Blockchain Technology

In the U.S. Government

Compiled and Edited by

Michael Erbschloe

Connect with Michael on LinkedIn

©2018 Michael Erbschloe

Table of Contents

About the Editor

Michael Erbschloe has worked for over 30 years performing analysis of the economics of information technology, public policy relating to technology, and utilizing technology in reengineering organization processes. He has authored several books on social and management issues of information technology that were published by McGraw Hill and other major publishers. He has also taught at several universities and developed technology-related curriculum. His career has focused on several interrelated areas:

- Technology strategy, analysis, and forecasting
- Teaching and curriculum development
- Writing books and articles
- Publishing and editing
- Public policy analysis and program evaluation

Books by Michael Erbschloe

Threat Level Red: Cybersecurity Research Programs of the U.S. Government (CRC Press)
Social Media Warfare: Equal Weapons for All (Auerbach Publications)
Walling Out the Insiders: Controlling Access to Improve Organizational Security (Auerbach Publications)
Physical Security for IT (Elsevier Science)
Trojans, Worms, and Spyware (Butterworth-Heinemann)
Implementing Homeland Security in Enterprise IT (Digital Press)
Guide to Disaster Recovery (Course Technology)
Socially Responsible IT Management (Digital Press)
Information Warfare: How to Survive Cyber Attacks (McGraw Hill)
The Executive's Guide to Privacy Management (McGraw Hill)
Net Privacy: A Guide to Developing & Implementing an e-business Privacy Plan (McGraw Hill)

Introduction

Blockchains are immutable digital ledger systems implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority. At its most basic level, they enable a community of users to record transactions in a ledger public to that community such that no transaction can be changed once published.

Blockchains are a new information technology that have the potential to invert the cybersecurity paradigm. First, blockchain networks are trustless: they assume compromise of the network by both insiders and outsiders. Second, blockchains are transparently secure: they do not rely on failure-prone secrets but rather on a cryptographic data structure that makes tampering both exceptionally difficult and immediately obvious. Finally, blockchain networks are fault tolerant: they align the efforts of honest nodes to reject those that are dishonest. As a result, blockchain networks not only reduce the probability of compromise but also impose significantly greater costs on an adversary to achieve it. The Air Force, for example, will research and develop blockchain technology and leverage it for national defense.

A blockchain is a shared, distributed, tamper-resistant database that every participant on a network can share—but that no one entity controls. In other words, a blockchain is a database that stores digital records. The database is shared by a group of network participants, all of whom can submit new records for inclusion. However, those records are only added to the database based on the agreement, or consensus, of a majority of the group. Additionally, once the records are entered, they can never be changed or erased.1 In sum, blockchains record and secure digital information in such a way that it becomes the group's agreed-upon record of the past.

The blockchain was first proposed in 2008 by Satoshi Nakamoto (a pseudonym) in conjunction with the cryptocurrency Bitcoin. Nakamoto's vision was to "allow online payments to be sent directly from one party to another without going through a financial institution." However, without a trusted central authority to oversee accounts and transactions, there would be no way to prevent dishonest actors from spending a single Bitcoin twice. Nakamoto's solution was a distributed database of time-stamped, consensus-based, cryptographically tagged transactions that form a record that cannot be changed—a blockchain. Bitcoin became a reality in 2009, and since then its market capitalization has gone from zero to more than $6.3 billion as of April 2016. Each day, some of Bitcoin's 6.6 million users exchange more than $75 million in 120,000 transactions across the network.

Bitcoin offers a noteworthy example of a blockchain's potential. All of Bitcoin's currency, transactions, and accounts that have ever existed are recorded in a blockchain database that lives on the open Internet. It is fully exposed to the hostile efforts of governments, criminal organization, and hackers. Yet, the Bitcoin blockchain has never been hacked. Clearly, this technology deserves study.

