PostgresBC

The OmniIndex Web3 Data Platform
with Native AI Analytics of Encrypted Data

OmniIndex

Simon Bain

The Headline

PostgresBC is an award-winning web3 data platform created by OmniIndex. It is a postgres fork providing enhanced data security and productivity.

What’s it for?

PostgresBC is available to customers as a stand-alone Web3 data platform to replace their PostgreSQL database. It provides enhanced security and compliance for data management, as well as powerful AI productivity through its native SLM and ability to work with fully encrypted data all of the time.

It is also the data platform for OmniIndex’s other secure solutions. Including the Dropblock File Store.

OmniIndex

Introduction:
What is Postgres?

PostgreSQL is an open-source relational database management system (RDBMS) that stores data in tables with defined relationships. This allows for efficient storage, retrieval, and analysis of complex data. The system enforces data integrity through foreign keys and reduces redundancy by referencing existing data. Additionally, PostgreSQL offers robust security features like access control, data encryption, and auditing to safeguard sensitive information.

PostgreSQL has a large and varied user base, including industry giants and small businesses alike. Stack Overflow's developer survey further highlights this popularity, with nearly half (45%) of over 90,000 respondents reporting PostgreSQL use compared to 41% for MySQL.

What's more, because it is open source it is primed for innovation with developers able to build on the established strengths of the database to add their own advancements and bring out their own versions.

OmniIndex

What is the PostgresBC Fork?

OmniIndex

PostgresBC uses the same tables and data structure as outlined in postgres, however data is stored within a chain in the database. This provides a number of security and privacy benefits for data due to its immutable nature and the decentralized storage.

Recorded data is stored as a trusted block and cannot be changed. While this places a constriction on this aspect of data management, it also protects the data from ransomware attacks and corruption as once the data is stored it cannot be changed or overwritten with an attacker's own encryption key.

Other differences include PostgresBC's native SLM AI (Small Language Model) and the ability to search and perform computations on encrypted data in real-time, as well as semantic search.

The below table shows the key differences between PostgresBC and PostgreSQL:

Functionality	PostgreSQL	PostgresBC
Read/Write	Yes	Yes
Modify Data	Yes	No (on the block data)
Multi-Node Replication	No	Yes
Multi-Node Cluster Support	No	Yes
Peer to Peer Clustering	No	Yes
AI Support Out of the box	No	Yes
ML Support out of the box	No	Yes
Extensibility	Yes	Yes
Full SQL Support	Yes	Yes
Record Level Encryption Without Administrator Access	No	Yes
Search on Encrypted Data	No	Yes

