Wall Street Occupies the Blockchain

FINANCIAL FIRMS PLAN TO MOVE TRILLIONS IN ASSETS TO BLOCKCHAINS IN 2018

WHEN BLOCKCHAINS first appeared nearly a decade ago as the technical backbone of Bitcoin, the world's leading cryptocurrency, they seemed to offer the masses a way to cut out the financial middleman. But now the big banks and other industry players are finding ways to spin the new tool to their advantage. • Their blockchains share a vision that is precisely the opposite of the one laid out in the Bitcoin white paper, published under the pseudonym Satoshi Nakamoto in 2009. Like Nakamoto

Blockchain

himself (or herself), you can own bitcoins without even stating your real name; nobody is in charge; and anybody can check the history of any given transaction. The financial industry's blockchains, however, are closed or, in their jargon, permissioned; to join one you must reveal your identity to a system administrator, who must then approve you. • Firms say a permissioned network is the best way to satisfy regulators and protect client privacy, but purists argue that trying to keep a close hold on information removes the very point of blockchains while threatening to create new problems both for companies and their clients. • In the past two years, giants such as BNY Mellon, Goldman Sachs, ING, Santander, and UBS have explored dozens of blockchain projects, and some of those are now moving beyond the proof-of-concept phase. One of the first to be released into the real world will come from a little-known financial corporation that mediates a US $11 trillion-a-year market for an arcane class of securities, the trading of which allows people to pay money to shed risk or make money by accepting it.

By **AMY NORDRUM**

If all goes well, a far larger chunk of the quadrillion-dollar securities market, along with many of the administrative tasks performed by banks and brokerages, could soon be running on corporate blockchains.

Nakamoto's paper sketched out a peer-to-peer financial network with no intermediaries to collect fees, botch a transfer, or trigger an economic meltdown. Transactions would be signed with a digital key and recorded in a public ledger—the master source for all accounts—stored across many computers. This setup ensures that the history of the transaction can't be altered.

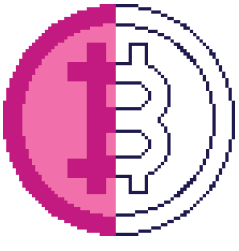
However, the first cryptocurrency exchanges and digital wallets were riddled with vulnerabilities, and the underlying public blockchains were difficult to scale up. Then in 2016 there was a high-profile $60 million heist at the DAO, an autonomous investment fund that ran on smart contracts placed atop Ethereum, the public blockchain for ethers, a cryptocurrency rival to bitcoins. The funds were recovered, but it was a painful reminder that blockchains and their accoutrements are still written by humans, who inevitably make errors in their code.

That's why financial firms have limited their own blockchain networks to clients who clearly identify themselves through digital keys. These permissioned ledgers are carefully tailored to achieve a company's specific goals, and they're easier to fix if something goes wrong

"I think permissioned looks more like how the world works," says Brian Behlendorf, executive director of the Hyperledger project. "I think permissionless looks like how some people think the world should be."

To others, though, permissioned ledgers fall short of blockchain technology's potential to enable all financial transactions to run on a transparent, decentralized system. It's disappointing to many early supporters of Bitcoin to see the momentum shift toward permissioned networks, and away from open, public blockchains.

"In some cases, the permissioned ones are a bit of a regression from what Bitcoin proved possible in 2009 back to distributed database technologies, like Paxos, that were developed in the '80s and '90s," says Peter Van Valkenburgh, research director at the nonprofit Coin Center. "They're seeking to address what is really low-hanging fruit in the IT industry, which is systems implemented by conservative industries like banks."



HACKS & HEISTS

2011

Unknown hackers used a bug in the Bitcoin code to create 184 million bitcoins out of thin air. This remains the only instance of Bitcoin itself being hacked.

Robert Palatnick first heard about blockchains three years ago from his son, a high schooler who had bought a few bitcoins. "He lost money and I just told him, 'That's a lesson learned,' " Palatnick says.

Today, as managing director and chief technology architect of the Depository Trust and Clearing Corporation (DTCC), in New York City, Palatnick is leading several projects to insert blockchains directly into the company's daily operations.