While "the blockchain" was virtually synonymous with Bitcoin for several years, it should be made clear that they are two separate technologies. Bitcoin is just the first popular application of blockchain, just as e-mail was the first popular application of the Internet.6 Its potential is so vast, in fact, that advocates compare the maturity and innovative potential of blockchain technology today to that of the Internet in 1992, an Internet before the World Wide Web. However, because blockchain technology simply rides on the existing Internet infrastructure, the maturity of blockchain technology is likely to progress three times faster than the Internet, with mainstream use expected within the next eight years.

Industry has recognized the potential of blockchain technology. Since 2013 more than $1 billion of venture capital has been invested into 120 blockchain start-ups. Aims are diverse, ranging from finance to the tracking and trade of indivisible assets (such as diamonds and art) to digital notary services that can serve as evidence in a court of law; however, interest has expanded beyond just start-ups. Large, mature companies such as Lockheed Martin, IBM, and Goldman Sachs have also begun investigating potential blockchain applications in their respective sectors.

Blockchains solve a challenging problem in data science: how to reliably exchange information over an unreliable network on which some of the participants cannot be trusted. The blockchain security model inherently assumes that these dishonest participants will attempt to create friction by not only generating false data but also attempting to manipulate valid data passed from honest participants. By using a variety of messaging and consensus techniques, blockchains ensure data integrity by both rejecting invalid data and preventing valid data from being secretly modified or deleted.

Blockchain technology is worthy of examination because it offers three significant advantages over traditional cyber defense strategies. First, rather than trying to defend boundaries from compromise, blockchains assume compromise by both adversaries and trusted insiders. They are designed to defend data in a contested cyber environment. Second, blockchain networks harness the aggregate power of the network to actively resist the efforts of malicious actors. Specifically, blockchains take advantage of the asymmetry of many against few. Finally, the security that blockchains provide is not dependent on secrets or trust. There are no passwords to be exposed, cryptographic keys to be protected, or administrators to be trusted. Blockchains provide an inherent security function on which additional security functions can be added, depending on the application. As result of these advantages, blockchains are capable of operating successfully and securely on the open Internet, without a trusted central authority, while fully exposed to hostile actors.

This paper examines the blockchain activities of the U.S. Government.

Source: http://www.airuniversity.af.mil/CyberCollege/Portal/Article/Article/1238526/blockchain-technology/

Blockchain Technology Overview NISTIR 8202

Aiming to clarify the subject for the benefit of companies and other organizations, the National Institute of Standards and Technology (NIST) has released a straightforward introduction to blockchain, which underpins Bitcoin and other digital currencies.

Virtual barrels of digital ink are flowing in the media nowadays about these cryptocurrencies and the underlying blockchain technology that enables them. Much of the attention stems either from the giddy heights of value attained lately by the most well-known of these currencies, Bitcoin, or from the novelty of blockchain itself, which has been described (link is external) as the most disruptive technology since the internet. Blockchain's proponents believe it lets individuals perform transactions safely without the costs or security risks that accompany the intermediaries that are required in conventional transactions.

The NIST report's authors hope it will be useful to businesses that want to make clear-eyed decisions about whether blockchain would be an asset to their products.

"We want to help people understand how blockchains work so that they can appropriately and usefully apply them to technology problems," said Dylan Yaga, a NIST computer scientist who is one of the report's authors. "It's an introduction to the things you should understand and think about if you want to use blockchain."

The NIST document, whose full title is Draft NIST Interagency Report (NISTIR) 8202: Blockchain Technology Overview (link is external), introduces the concept of blockchain, discusses its use in electronic currency, and shows its broader applications.

A blockchain is essentially a decentralized ledger that maintains transaction records on many computers simultaneously. Once a group, or block, of records is entered into the ledger, the block's information is connected mathematically to other blocks, forming a chain of records. Because of this mathematical relationship, the information in a particular block cannot be altered without changing all subsequent blocks in the chain and creating a discrepancy that other record-keepers in the network would immediately notice. In this way, blockchain technology produces a dependable ledger without requiring record-keepers to know or trust one another, which eliminates the dangers that come with data being kept in a central location by a single owner.

