures or metadata hashes in SDMX messages be practical or too complex?

- **User Perspective and Trust**

- Would authenticated data from third-party platforms increase public trust in official statistics?
- How do you imagine users (e.g., journalists, researchers, businesses) would engage with blockchain-authenticated data?

Data trust survey

- Where do the threats lie?
- What technical options are preferred?
- What are the benefits of cryptographically verifiable data?
- Granularity of trust. Dataset, series, observation levels?
- Where does data trust figure in your organisational priorities?

Self-paced survey open until **October 9**

<https://app.sli.do/event/jRrnP8ak2RNewFCkbEeouF>

