WHITE PAPER

GridGain

Enable Bitcoin and Blockchain Technology with In-Memory Computing

A GridGain Systems In-Memory Computing White Paper

Bitcoin and blockchain, the digital-ledger technology behind this electronic currency, are generating enormous amounts of interest in the financial services industry. Most of the larger banks are investigating this area, and many technology companies are building platforms to enable blockchain technology for financial services firms.

In a 2016 Deutsche Bank survey of 200 participants in the global financial industry, almost all respondents (87 percent) expected this revolutionary technology to have a major impact on the securities services market. Three-quarters of the respondents said they expected to see widespread adoption of blockchain technology within the next three to six years. In addition, almost two-thirds expected blockchain adoption to produce substantial savings, in the range of 11 to 25 percent.

However, the adoption of blockchain technology will require significant technology upgrades. Current legacy systems cannot provide the security and performance needed to support the decentralized blockchain architecture in a well-integrated way. Participants will need scalable, distributed, and well-protected computing platforms in order to leverage the technology successfully.

This white paper will discuss bitcoin and blockchain technology, describe the innovative opportunities this technology offers for financial services firms, and examine how in-memory options such as the GridGain in-memory computing platform can address the challenges and boost the effectiveness of tomorrow's blockchain applications.

Before diving into the details of bitcoin and blockchain, let's look at some of the issues behind the need for these technologies.

ISSUES IN TODAY'S FINANCIAL ENVIRONMENT

The widespread interest in blockchain technology springs from its potential to help address several current issues with the financial ecosystem, including:

- **Lack of trust**. With recent volatility around banks coming into and disappearing from the financial ecosystem, there is a great deal of uncertainty and mistrust. People and institutions are not certain who can be trusted with their money and their payments. In addition, the growing problem of sophisticated financial fraud has created doubt about whether transactions come from a reliable source, increasing the mistrust.
- **Isolated legacy systems and processes**. Many financial services companies today are using legacy systems that have trouble connecting with other systems, creating isolated data islands.
- **Too many intermediaries**. Today's transaction processes are a complex series of steps. Some of these steps involve overnight or batch-oriented processing. This increases the time needed to get through the process as a whole.
- **Slow and complex post-trade functions**. Automation initiatives in the trading business, such as straight-through processing, have sped up the trading process itself. However, in the post-trade space, high complexity and numerous intermediaries continue to slow down processing.
- **Time-consuming reconciliation**. Within a financial system, everything must work smoothly, with no loss of records. In a sequential series of processes, there must be reconciliation after each process to ensure that all transactions are accounted for. And, of course, reconciliation involves numerous record-keeping, record-checking, and record-enrichment steps—all of which create additional complexity.
- **Time-consuming compliance checks**. Since the financial crisis of 2008 through 2010, the financial services environment has been heavily regulated. All transactions must be checked for regulatory compliance, with rules differing depending on whether the environment is banking, trading, or payments. These compliance checks add numerous validation and rules-checking steps to each process.

Before we explore how blockchain technology can help to overcome these issues of mistrust, data isolation, and complexity of processing, let's look at what blockchain technology is and how it is currently being used—the most prominent example being the role of this technology in bitcoin.

BITCOIN: A NEW MODEL FOR ELECTRONIC CURRENCY

Bitcoin is a cryptocurrency—a fully electronic currency secured by cryptography—that operates without oversight from any central bank authority. Originally envisioned as a framework to allow small payments to be made electronically without incurring credit card fees, bitcoin technology has become much more. Bitcoin with a capital "B" is now a flourishing protocol and a payment network that is used in many areas within the general category of payments. There are virtual exchanges for buying and selling bitcoins (which

are stored in electronic "wallets"), as well as for exchanging them with traditional currency, and bitcoins have performed well as investments. According to Bloomberg, their value has surged more than 4,000 percent since 2011.

