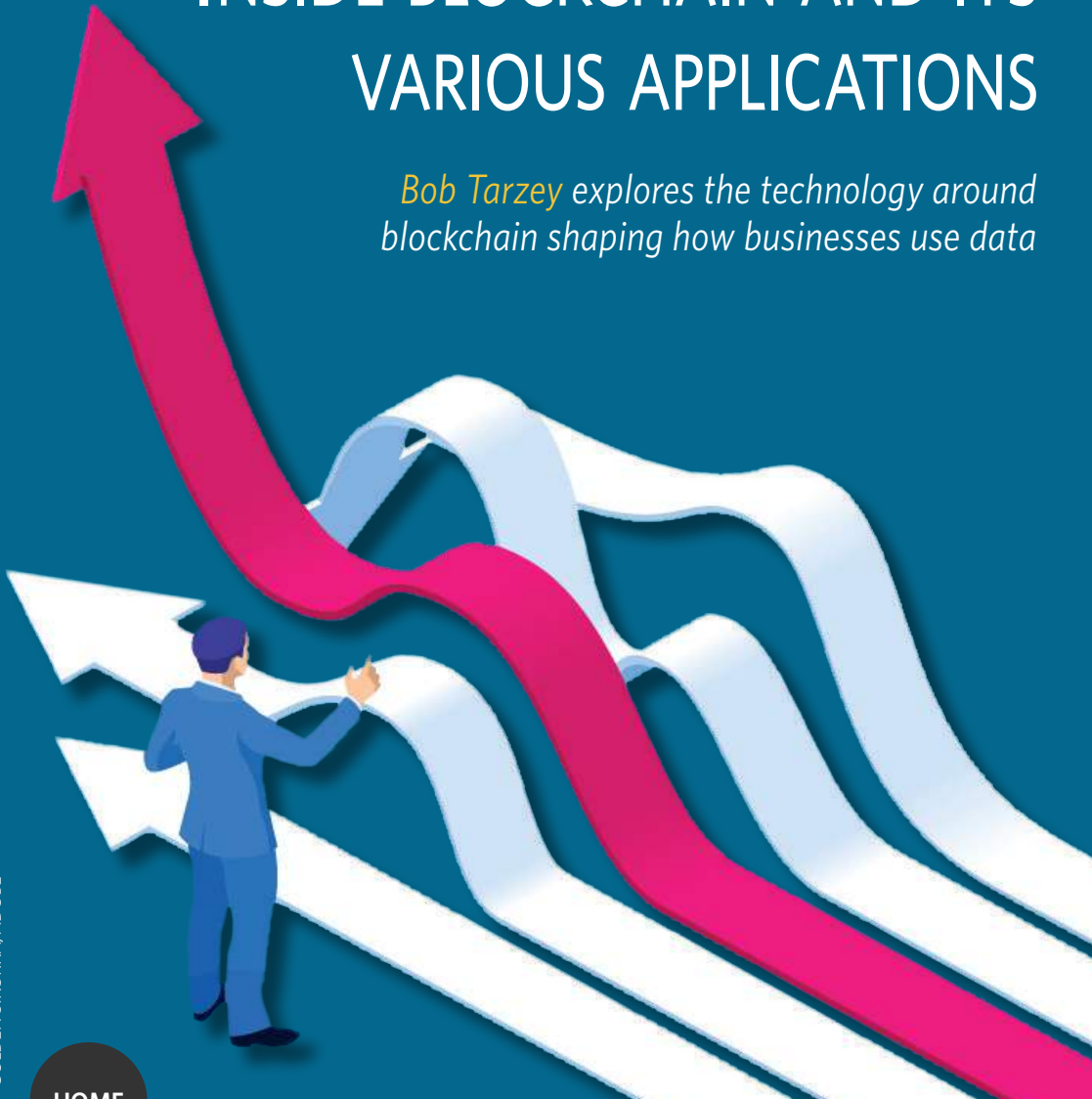


INSIDE BLOCKCHAIN AND ITS VARIOUS APPLICATIONS

Bob Tarzey explores the technology around blockchain shaping how businesses use data



GOLDEN SIKORKA/ADOBE

HOME

When people interact with each other, for example via financial transactions, sharing legal documents or trading through supply chains, they need a high level of confidence that the data recording their interaction is accurate and true.

A distributed ledger makes it possible to build applications where multiple parties can execute transactions online without the need to trust a central authority or indeed each other.

Over the past few years, the number of use cases for distributed ledgers, and their more specialised form, blockchains, has been increasing, as has the technology to support the underlying infrastructure and build applications on top of it.