The blockchain idea has attracted enough supporters that there are now several hundred digital currencies on the market (link is external), and the companies that are investigating ways to employ blockchain number many more. Because the market is growing so rapidly, several stakeholders, customers and agencies asked NIST to create a straightforward description of blockchain so that newcomers to the marketplace could enter with the same knowledge about the technology.

“Blockchain is a powerful new paradigm for business,” Yaga said. “People should use it—if it’s appropriate.”

The question is when it is appropriate. As with any new tool, there can be a temptation to employ it purely for its novelty value. The report outlines some possible use cases, including banking, supply chain management and keeping track of insurance transactions. The report, Yaga said, was created partly to help IT managers make informed decisions about whether blockchain is the right tool for a given task.

“In the corporate world, there’s always a push to adopt new technologies,” Yaga said. “Blockchain is today’s shiny new toy, and there’s a big push to adopt it because of that.”

“We want to help people to see past the hype,” he said, “as lofty a goal as that is.”

NIST has been tasked before with writing definitions of emerging concepts in information technology, such as the definition of cloud computing it released in 2011. While Yaga describes the blockchain description as approachable—it’s “as high-level as I can write it,” he said—the document is longer than some other NIST definitions because the technology combines so many complex ideas. Among them are digital signatures, peer-to-peer networking and hash chains, all of which are tools common in cryptography and with which NIST has had extensive involvement.

“We don’t have any axe to grind or product to sell, though,” Yaga said. “A lot of articles you’ll read online feature a disclaimer indicating that the author owns a certain amount of cryptocurrency or stock in a company. I have no vested interest in the monetary value of these networks. But we don’t pass judgment on the technology; we just want to get past the rumors.”

To that end, Yaga said, the document began as a sort of FAQ addressing falsehoods the authors had come across—such as the idea that there was no need for trust in the system. (“You do need trust,” he said, “just not a trusted third party, like a bank.”) It expanded to discuss the technical tools common to most blockchain-based systems and also explored related issues, such as the high demands blockchain systems place on network resources. The roughly 60-page report might enlighten anyone who wants a picture of blockchain that is not skewed to any players’ interests, but will give perspective to technical decision makers in particular.

“A company’s IT managers need to be able to say, we understand this, and then be able to argue whether or not the company needs to use it based on that clear understanding,” he said. “Some people are saying you should use it everywhere for everything. We wrote with the perspective that you shouldn’t use it if it’s not necessary.”

Source: https://www.nist.gov/news-events/news/2018/01/nist-report-blockchain-technology-aims-go-beyond-hype

This publication is intended to provide a high-level technical overview of blockchain technology. It discusses its application for electronic currency as well as broader uses. The document looks at different categories and approaches for different blockchain platforms.

This document is intended to help readers to understand the technologies which comprise blockchain systems and to understand how blockchains can be appropriately and usefully applied to technology problems.

Section 1 provides an introduction to the topic of blockchain technology.

Section 2 defines the high-level components of a blockchain system architecture, including hashes, transactions, ledgers, blocks, and blockchains.

Section 3 discusses how a blockchain is expanded through the addition of new blocks representing sets of transactions.

Section 4 examines the need for consensus models to resolve conflicts among blockchain mining nodes.

Section 5 introduces the concept of forking.

Section 6 defines and discusses smart contracts.

Section 7 looks at blockchain permission models, discusses their application considerations, and provides use case examples for each model.

Section 8 provides several examples of blockchain platforms in use today to indicate the variations from one platform to another.

Section 9 highlights some of the limitations of blockchain technology.

Section 10 gives a short conclusion for the document.

Appendix A contains a glossary for selected terms defined in the document.

Appendix B provides a list of acronyms and abbreviations used in the document.

Appendix C defines the references used throughout the document.