Where bitcoins come from. Bitcoins are introduced into circulation using a mechanism called mining. Mining involves competing with other parties to perform transaction-recording tasks and obtain bitcoins as a reward. This reward creates the incentive for miners throughout the Internet (anyone with sufficient knowledge and processing power) to perform the record-keeping tasks that are necessary to perpetuate the system. Miners record transactions in a public, distributed ledger called the blockchain. (Note: The word "Blockchain," when capitalized, can also refer to a software and wallet company that hosts a real-time browser of bitcoin transactions. Throughout this paper, we use the word to refer to digital ledgers and ledger technology in general.)

Challenges to bitcoin adoption. Some potential adopters are approaching bitcoins cautiously due to a variety of issues. Because bitcoin is a fully electronic currency, it requires special setup steps not needed for familiar currencies, and it is more vulnerable to cyber-theft, hacking, authentication issues, and system failures. Because it operates outside of existing currency controls, it is more volatile than other currencies and is also the focus of increasing government scrutiny. In addition, there are concerns about system independence, since about 70 percent of the bitcoin mining is currently done in China, according to Bloomberg. As familiarity with bitcoin technology grows, many or all of these concerns are likely to ease.

Wider implications of the bitcoin model. Regardless of the degree to which bitcoins are embraced as a currency, there is growing interest in the digital-ledger technology behind bitcoins—that is, the blockchain. This technology offers substantial promise for streamlining many types of transactions.

BLOCKCHAIN: THE REVOLUTIONARY TECHNOLOGY BEHIND BITCOINS

Describing a blockchain simply as a public, distributed ledger of transactions does not fully convey its power and potential. What makes blockchain technology particularly compelling is that it creates a decentralized, self-perpetuating infrastructure that transmits information simultaneously to all interested parties. This model can save substantial amounts of time and money for those needing access to the transaction data.

How blockchains operate. Whenever a transaction occurs, such as a person sending bitcoins to a company to purchase a product, a secure transaction message goes from sender to receiver (say, person to company). Only the sender and receiver can view the contents of the message, but a record of the transaction (that is, of the particular bitcoins being spent) is added to the blockchain and is viewable while encrypted by all blockchain subscribers, who can see the source and destination. If they need to see the contents, they decrypt the block.

Direct access to transaction data. Because all subscribers receive the blockchain update simultaneously, there's no need for costly intermediaries or a time-consuming set of reconciliation steps to complete the transaction.

Transparency plus security. While it might seem as though such a public infrastructure would be vulnerable to tampering and errors, the design of the blockchain ensures a very high level of integrity and security. A blockchain is a set of sequential blocks of encrypted transaction information that can never be removed or deleted, only added to, in chronological order. There is one blockchain for all bitcoin transactions, and each block of transactions contains both a timestamp and a hash of the previous block, making the blockchain highly tamper-resistant.

The randomness inherent in transaction verification also contributes to the security of blockchains. Each transaction is sent randomly to one of many computers that subscribe to the blockchain, and that computer can then verify its validity (in terms of source and destination, plus contents if it is a bitcoin transaction) before distributing it. The awareness that anyone anywhere might end up validating the transaction helps to deter those who might want to interfere with transactions; they can't influence the validator because there is no way to predict who the validator will be.

An open, decentralized model. The blockchain model is based on decentralized, peer-to-peer transactions. All subscribing computers can communicate with the blockchain and view records within an open, cloud-like interface—sometimes referred to as the "Internet of Trust."

This idea of direct connection between involved parties without much centralization is key to understanding blockchain technology and why it matters to the financial community. Transaction-processing systems based on this direct, decentralized system have tremendous potential to overcome the mistrust, isolation, and complexity that have plagued the financial ecosystem.

POTENTIAL BLOCKCHAIN USE CASES

Many banks, large financial institutions, registry houses, custodians, and payment centers are evaluating blockchain technology. Because all blockchain subscribers receive direct, simultaneous access to transaction data, few counterparties and transaction checks are needed. Each transaction requires only a couple of records to be sent, offering substantial streamlining compared to current transaction processes.