The DTCC is a financial utility that holds the books on which firms record their trades. It was established by industry titans in the 1970s to manage the flood of paperwork brought on by the rise of securities trading. Almost every broker or institutional investor in the world today who trades a U.S.-based security—whether a municipal bond or a share of Apple—settles it through DTCC.

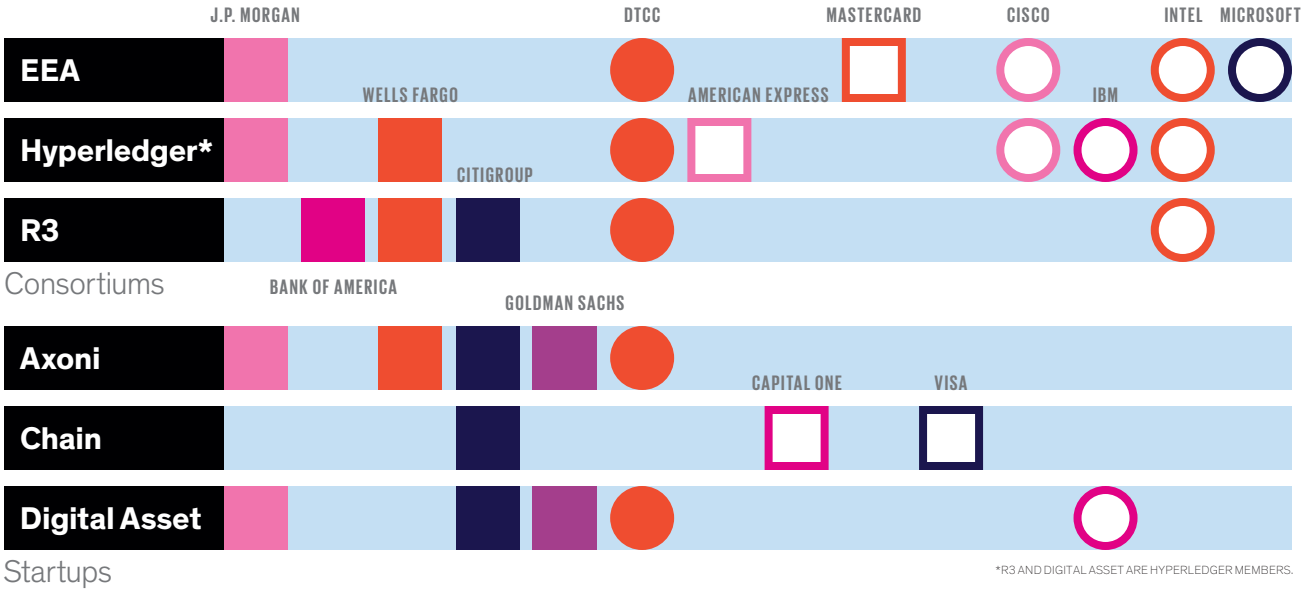
DTCC hopes that rejiggering its databases to run on a permissioned blockchain will save money. But the upgrade will ultimately change little about the way the financial system works today. As envisioned, it is still a proprietary system through which centralized players control trading behind walled-off networks.

When DTCC's inaugural blockchain network goes live, in late 2018, it will be the industry's most ambitious implementation to date, handling $11 trillion worth of credit-default swaps. That's a type of contract that allows one firm to pass risk to another firm. Credit-default swaps were invented in 1994 by bankers at J.P. Morgan. A decade later, one breed—those tied to mortgage-backed securities—helped ignite the U.S. financial crisis.

About 10 years ago, DTCC built an information warehouse on a mainframe that now handles 98 percent of all the world's credit-default swaps—a type of credit derivative. The warehouse does all the heavy lifting to keep track of who owes whom. Today, roughly 1,200 firms rely on it to trade swaps, to the tune of 60,000 transactions per day.

The system works well enough, but the process of trading swaps is still inefficient in ways that Palatnick believes a blockchain could solve. Today, every firm formats swaps in a slightly different way. When two firms wish to participate in a swap, they must both submit orders to a software program known as a matching service, which makes sure the terms are consistent. Then, a final agreement is forwarded on to DTCC's warehouse.