With a distributed ledger, every user has their own full, or in some cases partial, copy of the database, referred to as a node, which can be a physical device, a [virtual machine](#) or a software container.

Each node runs the relevant software to provide the infrastructure management and the relevant application, including the ability to complete “smart contracts” that negotiate the direct exchange of assets between participating nodes.

CONSENSUS

For a transaction to proceed, all nodes must verify a transaction and agree its order on the ledger.

Doing so is termed “consensus”, which is necessary, for example, to avoid double counting or overspending when it comes to financial assets.

Consensus involves four steps, from the transaction being initiated to it being committed on all nodes with a timestamp

 Home

 News

 How IT departments can find different ways to upskill in the new economy

 Travel company Clarity bakes ThoughtSpot search and AI functions into analytics tool

 Digital factory approach signals a new departure for Network Rail's IT strategy

 Editor's comment

 Buyer's guide to blockchain

 Delivering cloud in the financial services sector

 How 5G will transform your business

 Downtime

providing a unique cryptographic signature. These steps can be completed in seconds or minutes, depending on the technology.

Blockchains are distinguished from other distributed ledgers in being updated by adding blocks of new transactions to create an immutable tamper-proof log of sensitive activity.

The right to write blocks may require proof-of-work – which can be time and resource intensive – the aim being to prevent, for example, mass updates by bots.

Nomenclature has become confusing as the two terms, distributed ledger and blockchain, have been used interchangeably, with the latter prevailing, being punchier and, perhaps, sounding more contemporary.

PUBLIC OR PRIVATE

Blockchains can either be public or private and require permission to update or not. Use cases range from international money transfers, managing shareholder records and legal contracts to recording the provenance of gemstones and the condition of goods in transport.

To date, the most high-profile use of blockchain has been to operate [cryptocurrencies](#), a way of exchanging and storing value online independent of central banks. From this has involved initial coin offerings (ICO), a way of using cryptocurrencies as an alternative to [initial public offerings](#) (IPO) for companies to raise capital.

With the oldest and highest profile blockchain application, bitcoin, it can take many minutes for consensus to be reached, which is why the cryptocurrency has a reputation for poor performance and scalability. It is also criticised for the datacentre power

it consumes in a process called mining, the form of proof-of-work, rewarded with bitcoins, used to add new blocks of transactions to the bitcoin blockchain.

As the use of blockchains has extended to other use cases, the aim has been to overcome these deficiencies.

Different approaches are enabled through frameworks which provide the basic architecture, protocol and network support.

Frameworks simplify the development, deployment and support of applications that access a given blockchain. There are several blockchain frameworks which compete and/or address different requirements.

FRAMEWORKS

The most widely used is [Ethereum](#), an open source public blockchain framework. The first implementations were in 2015, but it is already thought to account for 80% of blockchain-based projects.

Ethereum suits highly distributed requirements where the transparency of data to all users is important – for example, a customer loyalty network where retailers need to independently verify a user's activity to provide benefits.

Ethereum was the first platform to enable full-fledged smart contracts, which, for example, makes it quick and easy to launch ICOs. Ethereum is also the name of a cryptocurrency based on the platform.

The Linux Foundation's [Hyperledger Fabric](#) is an open source enterprise private blockchain framework suited to applications that require privacy and permission controls with a known set of members – for example, a financial application where certain

 Home

 News

 How IT departments can find different ways to upskill in the new economy

 Travel company Clarity bakes ThoughtSpot search and AI functions into analytics tool

 Digital factory approach signals a new departure for Network Rail's IT strategy

 Editor's comment

 Buyer's guide to blockchain

 Delivering cloud in the financial services sector

 How 5G will transform your business

 Downtime

trade-related data is only shared with select banks. In effect, it is a hub for the open development of blockchains for solving corporate tasks.

The project started in 2015 and has more than 100 participating companies which pay a membership fee, starting at \$50,000 per annum, enabling them to contribute software code to the project.

Waves is an open source blockchain platform created by a Russian company specifically for launching ICOs; a distant second to Ethereum for doing this. It includes a decentralised trading exchange. [Ripple](#) is an open source platform used as an international currency exchange for both cryptocurrencies and fiat currencies. It is designed to allow fast and cheap international transactions.

The NEM Foundation's platform claims the scalability and performance to suit a range of use cases, including financial payments, cryptocurrencies, equity markets and escrow services, using a consensus algorithm called proof-of-importance that provides privileges to participants with the best reputations.

