kx | it's about time

How Cobalt Leverages Kx and Blockchain-Inspired Technology for FX Post-Trade Processing

A Discussion of Blockchain Capabilities for Financial Markets Applications and Hybrid Architectures to Boost Performance

Contents

1. Introduction

This white paper provides an overview of how Kx technology is being implemented alongside blockchain-inspired data immutability functionality to underpin a new service that is set to dramatically reduce costs and risks in the global foreign exchange trading markets.

Cobalt provides post-trade processing services for the evolving FX marketplace, with a focus on increasing efficiency and reducing risk and costs. The company was formed in 2015 with backing from multiple financial markets participants. Its service has been in live operation since mid-2018.

Existing FX post-trade infrastructure was designed and built to service the low-volume, high-touch trading market that emerged following the abandonment of the Bretton Woods agreement in the early 1970s. Transactions were negotiated and completed using voice communications or rudimentary electronic messaging systems, beginning with the Reuter Monitor Dealing Service from 1981.

Since then, trade volumes have grown significantly as electronic matching and algorithmic trading systems have been introduced and widely adopted. At the same time, marketplace execution latencies have dropped to milliseconds or less. Today, trade volume is in excess of $5 Trillion daily, although profit margins in markets such as spot currencies are much reduced.

While execution technology has become increasingly high performance, post-trade processing systems (handling trade confirmation through settlement) have failed to keep up. Because of their inefficiency, risk is increased while rising operational costs are having a serious impact on the profitability of trading.

The replication of trade records in post-trade systems is a key drawback of existing post-trade systems. A single execution leads to multiple trade records for buyers, sellers, brokers, clearers and other participants, and inconsistencies between them are commonplace.

As a result, processes such as affirmation, confirmation, netting and settlement fail, requiring costly and time consuming human intervention to identify and rectify. Cobalt estimates that using its service can reduce such costs by up to 80%.

To achieve this, Cobalt links directly into multiple banks and electronic execution venues and provides its market participant customers with a mechanism for reconciling trade reports, creating a single, shared ledger to record them and allowing for later confirmation that these reconciliations have not changed.

Cobalt's service is inspired by blockchain technology, which is best known as the platform that underpins the bitcoin cryptocurrency. In addition to reconciling trades between two parties, it guarantees that a record of the reconciled trade is held in an immutable form.

As such, banks and other financial participants can rely on Cobalt-reconciled trade records for settlement and other post-trade services, including analytics, risk management and regulatory reporting.

Kx technology, including elements of its Kx for Flow *(see figure 1 below)* foreign exchange trading platform, forms a key component of Cobalt's service – underpinning the reconciliation of trade reports, calculation of cryptographic hashes that are fundamental to ensuring the integrity of trade records, and maintaining the ledger of reconciled trades in its kdb+ database.

Immutability is provided by augmenting the Kx software components with Cobalt's Babylon Network service. Drawing on blockchain technology concepts, Babylon provides a secure, scalable and high performance storage and verification mechanism for cryptographic hashes.