Source: https://csrc.nist.gov/publications/detail/nistir/8202/draft#pubs-abstract-header

Executive Summary

Blockchains are immutable digital ledger systems implemented in a distributed fashion (i.e.,without a central repository) and usually without a central authority. At their most basic level, they enable a community of users to record transactions in a ledger that is public to that community, such that no transaction can be changed once published. In 2008, the blockchain idea was combined in an innovative way with several other technologies and computing concepts to enable the creation of modern cryptocurrencies: electronic money protected through cryptographic mechanisms instead of a central repository. The first such blockchain based approach was Bitcoin. These currency blockchain systems are novel in that they store value, not just information. The value is attached to a digital wallet—an electronic device (or software) that allows an individual to make electronic transactions. The wallets are used to sign transactions sent from one wallet to another, recording the transferred value publicly, allowing all participants of the network to independently verify the validity of the transactions. Each participant can keep a full record of all transactions, making the network resilient to attempts to alter that record (or forge transactions) later.

Because there are countless news articles and videos describing the "magic" of the blockchain, this paper aims to describe the method behind the magic (i.e., how a blockchain system works). Arthur C. Clarke once wrote, "Any sufficiently advanced technology is indistinguishable from magic" [1]. Clarke's statement is a perfect representation for the emerging use cases for blockchain technology. There is a high level of hype around the use of blockchains, yet the technology is not well understood. It is not magical; it will not solve all problems. As with all new technology, there is a tendency to want to apply it to every sector in every way imaginable.

This document attempts bring a high-level understanding of the technology so that it can be applied effectively.

As stated above, blockchain technology is the foundation of modern cryptocurrencies, so named because of blockchain's heavy usage of cryptographic functions. Users utilize public and private keys to digitally sign and securely transact within the system. Users of the blockchain may solve puzzles using cryptographic hashing in hopes of being rewarded with a fixed amount of the cryptocurrency. However, blockchain technology is more broadly applicable than its application to cryptocurrencies. In this work, we try to show this broader applicability while still focusing to a large extent on the cryptocurrency use case (since that is the primary use case today).

Organizations considering implementing blockchain technology need to understand important aspects of the technology. For example, what happens when an organization implements a blockchain system and then decides they need to make modifications to the data stored? When using a database, this can be accomplished through a simple query (or major changes can be made by updating the database schema or software). However, on a blockchain, it is much more difficult to change data or update the 'database' software. Organizations need to understand the

extreme difficulty in changing anything that is already on the blockchain, and that changes to the blockchain software may cause forking of the blockchain. Another critical aspect of blockchain technology is how the participants agree that a transaction is valid. This is called “reaching consensus”, and there are many models for doing so, each with positives and negatives for a specific business case.

Some existing blockchain technologies focus on storing wealth, while 154 others are a platform for smart contracts (software which is deployed on the blockchain itself, and executed by the computers running that blockchain). New blockchain technologies are being developed constantly to enable new use cases and to improve the efficiency of existing systems. Some blockchain implementations are permissionless, meaning anyone can read and write to them.

Other implementations limit participation to specific people or companies, allow finer-grained controls, and may be managed by a central entity. Knowing these specifics allows an organization to understand what will be most applicable to its needs.

Despite the many variations of blockchain systems and the rapid development of new technologies, most blockchains use some common core concepts. Each transaction involves one or more addresses and a recording of what happened, and it is digitally signed. Blockchains are comprised of blocks, each block being a group of transactions. All the transactions in a block are grouped together, along with a cryptographic hash of the previous block. Finally, a new hash is created for the current block’s header to be recorded within the block data itself as well as within the next block. Over time, each block is then chained to the previous block in the chain by adding the hash of the previous block to the header of the current block.

Each technology used in a blockchain system takes existing, proven concepts and merges them together in a way that can address problems that were previously difficult. This document explores the fundamentals of how blockchain technologies work, how the participants in the network come to agree whether a transaction is valid, what happens when changes need to be made to an existing blockchain deployment, and how permissions work. Additionally, this document explores specific blockchain applications and examples of when to consider using a blockchain system.