ILLUSTRATIONS: THIS PAGE BY Nicholas Little; PREVIOUS PAGES BY Mario De Meyer



Hedging Their Blockchain Bets

BANKS, CREDIT CARD PROVIDERS, and tech companies need help figuring out what blockchains can do for them. This chart shows membership in three leading blockchain consortiums, and which companies have worked with or invested in popular blockchain startups. Many believe it's still too early to choose a winner.

BANKS
CREDIT CARD PROVIDERS
TECH COMPANIES

During those handoffs, the swap is translated and reformatted several times.

Tomorrow, Palatnick argues, buyers and sellers recording swaps directly to a blockchain could use logic written into the agreement itself–a "smart contract"–to automatically manage trades. Every firm could use the same software to record trade contracts, eliminating costly trade and payment reconciliations. Because every computer, or node, would store its own copy of the full history of swaps, firms could be certain they were trading on the latest information.

This ability to access a "golden record" matters because failing to have the most recent market data can cause a firm to lose out on millions of dollars. To avoid this, banks and brokerages pay hefty subscription fees to data services from Bloomberg and Thompson Reuters.

For more than a year, DTCC has been working with IBM and the blockchain startup Axoni to develop a swap network on a unified code base called AxCore. When a swap is made, software by Axoni writes it into a smart contract and records the entry to Axoni's proprietary blockchain, stored across multiple nodes in the cloud.

So far, DTCC has installed three nodes, and based on the original business case, Palatnick expects the completed system will save the company 20 to 30 percent in costs, compared with running swaps through the mainframe. Eventually, firms that trade the most swaps may choose to set up their own nodes by installing Axoni's software, reaping even more savings across the industry.

Last year, Axoni built enough smart contracts to simulate the entire volume of credit-default swaps currently listed in DTCC's warehouse. Then it ran 85 tests, putting the system through the paces of a normal trade and even pulling the plug on a node to see how the rest of the network would react.

Afterward, DTCC said Axoni's software posted a 100 percent success rate in achieving the desired result in each test. Once the project goes live, all the Axoni code, or "secret sauce" as Palatnick calls it, will be placed in escrow or submitted to the open-source Hyperledger project, so that if Axoni goes out of business, the trading of swaps can continue.

When it's deployed next year, the new swap network will first operate in the background, running parallel to the existing warehouse. But Palatnick's goal is for it to replace that warehouse by the end of 2018. From that moment, the entire $11 trillion global market for credit-default swaps will be traded on a blockchain.

Before long, many more financial products may move to blockchains. Proponents have dreamed up countless ways the technology could improve the financial industry, by allowing real-time auditing, enabling regulators to halt illegal transactions, or empowering investors to trade without a broker or an exchange.

But some experts say that most of the time a blockchain doesn't offer much value beyond a traditional database or a basic messaging service. Applying it too broadly, or expecting too much, they say, will only lead to disappointment.

"I've watched a lot of proof of concepts that haven't really gone anywhere," says Jerry Cuomo, IBM's vice president of blockchain technologies. He estimates IBM has worked on blockchain projects for 400 companies in the past few years. So far, barely a dozen of those have moved into production.

Corporate enthusiasm for blockchains ramped up in 2016 and generated a swarm of press releases, but little is known about how most of those early projects fared. "To be honest, we don't have much data publicly about the health of these PoCs," Ian Lee, a director with Citibank's venture investment division, told the audience at Consensus, an annual blockchain conference held in May.

Still, the mood at Consensus was jubilant—the prices of several leading cryptocurrencies had swollen that quarter. The emcee, flanked by backup dancers dressed in gold, opened the conference with a song to celebrate that growth.

Meanwhile, financial companies are running up against some very real constraints in their own blockchain bets. Developers are still figuring out how to make simple applications, write smart contracts that are defensible in court, and keep their employers out of trouble with regulators. To help, several consortiums and companies are trying to set standards, create open-source software tools, or develop platforms that can plug into any blockchain.

