451 Research®

REPORT EXCERPT

THOUGHT LEADERSHIP

Blockchain Codex 2017

NOV 2017

Csilla Zsigri, Senior Analyst - Cloud Transformation & Blockchain CoE

Blockchain is the talk of the town, promising to revolutionize the way we do business with overwhelming disruptive force. As with any innovative technology, potential users need to understand blockchain's capabilities and benefits, and how it works, in order to apply it.

ABOUT 451 RESEARCH

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
1411 Broadway
Suite 3200
New York, NY 10018
P 212-505-3030
F 212-505-2630

SAN FRANCISCO
140 Geary Street
9th Floor
San Francisco, CA 94108
P 415-989-1555
F 415-989-1558

LONDON
Paxton House
(Ground floor)
30, Artillery Lane
London, E1 7LS, UK
P +44 (0) 207 426 1050
F +44 (0) 207 657 4510

BOSTON
75-101 Federal Street
5th Floor
Boston, MA 02110
P 617-598-7200
F 617-357-7495

ABOUT THE AUTHOR

CSILLA ZSIGRI

SENIOR ANALYST - CLOUD TRANSFORMATION & BLOCKCHAIN COE

Csilla Zsigri is a Senior Analyst for 451 Research's Cloud Transformation channel. Csilla also works on custom research, providing strategic guidance, as well as market and competitive intelligence, to technology vendors, service providers and enterprises. Previously, Csilla was a consultant on 451 Research's Advisory team, and before that she handled market intelligence and commercial exploitation in EU-funded research and innovation projects. Csilla is co-author of several forward-looking market studies prepared for the European Commission.

Executive Summary

INTRODUCTION

Blockchain promises to do for transactions what the internet did for information. Basically, anything of value, whether tangible or intangible – i.e., money, land, intellectual property or identity – can be represented digitally on a blockchain and be moved, stored and managed securely. Trust is established through clever code and peer consensus. Blockchain can eliminate inefficiencies by cutting out intermediaries and connecting the parties that are exchanging items of value directly. It can profoundly change the way we interact and operate today.

Before blockchain technology can take hold, however, people and organizations need to get educated about it, and there are still plenty of technology and business issues to overcome. The adoption process will likely be gradual and steady. It's like the internet in its first phase – complex and incomprehensible for most, but with huge potential for the future.

METHODOLOGY

This report equips the reader with an understanding of what blockchain is, how it works and how it can be applied in a business context. It also sheds some light on which organizations and industries are at the forefront of this nascent foundational technology. The analysis leverages interviews, reports and advisory work with enterprises, vendors, service providers and investors, as well as a Market Map™. Principal Analyst Carl Lehmann also contributed to the research included in this report.

451 Research Market Maps™ are designed to provide a view of the vendor landscape by major segment. The map highlights companies competing in multiple segments by connecting them through a circuit line. Identification and placement of companies into these segments is based on analysis, both published and unpublished, performed by 451 Research. This analysis includes interviews, reports and advisory work with several thousand enterprises, vendors, service providers and investors annually. 451 Research Market Maps™ are not intended to represent a comprehensive list of every vendor operating in this market. Inclusion on 451 Research Market Maps™ does not imply that a given vendor will be specifically featured in one or more 451 Research reports.

Reports such as this one represent a holistic perspective on key emerging markets in the enterprise IT space. These markets evolve quickly, though, so 451 Research offers additional services that provide critical marketplace updates. These updated reports and perspectives are presented on a daily basis via the company's core intelligence service, 451 Research Market Insight. Forward-looking M&A analysis and perspectives on strategic acquisitions and the liquidity environment for technology companies are also updated regularly via Market Insight, which is backed by the industry-leading 451 Research M&A KnowledgeBase.

Emerging technologies and markets are covered in 451 Research channels including Cloud Transformation; Customer Experience & Commerce; Data Platforms & Analytics; Datacenters & Critical Infrastructure; Development, DevOps & IT Ops; Information Security; Internet of Things; Managed Services & Hosting; Mobile Telecom; Multi-Tenant Datacenters; Networking; Storage; Systems & Software Infrastructure; and Workforce Productivity & Compliance.