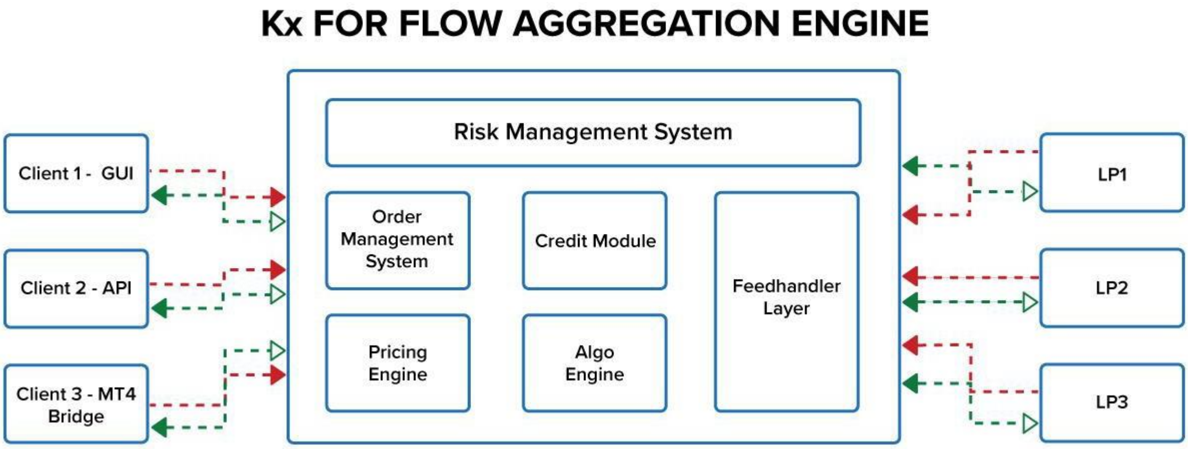

Figure 1 – Kx for Flow Aggregation Engine

2. The promise of Blockchain for the financial markets

Participants in the financial markets have been eager to experiment with blockchain technology, kicking off many proof-of-concept projects, some of which have shown enough promise to evolve into limited production pilots.

Blockchain platforms have been developed for commercial sale by a large number of companies, from IT giants like IBM and Fujitsu, to startups including Axoni, Chain, Digital Asset Holdings, R3 and SETL. In addition, open source platforms, such as Ethereum and Quorum (a development led by JPMorgan Chase) have received much focus.

In general, early financial markets PoCs sought to determine what functionality aspects of blockchain technology might be leveraged for applications. In particular, interest focused on:

* The data immutability offered by blockchains, as it is virtually impossible (given currently available computers) to modify or delete data stored within them. As such, blockchains can be thought of as tamper proof, append-only data stores.

* The shared and distributed nature of blockchains, whereby all participants have access to the same data store, which is automatically replicated across network nodes for security and resilience.

* The concepts of consensus and decentralization, establishing rules and technical processes that allow blockchains to be updated by multiple parties, without centralized control (or potential censorship). This includes the implementation of an agreed governance framework (known as consensus), and mechanisms to prevent centralization of control by nefarious participants.

Some financial applications require all the functionality provided by blockchain. The bitcoin cryptocurrency is the best known example, drawing on the entire functionality of its (open and public) blockchain platform to support the secure peer to peer transfer of value between two participants that have no existing relationship, and with no central intermediary to provide trust between the participants.

However, for many use cases that exist today in the financial markets, leveraging just a subset of a blockchain platform’s capabilities is sufficient to deliver the desired application functionality.

This is an important design issue. In general, limiting the use of blockchain functionality required by an application allows for higher performance. Consensus functionality in particular is expensive in terms of the compute resources it requires and tends to limit the performance of blockchain-based applications.

Following on from early PoCs, the focus evolved to rolling out pilots that demonstrated how blockchain technology might underpin existing financial applications, in both the institutional and retail/consumer markets.

Within the institutional space, the driver for the most part has been to reduce costs through efficiencies that the shared ledger and immutability of blockchains readily support.

In some instances, this has led to the implementation of so-called private blockchain platforms by consortia of banks and other financial players (that are known to one another and have existing business relationships), with some limited use of consensus capabilities.

Today, a number of blockchain pilots are being implemented in live production environments, albeit in limited rollouts. Examples of applications that are in production or showing promise as pilots are highlighted in table 1 below.

Blockchain Application	Example Production or Pilot Usage
Syndicated loans	Finastra's Fusion Lendercomm, using R3's Corda platform. Synaps (Ipreo, Symbiont JV), Credit Suisse.
Equities issuance and settlement	Nasdaq Private Market with Chain. Bolsa Italiano, working with IBM. Australian Securities Exchange, with Digital Asset Holdings.
Repo processing	DTCC with Digital Asset Holdings. Broadridge with Natixis and Societe Generale.
Reference data management	Credit Suisse working with Axoni. TruSet (a unit of ConsenSys).
Trade finance	IBM working with various bank consortia – Batavia, we.trade, and with shipping operator Maersk.

Table 1 – Applications of blockchain in production or pilot usage.

As promising pilots are evolving to production deployments, the utility of blockchain technology in the financial markets is becoming increasingly understood and appreciated.