Startups such as Axoni and Chain are writing industry-friendly code bases that clients can adorn with special applications (called DApps for "decentralized applications"), typically executed through smart contracts, to run across many servers. With custom-built application program interfaces and software development kits, clients can adapt these DApps for their own purposes and integrate them with legacy systems.

PEOPLE

Richard Gendel Brown

In 2015, the world's largest banks dived headfirst into the blockchain craze and formed a consortium called R3. Richard Gendel Brown, R3's chief technical officer, used its financial brainpower to create Corda, a distributed ledger designed specifically for financial agreements.

IBM and Microsoft have jumped into the fray with a suite of services to create specific projects running on permissioned blockchains. Microsoft has developed a middleware that provides features such as a digital key vault and identity management and works with any blockchain that Microsoft deems enterprise grade—Ethereum, for instance.

At IBM, most projects are based on Hyperledger Fabric, a distributed ledger with smart contracts written in the programming language Go. Fabric also allows companies to subdivide a ledger into sections, which IBM's Cuomo likens to Slack channels, in order to broadcast transactions only to participants on the same channel.

A number of efforts are also under way to develop permissioned offshoots, or forks, of Ethereum. These forks are open source and infused with corporate-friendly features that the public chains lack, such as the ability to broadcast a transaction only to the parties involved, which is similar to what Fabric offers. Depending on how forks are configured, participants can use ethers to pay for transactions or special tokens based on ethers that are accepted only on a specific fork—a type of digital Monopoly money.

The Enterprise Ethereum Alliance, a consortium of businesses interested in blockchains, has adopted J.P. Morgan's open-source Quorum framework as its basis. Another group, known as R3, has a separate blockchain-inspired project called Corda that is more like Fabric, in that it mainly functions as a distributed ledger.

In general, though, blockchain development is still a jumbled mix of techniques and tools. Even though financial firms have invested millions of dollars into the pursuit, there is still no widely accepted reference architecture or standards for a blockchain-based network. "Every vendor is kind of creating their own version," says Palatnick.

This disparate approach can make it difficult to compare features such as security. Jesse McWaters of the World Economic Forum, who coordinated a recent report on blockchain technology in finance, says developers must find a way to conduct security audits on all blockchain networks, so the industry and public can feel confident in their use.

With those growing pains in mind, Laurence Leblond, head of operations for Unigestion, a financial services company based in Geneva, is pro-

ILLUSTRATION BY Nicholas Little

ceeding cautiously. “For us, all the challenges of blockchain are about the security of the platform,” she says.

On Guernsey, an island in the English Channel famous for its high concentration of financial firms, Unigestion recently adapted a private investment fund to run on a distributed ledger. The fund is small, with Unigestion one of just two investors, but the firm believes private equity could be a big area of opportunity for blockchain technology.

“Our intent is to manage the whole life cycle of the fund on the blockchain,” says Arijit Das, a senior vice president at Northern Trust, which administers the fund on behalf of Unigestion.

For now, Unigestion’s new system is in shadow mode, mirroring the existing fund while Leblond awaits the results of a security report. In order for more blockchain-based projects to take hold, experts say the financial industry still needs to agree on standards, develop easy-to-use programming modules, and clarify regulatory uncertainties.