Beyond that, 451 Research has a robust set of quantitative insights covered in products such as Voice of the Enterprise, Voice of the Connected User Landscape, Voice of the Service Provider, Cloud Price Index, Market Monitor, the M&A KnowledgeBase and the Datacenter KnowledgeBase.

All of these 451 Research services, which are accessible via the web, provide critical and timely analysis specifically focused on the business of enterprise IT innovation.

For more information about 451 Research, please go to: *www.451research.com*.

REPORT EXCERPT

Table of Contents

1. WHAT IS BLOCKCHAIN AND WHY IS IT IMPORTANT? 1

BLOCKCHAIN TYPES . . . 1

WHY IS IT IMPORTANT? . . . 2

2. HOW DOES IT WORK? 3

Figure 1: How Blockchain Works . . . 3

CONSENSUS PROTOCOLS . . . 4

Figure 2: Consensus Protocols . . . 4

CRYPTOGRAPHY . . . 4

DECENTRALIZED APPLICATIONS . . . 5

DIGITAL TOKENS AND INITIAL COIN OFFERINGS . . . 5

3. BLOCKCHAIN APPLICATIONS AND USE CASES 6

HORIZONTAL APPLICATIONS . . . 6

VERTICAL APPLICATIONS . . . 6

4. BLOCKCHAIN CONSORTIA AND VENDOR LANDSCAPE 8

Figure 3: 451 Research Blockchain Market Map™ . . . 8

CONSORTIA DRIVING BLOCKCHAIN ARCHITECTURE, PROTOCOLS AND CORE PLATFORMS . . . 9

Enterprise Ethereum Alliance . . . 9

Hyperledger Project . . . 9

R3 . . . 9

Trusted IoT Alliance . . . 9

W3C Community and Business Groups . . . 9

Figure 4: Core Blockchain Platforms/Protocols . . . 10

MAJOR VENDOR STRATEGIES . . . 10

IBM . . . 10

Microsoft . . . 10

Oracle *10*
NOTABLE STARTUPS 11
FUNDING AND M&A 12
Figure 5: Notable Blockchain M&A Transactions *12*

5. DRIVERS AND CHALLENGES **13**
DRIVERS 13
Decentralization and Consensus *13*
Efficiency Improvements *13*
Security and Privacy Enhancements *13*
Transparency and Auditability *13*
CHALLENGES 13
Nascent Frameworks and Development Tools *13*
Data Management *14*
Integration *14*
Latency vs. Scale and Consensus Protocols *14*
Minimum Viable Ecosystems *14*
Industry Standards *15*
Regulatory Efforts *15*
Security *15*
Business Models and Economics *15*

6. CONCLUSIONS **16**

7. FURTHER READING **17**

8. INDEX OF COMPANIES **18**

1. What Is Blockchain and Why Is It Important?

The following is an excerpt from an independently published 451 Research report, "Blockchain Codex 2017" released in November 2017. To purchase the full report or to learn about additional 451 Research services, please visit *https://451research.com/products* or email *sales@451research.com*.

The term 'blockchain' is often coupled with the term 'Bitcoin,' which creates a lot of confusion. Blockchain was born with Bitcoin, as the underlying technology developed in 2009 for creating and trading the Bitcoin virtual currency (also known as cryptocurrency). Bitcoin was created as a response to the 2008 financial crisis, with the goal of circumventing currency control by any centralized power and simplifying online transactions by cutting out intermediaries. Bitcoin is all about payments and, while its future is uncertain, its lasting legacy will be the blockchain. Simply put, Bitcoin is to blockchain what email is to the internet – its first 'killer app.'

At its simplest, a blockchain is a distributed and decentralized database, shared among known or anonymous participants, that maintains a continuous list of records (transactions). Participants decide which transactions are executed based on consensus and each of them keeps a copy of the database (chain of transactions). Rules in a blockchain are encoded and data is encrypted.

The same way there is no one 'cloud,' there is no single 'blockchain.' A blockchain can be used not only for financial transactions, but basically for everything that has value, whether tangible or intangible – i.e., money, land, intellectual property or identity. The deployment of blockchain technology initially focused on the financial services industry, but use cases in supply chain management, identity and contract management, data storage and the Internet of Things (IoT), among others, are being studied to determine blockchain's ability to enable new efficiencies and ways of doing business. Several are making their way into production.