Some potential blockchain use cases for financial services include the following:

- **Post-trade processing**. Back-office post-trade functions such as netting, matching, and clearing (typically performed by multiple agencies) could be greatly simplified if trade details were available on a block within a blockchain. All involved parties could potentially read the details and perform their parts in the process without having to go through daily exercises, end-of-day processing, and numerous reconciliations.
- **Collateral management**. Reducing credit risk in financial transactions can require securing them with collateral—often through a complex set of steps that could be streamlined using a blockchain.
- **Payments processing**. Payment hubs are now looking into how to process those payments in a cheaper and more reliable fashion, and blockchain technology offers a potential solution.
- **Trade finance**. Typically, there are many parties and multiple reconciliation steps involved in trade finance processes, which can also require substantial transactional resources. Blockchain technology could make these processes simpler and less expensive.
- **Same-day settlement**. Companies are clearly moving toward reducing the number of days needed to settle a trade. With a blockchain, the full transaction can be completed within about 15 minutes from the time the initial message about the trade is sent.
- **Security servicing and processing**. With a blockchain, anybody who is subscribing to information about a security (for example, news about corporate actions or dividends) can immediately receive that information directly from the source.
- **Transfer agency and registrar functions**. Companies want to know who their shareholders are. Currently, when shareholder ownership changes, there is a long process before the company hears about it. With a blockchain, all of the steps in the process can occur on the same day.
- **Equilibrium and decentralization of players**. With a blockchain infrastructure, small players can play a larger role in markets that might otherwise be controlled by larger players (large custodians, depositories, transfer agencies and so on). Players will not need to invest a lot of money into the infrastructure, as everyone will use the shared infrastructure of the blockchain.
- **Private blockchains**. Anyone launching any of the use cases described here will need to decide whether they are comfortable using the same network used by today's bitcoins. The other option would be to build their own blockchain and allow only valid participants to use it, using a registration model instead of free entrance.

Let's take a close look at a specific example of how a blockchain could simplify a multi-step transaction process.

CREATING A BLOCKCHAIN-FRIENDLY INFRASTRUCTURE

Blockchain technology holds enormous potential for streamlining transaction processing. Making the most of this potential will require participants to develop an appropriate infrastructure.

With blockchains, there is no central data repository. Instead, the parties involved must collect the blocks of transaction information that are sent out to all subscribers. These blocks constitute an ever-growing amount of data (in fact, for bitcoins, there is just one blockchain of all transactions since the beginning, constantly increasing in size). Large-scale participants in this infrastructure will want to hold onto this data for their records—which means dealing with large amounts of data arriving in real-time.

Financial services firms not only need to store the incoming blocks, they also need to translate and validate the information. They need to maintain tables of security identifiers, validation information, cross-references, and so on. They need real-time transaction processing and analytical capabilities in order to leverage the advantage of immediate access to blockchain data for multiple transactions.

Any application that involves large-scale storing and processing of blockchain data will require a high-performance, scalable architecture. Some applications, such as bitcoin mining, require especially strong analytical capabilities and processing power. A blockchain-friendly architecture should also include streaming support, enterprise-level security features, and the high level of transactional consistency needed for financial systems.

GridGain

Fortunately, in-memory computing is available with these features and is well-suited to this type of high-speed, big-data use case. Let's look at why in-memory computing makes sense for blockchain applications.

IN-MEMORY COMPUTING: BENEFITS AND USE CASES

As noted earlier, blockchains can only grow, never shrink, since their integrity depends on no block being deleted. Large-scale blockchain subscribers must be prepared to quickly process, store, and analyze fast-growing amounts of transaction information arriving in real time. Because in-memory computing involves keeping data in RAM for extremely fast access, with no disk-related slowdowns, it is faster than any other storage-based computing method.

For applications that require heavy analytics and real-time transaction processing of hundreds or even millions of transactions per second, the market is now moving from disk to in-memory computing. The reasons for this trend involve both performance and Return On Investment (ROI).

1000x Faster. The move from disk to memory is a key factor in improving performance. However, simply moving to memory is not sufficient to guarantee the extremely high memory-processing speeds needed at the enterprise level. Enterprise-level speed requires cluster computing, with multiple machines performing analyses at the same time, and parallel distribution of data. These capabilities are important for providing high availability, disaster recovery, and concurrency across systems—and they are all provided in the GridGain in-memory computing platform. Clients who have implemented the GridGain In-Memory Data Fabric have found that they can process transactions about 1000 times faster.