SMART CONTRACT PLATFORM

EOS is a smart contract platform and decentralised operating system intended for the deployment of industrial-scale applications. It aims to eliminate transaction fees and be highly scalable. R3's Corda operates smart contracts, within the [Java Virtual Machine](#), and is aimed at financial institutions. Iota is



 Home

 News

 How IT departments can find different ways to upskill in the new economy

 Travel company Clarity bakes ThoughtSpot search and AI functions into analytics tool

 Digital factory approach signals a new departure for Network Rail's IT strategy

 Editor's comment

 Buyer's guide to blockchain

 Delivering cloud in the financial services sector

 How 5G will transform your business

 Downtime

an open source distributed ledger, customised to work with internet of things (IoT) applications providing feeless micro-transactions. JP Morgan's [Quorum](#) is Ethereum-based, claiming enterprise scalability and the ability to limit access to transaction history, while providing maximum transparency.

BLOCKCHAIN AS A SERVICE

Quorum has recently been selected by Microsoft as the first supported framework for its managed Azure Blockchain Service.

The aim of such managed, blockchain-as-a-service offerings is to avoid self-hosting of blockchain infrastructure, eliminating the need to provision hardware, configure software and set up networking and security components, as well as ease the development of applications on top of one or more frameworks.

The Microsoft Azure Blockchain Service was launched earlier in 2019, on top of earlier releases of a blockchain development kit and workbench. It integrates with Microsoft's Active Directory and Visual Studio, as well as a range of open source tools.

The Amazon Managed Blockchain was launched in December 2018 and supports both Hyperledger Fabric and Ethereum. [Amazon Web Services](#) (AWS) claims it enables the rapid creation of new blockchain networks that can span multiple AWS accounts, that can automatically scale to meet the demands of thousands of applications. It monitors the network and automatically replaces poorly performing nodes assigning processing power and memory flexibly, as would be expected on a managed platform.

The launch of the service means AWS now competes with some of its platform partners, such as ConsenSys's Kaleido.

The IBM Blockchain Platform, launched in 2017, is based on Hyper Ledger. It can be run on-premise or as a cloud service on a customer-chosen platform and includes a set of security services suited to the requirements of enterprise customers. Oracle also released a blockchain platform based on Hyperledger Fabric in February 2019.

SPECIALIST REQUIREMENTS

Alongside some of the IT industry's biggest names, many smaller, niche players are coming to market to serve specialist requirements and applications relating to blockchain.

Gospel Technology is a private permissioned blockchain aimed at safe data sharing. Use cases include human resources systems and pharmaceutical testing. To this end, it provides consensus on reads, as well as writes, ensuring that it is opaque about data, but open about who has accessed it.

Because Gospel is focusing on content as much as transactions, the data volumes involved can be high, so network nodes can store a subset of the data relevant to their needs. This also means it can make use of Byzantine fault tolerance, meaning it can continue to operate even if the status of certain nodes is unknown.

Gospel has just launched a version on the [Google Cloud Platform](#), however, customers can use other platforms such as AWS or Azure.

Modum is a Switzerland-based company currently operating mainly in Germany - with global plans. It partners with AWS and SAP. Its offering aims to automate, integrate and digitise supply chains, the initial focus market being pharmaceuticals.

 Home

 News

How IT departments can find different ways to upskill in the new economy

Travel company Clarity bakes ThoughtSpot search and AI functions into analytics tool

Digital factory approach signals a new departure for Network Rail's IT strategy

 Editor's comment

Buyer's guide to blockchain

Delivering cloud in the financial services sector

How 5G will transform your business

 Downtime

Modum provides an IoT-type device with a data logger to be included with transported goods to monitor environmental conditions, such as temperature and humidity to prove compliance with good distribution practices.

The data collected can be immutably secured in a blockchain and shared with stakeholders to add a layer of trust.

FRAUD PREVENTION

Tomia specialises in fraud prevention, traffic optimisation and roaming insights for mobile carriers. It provides real-time analytics and recently announced a partnership with Microsoft, [KPMG](#) and R3 to provide a blockchain-based system to optimise dispute management and help resolve billing and settlement disputes.

Quant Network's Overledger is a blockchain operating system providing the ability for applications to interact with multiple blockchains.

The need for many-to-many relationships between applications and databases is not new: it was one that had to be addressed in the 1980s and 1990s with the rising use of relational databases. Standards were introduced and the market consolidated. This is what will happen in the world of blockchains. Furthermore, blockchain is not a panacea: it will never suit many applications where central control, extremely high speed or the mass storage of unstructured data are required.

Blockchain merely provides another choice in the range of database options available. ■



SASHKIN/ADOBE

Copyright of Computer Weekly is the property of TechTarget, Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.