Fighting Fraud in Financial Services?
How Blockchain Can Help
Fraud – A Growing Challenge

Fraud is a massive and growing challenge for the financial services industry, representing a loss of up to 3% of annual revenues according to a recent LexisNexis Risk Solutions survey.¹ For every dollar they lose to fraud, companies incur an additional $2.67 in costs.²

The challenge of countering fraud in financial services is only exacerbated by ongoing pressures to build more personalized, always-available services, while at the same time countering disruptive new market entrants.

Established providers risk adopting novel technologies that open new avenues for fraud—or that offer gains such as faster development and increased automation at the cost of weakened security controls. “As more channels and new financial service offerings emerge, threats will diversify,” warns Kaspersky Lab.³

Blockchain’s Role in Fighting Fraud

Blockchain-based technologies have the potential to disrupt multiple specific financial services transactions, such as trade finance, international payments, and foreign exchange. Limited solutions for these sectors already exist.

But most current blockchain-based services remain plagued by problems with scale, methodology, lack of consensus, and insufficient investment. As a result, they remain far from meeting their potential. That’s especially true when it comes to countering fraud.

We believe, however, that blockchain can underpin new financial services transactions that transform our ability to counter fraudulent financial activities. VMware is actively researching how such solutions might be designed and foresees developing powerful new products in partnership with multiple financial services customers that reduce fraud for a wide variety of potential use cases.

“Blockchain’s inherent design ensures that subsequent transaction records contain artifacts and identifiers of previous transactions. This allows authorized investigators to backtrack transactions on the blockchain more easily than with current AML and EFM systems.”

“BLOCKCHAIN WILL TRANSFORM AND RADICALLY IMPROVE FRAUD MANAGEMENT AND ANTI-MONEY LAUNDERING” MARCH 2018, FORRESTER.
Uses Cases for Countering Fraud in Financial Services

At its heart, fraud is a consequence of failed information management. Blockchain, at its heart, is a sophisticated system for controlling the security and flow of information. And because blockchain can do both so well, it can underpin financial systems that level the information playing field—allowing providers to deliver their services more efficiently, assuring consumers that their transactions remain private and secure, and offering regulators the access they need to ensure compliance without intruding on provider/customer relations.

There are numerous potential use cases for blockchain-based solutions in addressing fraud in financial services. Among them:

Anti-money Laundering (AML)
Money laundering operations work across multiple accounts held by multiple institutions. At present, banks’ understandable reluctance to share customer data with institutions that are often their main competitors seriously impedes AML interdiction efforts. Blockchain-based solutions can offer a “common plane of data” across, and thus a framework for establishing trust between, multiple institutions and their various databases. A blockchain-enabled AML solution might, for example, establish account ownership without revealing details of the individual account held since Blockchain-enabled zero knowledge proofs allow banks to prove information about their customers without actually sharing that information.

47% of respondents globally confirm their organization has suffered at least one incident of financial crime in the last 12 months.

THOMSON REUTERS 2018 SURVEY: “REVEALING THE TRUE COST OF FINANCIAL CRIME”
Know Your Customer (KYC)

Thanks to information bottlenecks, financial institutions can easily be defrauded by customers with fake credentials or histories of fraud with other providers. Blockchain can support solutions that let banks know whether their customers are who they claim to be—without revealing details of the customers’ other account holdings. Such systems could also allow customers to easily prove their identity when opening accounts at new institutions, reducing friction in new customer acquisition.

Handling Compliance Queries

Regulatory mechanisms such as sanctioning queries are essential for deterring fraud, but as currently operated they also impose burdens upon both the creators and consumers of financial services solutions. Blockchain solutions can offer protected access into shared information repositories that allow regulators to confirm that accounts and account activity are legitimate while protecting provider and client privacy.