10x ROI Improvement. The cost of memory has dropped roughly 30 percent per year since the 1960s, so memory has become much more affordable in recent years. While it may still be slightly more expensive than disk, the performance is so much better that it improves ROI significantly. Clients who have implemented the GridGain in-memory computing platform have seen a tenfold or more improvement in their ROI.

Customer Case Study: Sberbank

One of the most noteworthy GridGain Systems financial services customers is Sberbank, the largest bank in Russia and the third largest in Europe. Sberbank was faced with a similar problem to the one currently facing companies who are transitioning from legacy systems and methods to real-time, synchronized transaction processing using blockchains. The bank was switching from a more traditional, brick-and-mortar setup—one in which people would come into their offices and manually process a limited number of financial transactions each day, during a limited time period—to a new world with online and mobile customers transacting with them 24/7.

The company forecasted future throughput requirements and determined that it needed to move to a next-generation data-processing platform to handle the expected transaction volume. Sberbank analyzed more than ten potential solutions from vendors in the in-memory computing space and found that the GridGain in-memory computing platform was the most comprehensive solution. The bank concluded that GridGain would provide the next-generation platform with a significant improvement in performance and scalability.

The GridGain in-memory computing platform provided several other important capabilities that Sberbank's next-generation platform would require such as machine-learning and analytics, flexible pricing, artificial intelligence, ease of deployment, hardware independence of cluster components, and a rigorous level of transactional consistency. Of particular importance was the ability to conduct integrity checking and rollback on financial transactions. Sberbank could not find that level of consistency with other in-memory computing solutions.

In a January 2016 article in RBC, Herman Gref, the CEO of Sberbank, said that the bank selected the GridGain Systems technology to build "a platform that will enable the bank to introduce new products within hours, not weeks." He went on to state that the GridGain in-memory computing platform enables Sberbank to provide "unlimited performance and very high reliability" while being "much cheaper" than the technology used previously. Sberbank is using GridGain's in-memory computing platform to implement capabilities that could not be provided by the other vendors evaluated—a group that included Oracle®, IBM® and others.

GRIDGAIN SYSTEMS: A LEADER IN IN-MEMORY COMPUTING

As blockchain interest grows, many financial services firms are looking toward the GridGain in-memory computing platform. Of particular interest are GridGain's in-memory Data Grid, Compute Grid, SQL Grid, and streaming functionality. These features provide the performance, scale, and interoperability required for successful blockchain projects.

In addition to working with Sberbank on its next-generation system, GridGain is working with other banks that are now in a proof-of-concept stage or are close to moving blockchain applications into production. In addition, technology firms are evaluating GridGain as a means of offering Software-as-a-Service platforms around their blockchain implementations. GridGain's comprehensive platform contains a complete feature set that surpasses the capabilities of in-memory database point solutions, making it well suited to these types of financial use cases.

As a complete in-memory computing platform, GridGain helps users consolidate onto a single high performance and highly scalable big-data solution for transactions and analytics, resulting in lowered TCO. Advanced SQL functionality and API-based support for common programming languages enable rapid deployment. These features, along with the rapidly decreasing cost of memory, boost ROI for in-memory computing initiatives, enabling financial services companies to build less expensive systems that perform thousands of times better.

Clients enjoy the following:

A Unified High-performance Architecture

The GridGain in-memory computing platform consists of multiple grids connected by a clustered in-memory file system. The In-Memory Data Grid, In-Memory Compute Grid, In-Memory SQL Grid and In-Memory Service Grid are interconnected. Computations occur as close as possible to the data used in the computation. Additional features such as high throughput, low latency, load balancing, caching, in-memory indexing, streaming, Hadoop acceleration and other performance improvements are crucial to success in real-time modeling, processing, and analytics.