At the same time, the performance and capabilities of traditional blockchain platforms are improving as the result of R&D by IT majors and industry consortia (such as the Linux Foundation's Hyperledger initiative and the Enterprise Ethereum Alliance). But performance in particular is a work in progress, and is currently a common challenge to deploying blockchains in the financial markets.

3. Blockchain shortcomings and the need for Babylon

Despite the very real promise of blockchain technology in the financial markets, there remain a number of business, operational, regulatory and technical reasons why its adoption is challenging and will take considerable time.

Like many new technologies that have been labeled as transformational, the capabilities and applicability of blockchain technology has been overstated by some, including major IT vendors and consulting companies.

Blockchain is not a "magic bullet" solution to every existing problem, although in many cases its implementation might be desirable as part of a new business or technology approach.

A case in point is reconciliations as part of post-trade processing in the financial markets. Industry pundits, consulting firms and vendors often suggest that simply implementing a blockchain (with its shared ledger) can eliminate the requirement for the reconciliation process (which is costly and laborious).

This is a falsehood. In general, a blockchain cannot in itself accept multiple trade inputs, compare them, match them and create a single reconciled trade record. This process requires reconciliation processing to be performed before the (reconciled) trade record is stored in the blockchain, which will then ensure that the record is not changed or tampered with.

Compliance with regulations and corporate data privacy policies can limit what data a financial markets participant can store in a shared environment, even if it is encrypted. This impacts the usage of the shared ledger aspect of blockchains, and may limit what data can actually be stored within them.

The introduction of the General Data Protection Regulation (GDPR) in the European Union is also likely to impact how blockchains are implemented. GDPR mandates that an individual can insist data is removed from a third party data store, which is highly problematic if it is stored in an immutable blockchain.

Even when regulations and privacy policies allow data to be stored within a blockchain, technical considerations can impact their use. Because of their distributed design, the requirement to replicate data stores and their append-only data model, the practical data capacity of blockchains is low, compared to conventional databases.

Moreover, the consensus mechanisms that are required to support updates from multiple participants (even in private blockchains where the participants are known to one another) impose significant processing overhead on a blockchain's ability to support high update rates.

Another drawback of traditional blockchain platforms is that they tend to make use of simple data storage mechanisms – often binary objects stored in a flat file – in order to boost performance. Storing data in this way makes it very difficult to leverage it for subsequent analytics and transaction processing.

As a result of the performance shortcomings of commercially available blockchain platforms, as well as the regulatory requirement for market participants to keep data stored within their own enterprises, Cobalt has designed and built Babylon as a proprietary technology architecture to underpin its service.

Inspired by blockchain concepts, Babylon provides very high performance and security with a focus on ensuring the immutability of data sets.

The Babylon service comprises a global network of servers, connected via BT Radianz's high performance broadcast network, which combine to provide a high performance, scalable and secure network layer. Servers are typically hosted in premium grade data centers, such as those operated by Equinix.

Babylon services are accessed by applications via a range of application programming interfaces and also via a web-based interface.

For security and resilience, data within Babylon is replicated across servers, using a patent-pending architecture known as BlockMatrix. Connections between servers use highly efficient UDP broadcast communications protocols.

Babylon supports data payloads from applications up to 256 bits in length, which along with Babylon's unique BlockMatrix architecture allows servers to handle up to 30 million updates per second (in its initial implementation).

The 256 bit data payload limit stems from Babylon's focus on the storage of data hashes that are 256 bits in length. These hashes provide a unique digital fingerprint of source data records (see Hash Basics below).

While hashes are unique to the source data that created them, they cannot be reversed to determine the original source data itself. Thus, by storing just hashes within Babylon, and not the source data, its use does not compromise corporate privacy policies and regulatory edicts related to storage of data in shared environments, outside of an enterprise.

As well as providing a way to store hashes of source data, Babylon also offers a verification function that allows applications to determine whether source data records are the same as those that were originally submitted to Babylon.