BLOCKCHAIN TYPES

A public or permissionless blockchain network is open to anyone who wants to participate, and gives them the same privileges to view and authorize transactions. However, while the ledger itself is visible to all participants, the identity of the transacting parties is not revealed. A public blockchain typically has some kind of mechanism to encourage participants to join (e.g., cryptocurrencies used to pay for processing transactions to reward those nodes/computers underpinning the network). Examples are Bitcoin and Ethereum.

For some use cases, the anonymity of a public network and the exposure of all transaction data are not acceptable. A private or permissioned blockchain network requires an invitation validated by either the network starter itself or a set of rules the starter put in place. Businesses will typically set up private blockchain networks. Examples are Hyperledger Fabric and R3 Corda.

Between these two extremes lies the hybrid blockchain, which has a combination of public and private blockchain characteristics. Its network members can determine which data/transactions remain public and which are restricted to a smaller group of members. One example is Dragonchain.

WHY IS IT IMPORTANT?

In the quest for a more connected digital economy, businesses are still confronted with inefficiencies in processes, as well as cost- and security-related friction. Blockchain technology has the potential to make trade as frictionless as possible by reducing all sorts of market barriers (such as bureaucracy, regulations, fraud, intermediaries, etc.) that slow down and add costs to the different interactions within a business and among businesses.

With the blockchain:

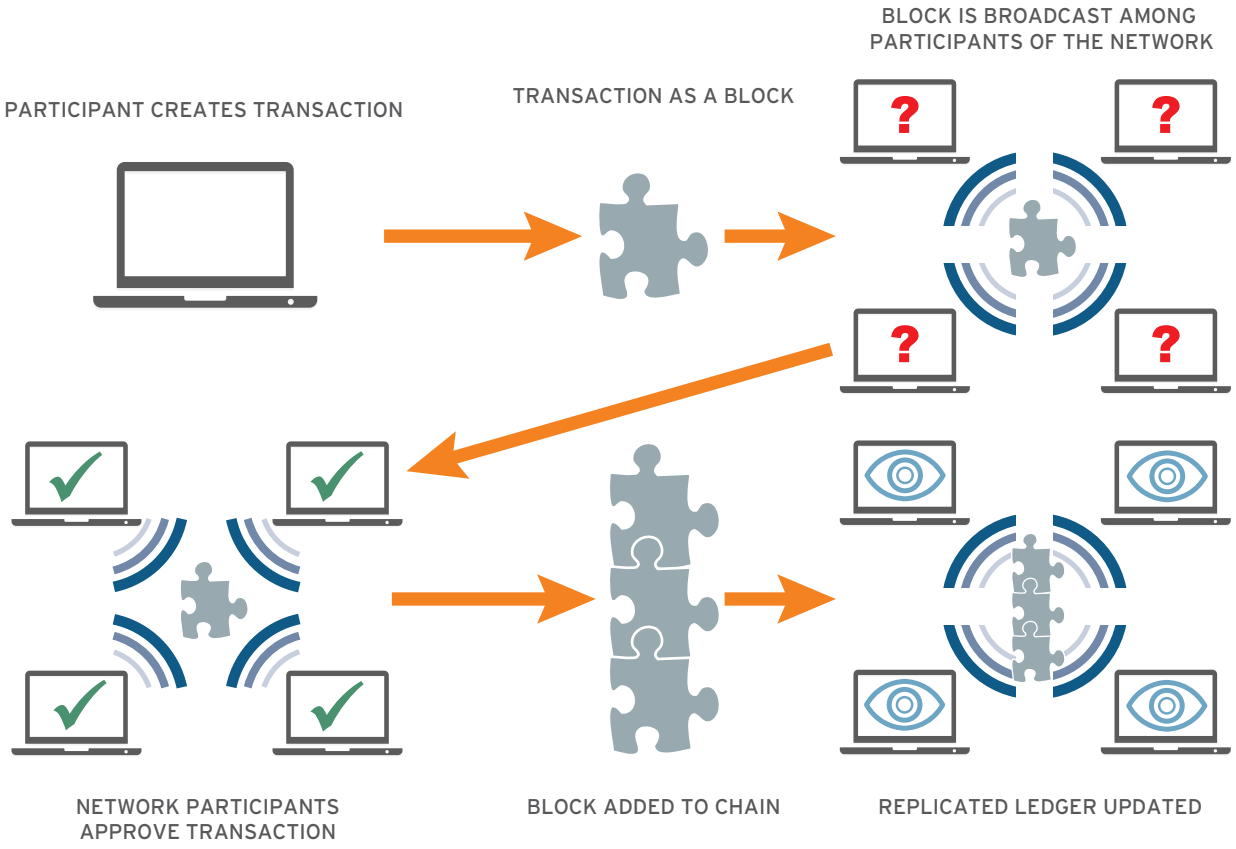
- Trust becomes intrinsic. Integrity is encoded in every step of the process and not bestowed on a single participant or a third-party authority. Blockchain promotes a single source of truth, and with transparency as a norm, trust becomes business as usual.
- Power is distributed throughout the network. Every transaction is broadcast across the network and its execution is consensus-based.
- Data is encrypted and private to the network participants. No data is stored in a central location (unless so required by a specific use case) and in a permissioned blockchain, participants can determine the level of privacy they want to have for a particular transaction.
- Ownership rights are encoded and preserved. Intellectual property creators can be compensated for the value they create.
- Bureaucracy is eliminated by cutting out the middlemen. Transaction speed increases while transaction cost decreases.
- Inclusion is promoted by low barriers to participation. Basically, anyone and anything with an internet connection can hook up to a public blockchain.
- Co-creation of value is promoted by connecting vendors and consumers directly.