Scalability

The GridGain in-memory computing platform excels in terms of scalability, allowing companies to add cluster nodes and memory in real-time with automatic data rebalancing. As a hardware-agnostic solution, clients can choose their preferred hardware for scaling up.

Full SQL Support

GridGain is ANSI SQL-99 compliant and the In-Memory SQL Grid supports DML users can leverage their existing SQL code using the GridGain JDBC and ODBC APIs. For users with existing code bases which are not based on SQL, they can leverage their existing code through supported APIs for Java, .NET, C++, and more.

High Availability

The GridGain in-memory computing platform provides essential high availability features such as data-center replication, automatic failover, fault tolerance, and quick recovery on an enterprise-level scale.

Transaction Processing

The GridGain in-memory computing platform supports ACID-compliant transactions in a number of user-configurable modes.

Security Features

The GridGain in-memory computing platform supports authentication, authorization, multiple encryption levels, tracing, and auditing.

Open Source Framework

GridGain is based on Apache® Ignite™, a popular open source project with many contributors that has been tested globally. GridGain Systems was the original creator of the code contributed to the Apache Software Foundation that became Apache Ignite and fully supports the technology behind Apache Ignite. The GridGain Enterprise Edition extends the features in Apache Ignite to provide enterprise-level capabilities and services, such as additional security, data center replication, auditing mechanisms, a GUI for management and monitoring, network segmentation, and a recoverable local store.

Production Support

GridGain Systems Support is available for GridGain Community Edition, GridGain Enterprise Edition and GridGain Ultimate Edition users. The Enterprise and Ultimate editions include rolling updates, faster availability of all releases and patches, and 24/7 enterprise-level support.

LEVERAGING THE POWER OF BLOCKCHAINS

Blockchain technology offers a compelling path forward for financial firms seeking to move away from a batch-processing and reconciliation-based model and toward real-time, synchronized transaction processing. Companies are embracing this digital-ledger technology bitcoin and non-bitcoin transactions. These companies require the performance and scale provided by in-memory computing to store, aggregate, and process large volumes of blockchain data at real-time speeds.

The GridGain in-memory computing platform overcomes the challenges of Bitcoin and blockchain projects with features that improve performance, scale, and interoperability. Data Grid improves the speed and scale of blockchain transactions. Compute Grid provides parallel processing for calculations required for building and updating blockchains. Compute Grid's parallel processing capabilities also speed up reconciliation and compliance checking. SQL Grid allows companies to connect the GridGain In-Memory Data Fabric to other systems for analytics and reporting.

Combining an open source framework with enterprise-level features, the GridGain in-memory computing platform offers a high performance, scalable, and comprehensive solution. The GridGain in-memory computing platform is an elegant and efficient solution to leverage the power of blockchains for streamlined transaction processing.

Contact GridGain Systems

To learn more about how GridGain can help your business, please email our sales team at sales@gridgain.com, call us at +1 (650) 241-2281 (US) or +44 (0)208 610 0666 (Europe), or complete our contact form at www.gridgain.com/contact and we will contact you.

About GridGain Systems

GridGain Systems is revolutionizing real-time data access and processing with the GridGain in-memory computing platform built on Apache® Ignite™. GridGain and Apache Ignite are used by tens of thousands of global enterprises in financial services, fintech, software, e-commerce, retail, online business services, healthcare, telecom and other major sectors, with a client list that includes ING, Raymond James, American Express, Societe Generale, Finastra, IHS Markit, ServiceNow, Marketo, RingCentral, American Airlines, Agilent, and UnitedHealthcare. GridGain delivers unprecedented speed and massive scalability to both legacy and greenfield applications. Deployed on a distributed cluster of commodity servers, GridGain software can reside between the application and data layers (RDBMS, NoSQL and Apache® Hadoop®), requiring no rip-and-replace of the existing databases, or it can be deployed as an in-memory transactional SQL database. GridGain is the most comprehensive in-memory computing platform for high-volume ACID transactions, real-time analytics, web-scale applications, continuous learning and hybrid transactional/analytical processing (HTAP). For more information on GridGain products and services, visit www.gridgain.com.