Uniquely, the Babylon verification function not only detects whether a data record has changed, but it can also determine what has changed within the data record. This patent-pending feature is achieved without storing original data records within Babylon.

For applications that require the highest level of immutability, collections of hashes stored within Babylon can themselves be hashed and committed to a public blockchain, such as Bitcoin or Ethereum.

In short, Babylon provides a mechanism for ensuring the immutability of data sets, for applications that do not require the full functionality of traditional blockchains, such as consensus. It also supports requirements for data privacy, since only hashes are stored within it.

Hash Basics

A hash can be thought of as a digital fingerprint of a set of data. Just like human fingerprints are unique to each person, so a hash is unique to a particular set of data.

Hashes are commonly 256 bits in length – as calculated using an algorithm called SHA-256. The algorithm was created by the US National Security Agency in 2001 and is widely used in cryptography for data encryption. Software functions that implement it are available for many programming languages.

A data set of any size can be processed using a SHA-256 function, which always results in a hash of 256 bits. Whenever the same data set is used as an input to the hash function, the same 256-bit hash will be calculated. However, any change – even a single binary digit – in the data set supplied to the hash function will result in a different 256-bit hash being calculated.

See this example – an input string of:

“Babylon provides immutability for Cobalt”

Always results in a 256-bit hash of:

“DC577E0A846AB58C567E69DB5B3AE023EF3891B591DBC81BB7BF7B0D8BB08028”

However, changing just one character – in this example, the “C” in “Cobalt” to lower case as in:

“Babylon provides immutability for cobalt”

Always results in a 256-bit hash of:

“4F09A2FADE04CDA2078EFF834AB4BBB173A7130F8AE39FA7122C10BE54113F0C”

As can be seen, even a small change in the data set results in a very different hash being calculated.

Typically, a hash is calculated when a data set is created and then both are stored securely. When the data set is retrieved at a later time, another hash is calculated, and compared to the original hash. If the two hashes are identical, then the data set has not been modified.

Thus, a hash can be used to detect a change – any change – in a set of data – of any size by simply comparing two 256-bit hash numbers.

Importantly, given a hash, it is not possible to determine what a data set is by some reversal of the hashing calculation. It is a one-one mathematical function.

4. How Cobalt leverages Kx Technology and Babylon

The business requirements for Cobalt led to the design of a technology architecture that draws on a combination of low-latency data communications and blockchain concepts. Specifically, Cobalt requires:

* High performance reconciliation of trade reports, calculation of hashes and secure storage in the shared ledger, resulting from executions between financial market participants, up to 100,000 per second.

* A guarantee of immutability of stored reconciled trade records – i.e. proof that they have not been altered since they were created.

* A way for Cobalt participants to confirm that trade data records have not been changed since they were originally created.

Within Cobalt, trade reports from banks and execution venues are processed by Kx. This includes normalization of trade reports, credit checking and creation of a reconciled trade record.

As soon as a trade record is created, a SHA-256 hash of it is calculated, which is fed into Babylon (via messaging middleware provided by Solace Systems). The trade record itself is stored within Cobalt, in a kdb+ database *(see figure 2 below).*