Payment Processing

Most international transfers take about 1 to 4 business days⁴—which amounts to trillions of dollars-worth of cash flow every day. These funds are getting stuck in AML, sanctioning queries, and other kinds of fraud prevention mechanisms. To the degree that blockchain-based solutions impact fraud prevention, they will have an additional positive influence on the flow of international payments.

It’s not hard to find more examples. Every time a financial institution moves money—for remittances, trade financing, foreign exchange transfers, escrow transactions and so on—they rely on trust. By tackling fraud, blockchain technologies help build trust—and thus drive business, profits, and growth.

Why VMware Blockchain

Clearly, individual solutions that successfully addresses the use cases outlined above will be very different from each other. Each will necessarily tie into different tools and different backend systems. But blockchain—done right—can underlie them all.

As noted, almost every major financial services provider is already experimenting with blockchain-based solutions. Most efforts, however, remain too limited in breadth, scale, and operational utility to have the potential impact on fraud outlined above. Too often, current solutions:

• Rely on blockchain models with poor latency, energy-inefficiencies, and low fault-tolerance.
• Can’t satisfy risk management team requirements.
• Can’t meet regulatory demands.
• Don’t have the buy-in required to work across large network consortia.
• Only allow management of one blockchain solution.
• Perform poorly in day two operations.
• Can’t scale to the large number of nodes needed in global banking systems.
• Can’t scale to the throughout needed in banking transactions.
• Can’t accommodate new regulations such as GDPR or secure deletes of customer data.

Advantages of VMware Blockchain

- Full audit capability and data visibility
- Access across multiple different clouds
- A hybrid approach
- Management across multiple blockchain environments
- A solution that scales
Introducing Scalable Byzantine Fault Tolerance

VMware is pioneering an approach that builds on the Byzantine Fault Tolerance (BFT) approach to blockchain, which replaces the energy-inefficient mining required by systems like Bitcoin and Ethereum with voting and is designed to keep working even when there are malicious activities detected in the blockchain network. BFT systems, however, require a lot of back and forth communication and thus don’t scale well. VMware’s solution deploys an internally-developed Scalable Byzantine Fault Tolerance (SBFT) approach. This simplifies and streamlines communication between nodes, which in turn makes it possible to scale the number of nodes in the network while also increasing overall network throughput.
The VMware Blockchain model

The VMware blockchain model is also open only to known and registered participants. This keeps transaction records private and extends security beyond the fact of a transaction to the transaction’s substance (such as a record of specific assets or units of currency).

Crucially for the financial services sector, VMware’s solution is uniquely optimized for day two operations. It offers:

- **Full audit capability and data visibility.** You can track the location of your data, who is touching it, which nodes are seeing it, and who owns those nodes.

- **Access across multiple different clouds.** With over 4,000 cloud partners, VMware is unmatched in offering multi-cloud access.

- **A hybrid approach.** VMware is the only blockchain solution that lets you participate both with network nodes in a hosted cloud solution and also the local on-prem nodes you need to meet data sovereignty regulations.

- **Management across multiple blockchain environments.** VMware’s blockchain interface is alone in supporting other current and emerging blockchain technologies, including HyperLedger, and offers full support for Ethereum-based smart contracts.

- **A solution that scales.** The VMware blockchain consortium has the design, the volume of nodes and transactions, and the fault-tolerance required to scale at the rate needed by major financial services providers.

Blockchain, of course, won’t reduce all types of financial fraud. A poorly-secured underlying infrastructure, for example, will still expose vulnerabilities that allow unauthorized access. But VMware’s blockchain technology is uniquely equipped to close off many significant avenues for fraud in financial services—and at the same time empower financial services providers to further streamline operations, improve speed to market, and get closer to their customers.
Learn About VMware Blockchain for Financial Services

Learn more

If you are interested in learning more about how VMware’s blockchain solutions can help you create secure, transparent, cost-effective, and efficient financial services, please visit VMware.com/blockchain or contact us at blockchain-info@VMware.com.