2. How Does It Work?

A blockchain is a distributed and decentralized database, shared among known or anonymous participants, that maintains a continuous list of records (transactions). Participants in a blockchain do so using technology called blockchain nodes. Each blockchain node (a computer connected to the network) uses cryptography to secure strings of records (called blocks). Algorithms enable consensus among participants that new records are valid, and reject them if this consensus is not reached. Blockchain tracks the chronology of records (provenance), and ensures that records cannot be modified after being created (immutability). Each block includes a transaction and the reference to the previous block. This linear chain of blocks is replicated across all participating nodes, so that every participant is aware of all the transactions. Figure 1 illustrates the process.

Figure 1: How Blockchain Works

Source: 451 Research, 2017



A blockchain builds trust among participants as peers without the need for a central authority, by distributing and securing records management, and authenticating records using distributed consensus algorithms. Any participant can thus confidently engage in transactions or commerce with any other participant in the blockchain. Using a blockchain does not magically eliminate the possibility of fraud, but it makes it nearly impossible, or at least economically or practically unfeasible.

The blockchain's components – distributed database, cryptographic hashes and consensus protocols – are nothing new, but combined, they create a new way for sharing data and transferring assets.

CONSENSUS PROTOCOLS

The consensus mechanism is the essence of blockchain. Consensus protocols are distributed protocols, governed by multiple parties, for deciding which transactions are executed. (Different blockchains may use different algorithms to achieve consensus.) They guarantee the integrity and consistency of the blockchain across distributed nodes. Consensus protocols are not new inventions – they have been a topic of active research for decades and a wide variety are used today.

The Bitcoin blockchain, where participants are anonymous, uses the proof-of-work (PoW) consensus mechanism (a concept which was first presented by Cynthia Dwork and Moni Naor in a journal in 1993, and formalized in a paper by Markus Jakobsson and Ari Juels in 1998), where the process by which transactions are verified and added to the blockchain is called mining. PoW is basically an economic measure to deter service abuses on a network by requiring some work from the service requester. Miners (validators) compete to process and add a new block (transaction) to the blockchain. As participants can't rely on the identity of the miners to select who creates the next block, miners need to solve a complex cryptographic problem using a lot of computing resources. This can take from one minute up to one hour; on average it's about 10 minutes. The miner that finds the right answer (the right hash value) first, often the miner with the most powerful computer, gets to create the next block and receives a reward for it – in this case, a set quantity of new Bitcoins. In some ways, it's like mining gold.

The proof-of-stake (PoS) model requires miners to invest in the cryptocurrency or token of the blockchain system, and the algorithm then selects miners for block creation in a pseudorandom manner. Ethereum is developing a PoS algorithm called Casper, to which it expects to switch in the future.