OmniIndex

Key Features of PostgresBC

OmniIndex

Blockchain Storage

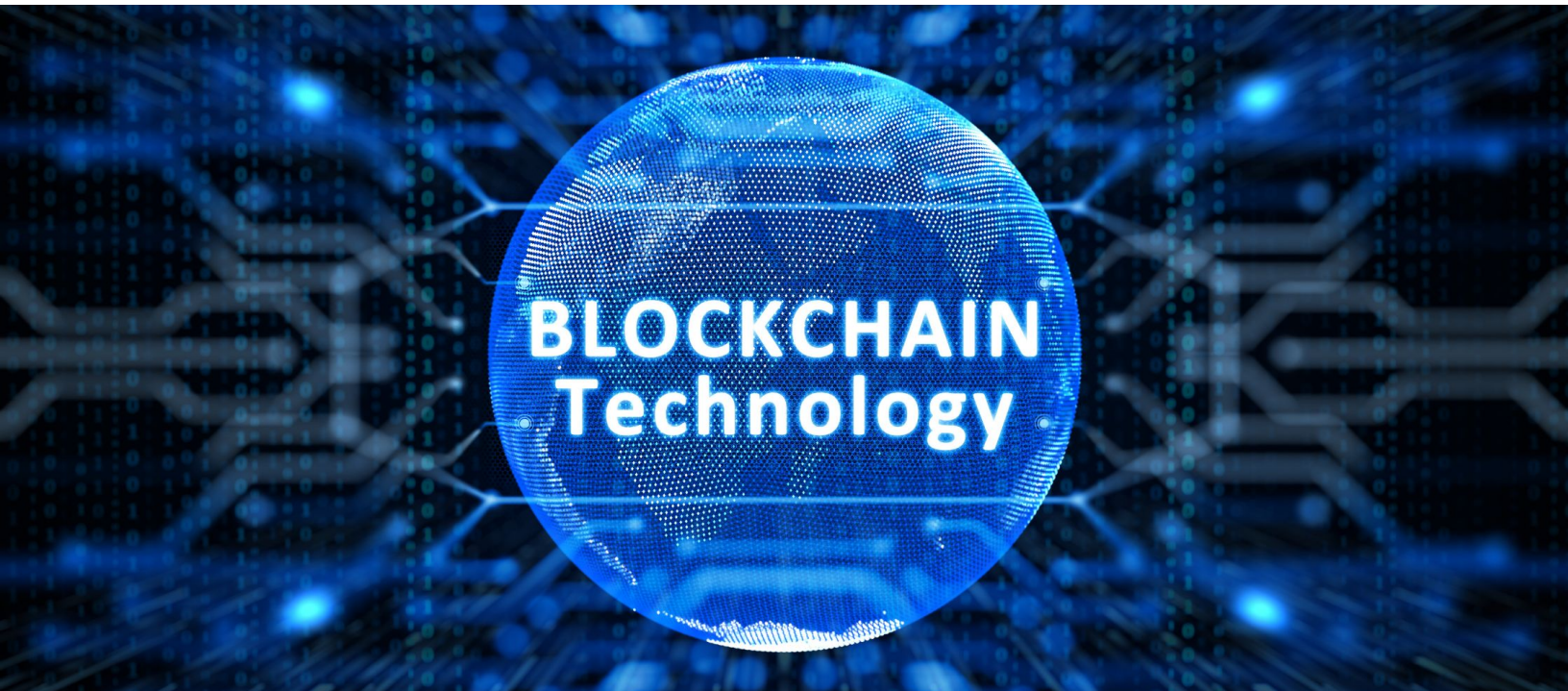
PostgresBC is a web3 data store with all data stored on the user's own blockchain. This is fully integrated into the system with users able to create new blocks and manage their blockchain data through basic SQL commands. For example: CREATE BLOCK <instancename>.<new block name> (stuff).

The security and privacy benefits of blockchain storage over traditional cloud and on-premises storage revolve around the enhanced integrity of the data with it being tamperproof, and the decentralization of the network making it more difficult to attack.

Immutable data: Data cannot be modified once it is stored. This means it cannot be corrupted or held to ransom because an attacker cannot overwrite data with their own encryption.

Decentralized storage: This, along with strong cryptography, significantly hinders attack attempts as there's no single point of vulnerability.

What's more, if a node in the decentralized network is somehow compromised, data can be recovered instantly by accessing one of the other nodes with zero data loss or disruption.



OmniIndex

Fully Homomorphic Encryption

OmniIndex's patented fully homomorphic encryption provides the only commercial solution for searching and performing computations on fully encrypted data.

It is based on Synchronous AES 256 using the CryptoPP libraries which are deemed uncrackable through brute-force attacks.

This means data does not have to be decrypted and left vulnerable to exposure through accidental or deliberate actions.

For example, Cross River State in Nigeria is using PostgresBC and this technology to keep the personally identifiable information of students protected and private while still being able to gain insights into educational outcomes across the institutions.

It is also a core technology in Dropblock's threat and compliance intelligence for secure file storage. This is because it enables authorized users to analyze their fully encrypted log files to identify vulnerabilities and breaches, as well as to predict potential attacks and compliance issues.

> "The problem with encrypted data is that you must decrypt it in order to work with it. By doing so, it's vulnerable to the very things you were trying to protect it from by encrypting it.
>
> There is a powerful solution to this scenario: homomorphic encryption."

FORBES

OmniIndex

Native AI

Boudica is an SLM (Small Language Model) AI engine empowering users to gain insights on their encrypted data without any data ever being exposed or shared externally. This private AI engine has a number of direct benefits for users.

