Technology | DOI:10.1145/2994581

Sarah Underwood

Blockchain Beyond Bitcoin

Blockchain technology has the potential to revolutionize applications and redefine the digital economy.

IMAGE BY IMAGENTLE

BLOCKCHAIN TECHNOLOGY HAS attracted attention as the basis of cryptocurrencies such as Bitcoin, but its capabilities extend far beyond that, enabling existing technology applications to be vastly improved and new applications never previously practical to be deployed.

Also known as distributed ledger technology, blockchain is expected to revolutionize industry and commerce and drive economic change on a global scale because it is immutable, transparent, and redefines trust, enabling secure, fast, trustworthy, and transparent solutions that can be public or private. It could empower people in developing countries with recognized identity, asset ownership, and financial inclusion; and it could avert a repeat of the 2008 financial crisis, support effective healthcare programs, improve supply chains and, perhaps, clean up unethical behavior in high-value businesses such as diamond trading.

Blockchain, like the Internet, is an open, global infrastructure that allows companies and individuals making transactions to cut out the middleman, reducing the cost of transactions and the time lapse of working through third parties. The technology is based on a distributed ledger structure and consensus process. The structure allows a digital ledger of transactions to be created and shared between distributed computers on a network. The ledger is not owned or controlled by one central authority or company, and can be viewed by all users on the network.

When a user wants to add a transaction to the ledger, the transaction data is encrypted and verified by other computers on the network using cryptographic algorithms. If there is consensus among the majority of computers that the transaction is valid, a new block of data is added to the chain and shared by all on the network. Transactions are secure, trusted, auditable, and immutable. They also avoid the need for copious, often duplicate, documentation, third-party intervention, and remediation.

Blockchains can be either public and unpermissioned, allowing anybody to use them (bitcoin is a case in point) or private and permissioned, creating a closed group of known participants working, perhaps, in a particular industry or supply chain.

Michael Versace, global research director for digital strategies at research firm IDC, describes blockchain as an industry and innovation accelerator based on the capability of the third platform of technology—the first platform being mainframes and their networks, the second Internet, personal computers, and local area networks. The third platform delivers computing anywhere, immediately, and allows organizations to deploy and consume computing resources in shared communities.

Says Versace, "The core capabilities of the third platform of technology are beyond any we have seen before. Innovation accelerators like blockchain mean we can achieve technology value outcomes that we couldn't achieve before."

This is promising, but there are caveats. Sandeep Kumar, managing director of capital markets and a blockchain specialist at digital business consulting and technology services firm Synechron, names data privacy, scalability, and interoperability as three key challenges to blockchain technology that are pervasive across applica-

Benefits of Blockchain in Financial Services

Secure transactions

- **Avoid information leakage**
- **Reduce transaction time**
- **Remove transaction intermediaries**
- **Reduce risk of fraud and cybercrime**
- **Observe transactions in real time**

Source: IBM

Early Adopter Views on Blockchain

- **Platform openness is required.**
- **Features like identity, privacy, security, operations management, and interoperability need to be integrated.**
- **Performance, scale, support, and stability are crucial.**
- **Consortium blockchains, which are permissioned networks on which consortium members may execute contracts, are ideal.**

Source: Microsoft

tions and have not yet been solved cleanly. Other sticking points are data transfer, and integrating with existing systems and sometimes security, which depends on application coding.

Financial Applications

The financial services sector, which must innovate to cut the costs of legacy systems and manage increasing regulation, is leading the way with blockchain and taking advantage of the technology's security, immutability, transparency, and ability to cut out the middleman. Fintech startup R3, backed by over 40 global banks, is developing a standardized architecture for private ledgers that could significantly cut the cost and time of settling transactions. Similarly, the Linux Foundation's Hyperledger project is an industry initiative including tech giant IBM that is evolving open source technology and building the foundation of a standardized, production-grade digital ledger.

Deloitte is working with clients and startups to develop solutions including Smart Identity, which can support banks' regulatory client onboarding and Know Your Customer (KYC) processes, while individual financial institutions, insurance companies, exchanges, and solutions vendors also have thrown their weight behind blockchain.

Many are taking advantage of the technology's ability to act as a giant time stamp. Nasdaq is using its Linq blockchain technology to complete and record private securities transactions, and the Depository Trust & Clearing Corporation, working with market participants and technology firm Axoni, is managing post-trade events for credit default swaps. Regulators are also interested in the technology, as its transparency and integrity allow market activity to be monitored in real time.

These early applications show great potential, but there are problems around data privacy, scale and latency in financial markets. The privacy issue is about how much information needs to be exposed to verify a transaction. This could be more than at present and could compromise the privacy of a trade. Scale and latency are also issues in a market managing huge data volumes. These problems are being addressed by industry consortia and individual firms, but robust solutions remain elusive.

Commercial Applications

In the commercial world, two startups making progress with blockchain are Factom and Everledger.

Factom's focus is on securing data. The company is participating in the Honduran land registry project and working on a number of projects in China, including data infrastructure for 80 smart cities, financial technology solutions, and integrating blockchain technology with electronic data notarization services to enhance integrity in information management.

The company has also secured funding from the U.S. Department of Homeland Security's Science and Technology Directorate under the 'Blockchain Software to Prove Integrity of Captured Data from Border Devices' project.