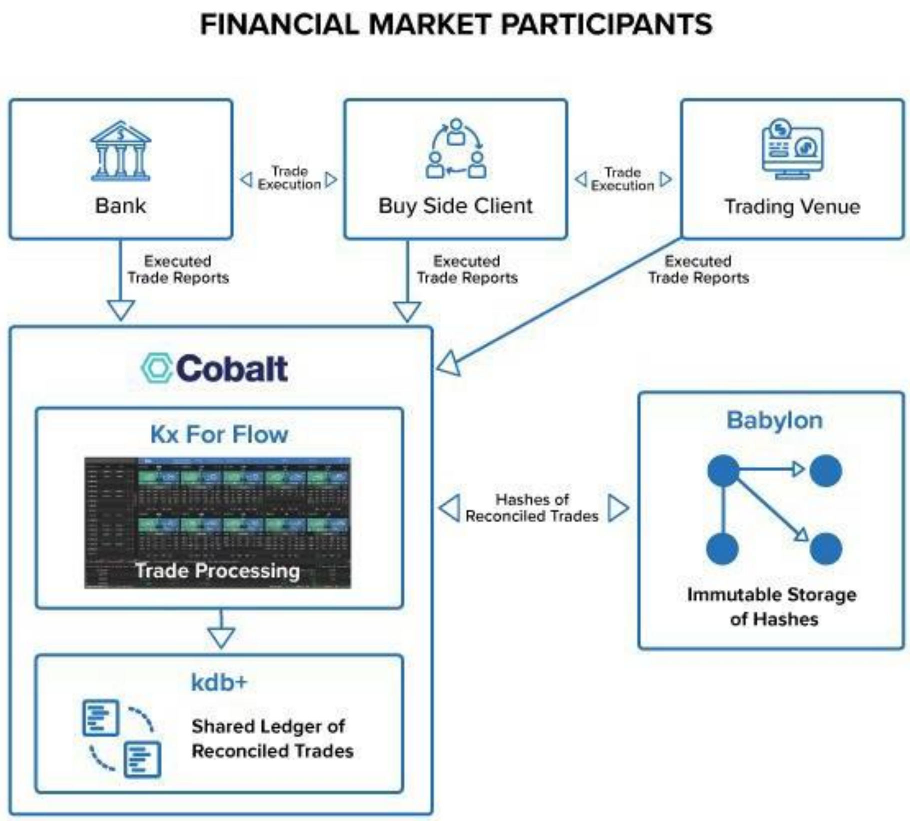

Figure 2 – Financial Market Participants

Babylon responds with a receipt that includes information that allows the hash to be retrieved from it at a later time.

Should later verification be required, the original hash can be retrieved from Babylon, and compared to a new hash that would be calculated from the trade record held in kdb+.

A positive comparison indicates the trade record has not been changed, and can be used for processes such as netting and payments.

However, a mismatch indicates that some change has been made. In this case, it is possible to query Babylon using a so-called granular lookup. This returns information that identifies the elements of the trade record that have changed, enabling more rapid resolution of reconciliation issues.

In conclusion, Cobalt’s requirement for high transaction performance, data immutability and scalability provides an ideal showcase for the integration of Kx and Babylon technology, leveraging the unique capabilities of each.

5. Beyond Cobalt with Kx and Babylon (and Blockchain)

Cobalt's pairing of Kx technology along with Babylon's unique immutability functionality implements a data architecture that has applicability across the financial markets and the related broader financial services space.

Financial markets applications, such as equities and options clearing, market surveillance and real-time payments are candidates for a data architecture that comprises a hybrid Kx kdb+ database and Babylon approach.

In particular, Babylon can provide immutability to augment and complement kdb+'s high performance, big data capacity and ready support of analytics and machine learning applications.

As such, the kdb+ and Babylon combination showcases the marriage of big data and blockchain concepts and highlights the complementary nature of these technologies.

Outside of the financial markets, other verticals also have a need for immutability of big data sets within high performance applications, where data privacy is also often important.

Verticals that are likely to benefit from combination kdb+ and Babylon data architectures include:

- Supply chain logistics, which can be automated by deployment of Internet-of-Things sensors to track the location and status of shipments in order to reduce fraud, optimize deliveries and automate payments.

- Trade finance, which involves transactions on a global scale involving many documents that are prone to loss and fraud. Such documents often contain sensitive information and hence privacy is paramount.

- Healthcare informatics and wellness data systems, which generate large quantities of data required for analytics and machine learning applications, but which also need to comply with stringent data privacy regulations.

- Utilities infrastructure, such as smart meters, which generate large quantities of data for real-time management. Such systems are often subject to significant regulations, and so immutable recording of data is important.

- Retail information and analytics systems, which process and secure data generated from multiple channels, including physical retail locations, web and mobile services.

It should also be noted that when the performance and functionality of Babylon is not required, or where a particular industry or application mandates the use of a traditional blockchain, then kdb+ can be integrated as a highly scalable, analytics friendly data store, which leverages the blockchain's immutability capability. Such a capability might be offered either as an enterprise deployment or a cloud-based on-demand platform.