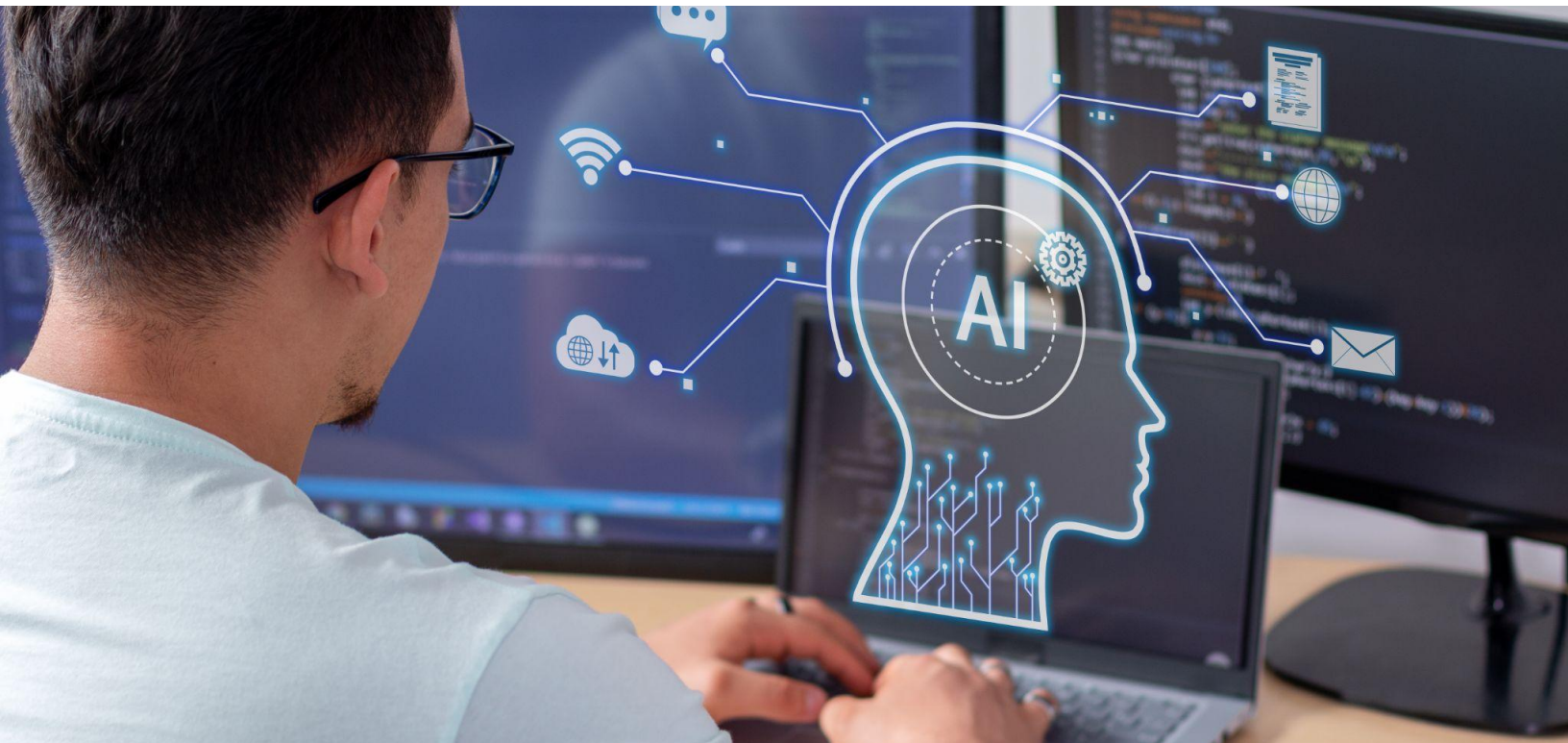
1: Privacy
Boudica is a private and native AI solution. This means user data is not shared externally of the system to generate answers, and there is no third-party access to the user's queries or answers.

Finally, all data is encrypted while it is being subjected to AI analytics.

2: Accuracy
SLMs like Boudica only work on small pools of controlled data that they are supplied with and are therefore far less likely to contain biases and inaccuracies than LLMs which learn from huge pools of varied data.

Boudica's use of multiple separate thesaurus models and its probability matrices also ensure that only the optimum response is given to a user.

3: Efficient & Optimized
SLMs do not require extensive training on huge pools of data in order to be used and can be adapted to offer specialist services in different languages and areas simply by changing their ontologies. They also require less powerful hardware to run.



The only way to safely utilize vulnerable and confidential data is to use a data platform that protects that data from attack, and enables it to be analyzed in a fully encrypted state with no third-party access and no risk of exposure.

OmniIndex's PostgresBC is the only commercial solution that makes this possible.

www.omniindex.io
info@omniindex.io
+1 (650) 297-4682