Everledger's focus is on the identity and legitimacy of objects. Blockchain works well here because its history cannot be changed and it enables trust by consensus. The company's initial work provides a distributed ledger of diamond ownership and transaction history verification for owners, insurance companies, claimants, and law enforcement agencies. The system assists with prevention of fraud in the supply chain, but also helps consumers decide whether to buy particular diamonds.

Leanne Kemp, founder and CEO of Everledger, explains, "The ultimate goal is to track diamonds from mine to market, so that consumers can see if correct duties and taxes have been paid and whether a diamond is a 'blood diamond' that has been mined and traded in a war zone and contributed to human atrocity." The company also is considering applying its technology to other big-ticket items, such as fine art, vintage cars, and wine.

In addition, blockchain is expected to be well suited, with the addition of smart contracts that use computerized transaction protocols to execute the terms of contracts agreed by users of a blockchain, to applications such as product manufacturing, supply chain management, vehicle provenance, and sharing resources such as electricity.

Emin Gün Sirer, an associate professor of computer science at Cornell University and a participant in a number of blockchain projects, says blockchain could democratize the in-

The financial services sector takes advantage of blockchain's security, immutability, transparency, and ability to cut out the middleman.

surance industry by using smart contracts to pay out against insurance policies without policyholders having to make a claim. He adds: "The Internet of Things could be an enormous application area where people want to communicate with devices, but not through intermediaries. There is no killer app yet, but it is likely to feature the transparency of blockchain."

While start-ups can skip some of the challenges presented by blockchain technology, established firms must set up a network of blockchain participants, perhaps suppliers and customers, and agree on technology protocols. Commercial firms, like others, will also hit the interoperability barrier identified by Synechron and by Microsoft in feedback from early blockchain adopters. Kumar explains: "Blockchain is evolving in many ecosystems, such as Hyperledger and Ethereum, but there needs to be a native way to integrate blockchains that would allow, for example, a transaction on Hyperledger to invoke information from Ethereum."

Sirer warns of less-advantageous applications such as gambling and ongoing security problems. He cites the spectacular rise and fall of The DAO, a distributed autonomous organization based on Ethereum technology that acted as an investment vehicle, raising $220 million, then swiftly losing $53 million to a hacker. "We looked at the DAO code and found it was written so badly it was open to attack from nine different angles. Incidents like this uncover the need for more multi-disciplinary research on blockchain technology."

Developing Countries

The potential of blockchain is also diverse in developing countries, but where the commercial world is concentrating on outstanding technology challenges, developing countries are initially focusing on the trust element of blockchain.

Mariana Dahan, senior operations officer at the World Bank in charge of the 2030 development agenda and United Nations (U.N.) relations, says, "We believe blockchain is a major breakthrough and has great potential. It will make an impact on, and bring value to, any transaction that requires trust, a social resource that is all too often in short supply."

The potential of blockchain is diverse in developing countries, where the initial focus is on the trust element.

Dahan suggests the trust element of blockchain will play well into the 2030 Sustainable Development Goals adopted by U.N. members in 2015 and designed to end poverty, protect the planet, and ensure prosperity for all. More specifically, she notes high-potential applications of blockchain in land registration, digital identity, and finance for small and medium-sized enterprises.

Land registration and awareness of its relevance to issues such as food security, climate change, urbanization, and indigenous people's rights has increased over recent years, yet the Independent Evaluation Group of the World Bank says 70% of the world's population lacks access to proper land titling or demarcation.

Beginning to solve this problem are projects like one in the Republic of Georgia, where the National Agency of Public Registry is working with BitFury on a pilot project that will use a transparent, secure ledger to manage land titles and, if successful, cut property registration fees by up to 95%, increase transparency of land ownership, and reduce fraud. A similar project partially funded by the World Bank is being developed in Honduras, where Factom is working with the government to prototype a blockchain-based land registry.

Beyond land registration, Dahan explains how the ability to store and update property titles on a blockchain could, for the first time, allow poor people to assert reliable title claims to their homes and use them as collateral for borrowing. Small and medium-sized enterprises also could prove ownership of assets, perhaps equipment or livestock, and provide access to working capital and, by extension, a wider market.

Digital identity enabled by blockchain has the potential to change lives. Says Dahan, "If blockchain technology can be used to secure robust, self-sovereign digital identities around personal data, there's a real possibility that people in places with poor documents, registries and rules of law can establish trusted measures of their good reputation. This would allow them to assert who they are and access proof of their digital identity anywhere using a private key."

With the benefit of digital identity, many of the world's two billion unbanked individuals could store their identities on a blockchain, permission banks to fulfill regulatory requirements such as Know Your Customer, and gain access to bank accounts, loans, and other financial services previously inaccessible to them.

The potential of blockchain to revolutionize applications and drive global economic change is certainly there, but problems persist in wide-scale execution. As Kumar concludes: "Blockchain is not yet ready for prime time."

Further Reading

The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services,
World Economic Forum,
https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services/

Cuomo, J.
How Businesses and Governments Can Capitalize on Blockchain,
http://www.ibm.com/blogs/think/2016/03/16/how-businesses-and-governments-can-capitalize-on-blockchain/

Sirer. E.G.
Introducing Virtual Notary
Hacking, Distributed
http://hackingdistributed.com/2013/06/20/virtual-notary-intro/

Casey, M., and Dahan, M.
Blockchain technology: Redefining trust for a global, digital economy
http://blogs.worldbank.org/ic4d/blockchain-technology-redefining-trust-global-digital-economy?cid=EXT_WBBlogSocialShare_D_EXT

Sarah Underwood is a technology writer based in Teddington, U.K.