The Byzantine Fault Tolerance (BFT) algorithm and its variation SIEVE are protocols supported by the permissioned Hyperledger blockchain. In a nutshell, the BFT algorithm makes nodes agree on an input by majority voting before moving on to execute what was decided (order-then-execute). The SIEVE protocol first executes operations speculatively and then agrees on the output of the operation (execute-then-order). In this latter case, operations with diverging results are rejected.

Figure 2: Consensus Protocols

Source: 451 Research, 2017

	POW	POS	BFT (AND DERIVATIVES)
BLOCKCHAIN TYPE	Permissionless	Permissionless/Permissioned	Permissioned
SCALABILITY OF NETWORK (PEERS/NODES)	High	High	Low
TRANSACTION FINALITY	Probabilistic	Probabilistic	Immediate
TRANSACTION VALIDATION TIME	High	Low	Low
CRYPTOCURRENCY/NATIVE TOKEN	Yes	Yes	No
COST OF PARTICIPATION	Yes	Yes	No

CRYPTOGRAPHY

Cryptography is a mature science – it has been researched and used for decades, particularly in the financial services markets. At its simplest, it can be thought of as the art of 'secret writing.' Cryptography (along with permissions) helps ensure privacy on the blockchain network, as well as preventing fraud and unauthorized access to transaction details. Digital signatures are typically standard components of cryptographic protocols and help authenticate the source of digital messages (data and transactions).

In a blockchain, a cryptographic hash function takes the information in each block and creates a unique string of characters, also known as a hash or hash value. The hash of a block is added to the data in the next block, where the function creates a new hash, and this goes on in all subsequent blocks. If someone tries to alter a previously created block, the hashes in the subsequent blocks will not match up anymore. Since all participants keep copies of the entire blockchain, a mismatch would raise the alarm and reject the block.

DECENTRALIZED APPLICATIONS

There are countless software applications in use today, and most of them follow a centralized model. Some of them are distributed and a few novel ones are decentralized. People often confuse distributed systems with decentralized ones. Distributed means that computation is spread across multiple nodes; decentralized means that no node is instructing any other node – if one node fails, the network is still able to operate. Blockchain applications are typically both distributed and decentralized. Any task that can be written as a piece of code can be automated and any multi-party application that relies on a central server can be disintermediated by a blockchain.

A blockchain application can be exclusively about money (e.g., Bitcoin), involve money (e.g., decentralized cloud storage) or have nothing to do with money (e.g., digital identity and voting).

Centralized applications control the operation of individual units and the flow of information from a central point. With decentralized applications, individuals are not dependent on a central power to send or get information. Participants – vendors and consumers – are connected directly. The concept of decentralized applications is one of the most novel and innovative ideas to emerge from the blockchain community.

Bitcoin could be considered the first decentralized application. Another popular group of decentralized applications running on blockchain are smart contracts, also known as self-executing or digital contracts, which are computer protocols/algorithms that automatically enforce and execute the terms of a contract whenever its conditions are met. (The concept of smart contracts was first proposed 20 years ago by cryptographer Nick Szabo.) When aggregated, smart contracts can stretch corporate boundaries and make businesses resemble networks; as the level of automation increases, these can become decentralized autonomous organizations that require little to no human intervention unless anomalies occur.

DIGITAL TOKENS AND INITIAL COIN OFFERINGS

There are blockchain systems that can't run without an incentive scheme for validating transactions or creating blocks. These schemes operate via native or intrinsic tokens. Examples of native tokens include cryptocurrencies like Bitcoin or Ether.

Utility tokens are created to promote the use of a new platform or service. These tokens can be purchased, typically using cryptocurrencies. Examples include Dragonchain, Filecoin or Storj.

Initial coin offerings (ICOs) are driving interest in the blockchain startup scene as a way to crowdsource the purchase and use of digital tokens and to fund new projects. Tokens in an ICO enable owners to participate in an element of an emerging company's service, but are an unregulated and overheated market that seems to be growing well ahead of blockchain's business applications. There is a lot of experimentation in business models, and product development takes place in a background of market volatility.

Not all blockchain systems need a token. For example, in a permissioned blockchain network, participants may be contractually obligated to validate transactions and create blocks.