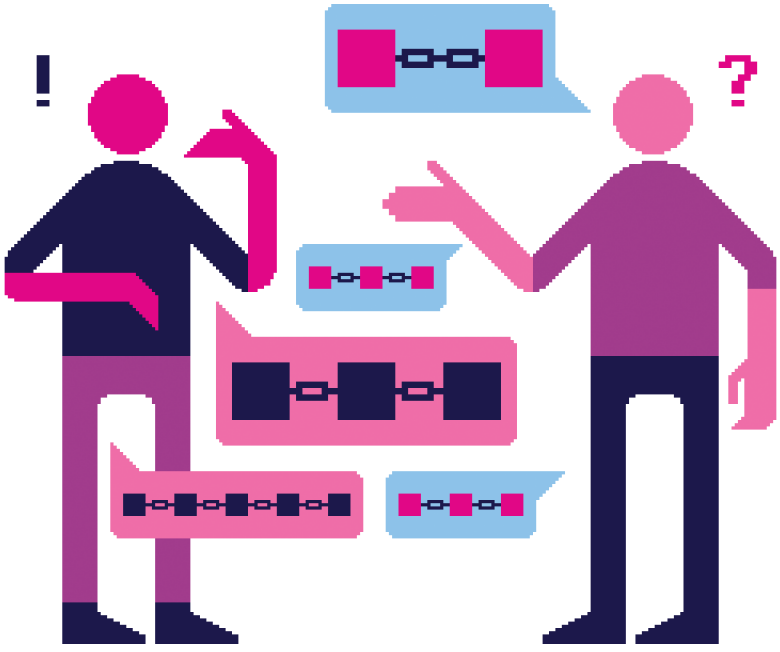
Working through those issues can be frustrating. That’s why Tom Jessop, who left his managing director job at Goldman Sachs earlier this year to become president of the startup Chain, says blockchains have momentarily slid into the “trough of disillusionment.” That’s the phase in the infamous Gartner “hype cycle” that follows the peak frenzy of investor interest and then, with luck, proceeds to a “plateau of productivity.”

Many firms are still waiting for that maturation in order to feel confident in rolling out blockchain-based systems. “Everyone’s a little skittish here because we’re dealing with real assets and real money,” says Hyperledger’s Behlendorf.

And if the financial industry truly wants to adopt blockchains as its own, it should practice extreme patience throughout this process. “You have to take baby steps,” says Tim Swanson, director of market research for R3. “Financial systems cannot break.”

Blockchain technology may well prove itself capable of handling many aspects of the financial system more aptly than humans ever could. Whether it will shift the balance from walled-off, corporate networks to wide-open, distributed systems will boil down to which we ultimately choose to trust. ■

↗ POST YOUR COMMENTS at http://spectrum.ieee.org/banking1017



Blockchain Lingo

BLOCKCHAIN: A shared database that grows only by appending new data, authenticates users with strong cryptography, and leverages economic incentives to encourage mistrustful strangers to manage and secure updates.

BLOCK SIGNERS: The actors in a **proof-of-stake** blockchain that are responsible for validating transactions and adding them to the blockchain.

ETHEREUM: A **public blockchain** designed to store and execute **smart contracts** and other complex software apps. It features its own cryptocurrency, ethers. The first version of the software was released in 2014.

HASH FUNCTION: An algorithm that digests a chunk of data of arbitrary size and turns it into a string of numbers and letters of fixed length, called a hash. The function is a one-way operation used in blockchains to choose which participants update the chain.

ICO: Initial coin offering. A way of funding new app development on blockchains, it involves the sale of cryptocurrency before the software is released to the public. The cryptocurrency typically gives users access to the app under development.

MINERS: The individuals that add new blocks to **public blockchains** that use **proof of work**, such as Bitcoin. Their actions both secure the entries on a public blockchain, and provide a mechanism for the distribution of new coins. They gain the right to add new blocks by spending computational resources, and the network rewards miners by allocating new coins to them.

ORACLE: An entity that records data about real-world events—such as the ambient temperature or the outcome of a presidential election—on a blockchain. It serves as a reference for **smart contracts**.

PERMISSIONED LEDGER: A database, inspired by blockchain technology, that restricts access to reading, writing, or both to a set of known actors. It’s also called a private blockchain.

PROOF OF STAKE: A mechanism for allocating the right to add new blocks of data to a **public blockchain**. Participants gain the right to add new blocks by proving they own cryptocurrency.

PROOF OF WORK: A mechanism for allocating the right to add new blocks of data to a **public blockchain**. Participants (**miners**) gain the right to add new blocks by repeatedly running a **hash function**.

PUBLIC BLOCKCHAIN: A blockchain that is open for anyone to look at and to add new blocks to. Certain resources (computing power, possession of the native cryptocurrency) may be required to add new blocks, but anyone has the right to do so.

SMART CONTRACTS: Software-based agreements deployed in systems capable of automatically executing and enforcing the terms of the contracts.

ILLUSTRATION BY **Nicholas Little**