The use of blockchain technology is not a silver bullet, and there are issues that must be considered such as how to deal with malicious users, how controls are applied, and the limitations of any blockchain implementation. That said, blockchain technology is an important concept that will be a basis for many new solutions.

For more information visit https://csrc.nist.gov/publications/detail/nistir/8202/draft#pubs-abstract-header

Table of Contents

263

Blockchain at the GSA

Federal agencies are eager to better evaluate and adopt distributed ledger technologies (like blockchain) that use encryption and coding to improve transparency, efficiency and trust in information sharing. Blockchain use cases that agencies submit for exploration touch many parts and processes of an organization, including:

- Financial management
- Procurement
- IT asset and supply chain management
- Smart contracts
- Patents, Trademarks Copyrights, Royalties
- Government-issued credentials like visas, passports, SSN and birth certificates
- Federal personnel workforce data
- Appropriated funds
- Federal assistance and foreign aid delivery

GSA's Emerging Citizen Technology Office launched the U.S. Federal Blockchain program for federal agencies and U.S. businesses who are interested in exploring distributed ledger technology and its implementation within government.

We hosted the first U.S. Federal Blockchain Forum on July 18, 2017, uniting more than 100 federal managers from dozens of unique agencies to discuss use cases, limitations, and solutions. Agency teams submitted their own potential use cases for blockchain technology to our current repository of almost 200 submissions.

Get Involved: If you are a government employee with a .gov or .mil email address, join our Federal Blockchain Community.

To join our public listserv for Blockchain, contact listserv@listserv.gsa.gov with the message body"SUB BlockchainPublic."

Source: https://www.gsa.gov/technology/government-it-initiatives/emerging-citizen-technology/blockchain

Use of Blockchain in Health IT and Health-related Research Challenge

The goal of this Ideation Challenge was to solicit White Papers that investigate the relationship between Blockchain technology and its use in Health IT and/or health-related research. The paper should discuss the cryptography and underlying fundamentals of Blockchain technology, examine how the use of Blockchain can advance industry interoperability needs expressed in the Office of the National Coordinator for Health Information Technology's (ONC) Shared Nationwide Interoperability Roadmap, as well as for Patient Centered Outcomes Research (PCOR), the Precision Medicine Initiative (PMI), delivery system reform, and other healthcare delivery needs, as well as provide recommendations for Blockchain's implementation. In addition to a monetary award, winners may also have the opportunity to present their White Papers at an industry-wide "Blockchain & Healthcare Workshop" co- hosted by ONC and NIST.

ONC selected the winning papers based on several factors, including the papers' proposed solutions or recommendations for market viability; creativity; ability to inform and foster transformative change; and potential to support a number of national health and health information objectives, including advancing the flow of health information for where and when it is needed most.

The final winners were:

1. **Blockchain and Health IT: Algorithms, Privacy, and Data [PDF – 507 KB].** A peer-to-peer network that enables parties to jointly store and analyze data with complete privacy that could empower precision medicine clinical trials and research.
   Authors: Ackerman Shrier A, Chang A, Diakun-thibalt N, Forni L, Landa F, Mayo J, van Riezen R, Hardjono, T.
   Organization: Project PharmOrchard of MIT's Experimental Learning "MIT FinTech: Future Commerce."

2. **Blockchain: Securing a New Health Interoperability Experience [PDF – 609 KB].** Blockchain technologies solutions can support many existing health care business processes, improve data integrity and enable at-scale interoperability for information exchange, patient tracking, identity assurance, and validation.
   Authors: Brodersen C, Kalis B, Mitchell E, Pupo E, Triscott A.
   Organization: Accenture LLP
3. **Blockchain Technologies: A Whitepaper Discussing how Claims Process can be Improved [PDF – 1 MB].** Smart contracts, Blockchain, and other technologies can be combined into a platform that enables drastic improvements to the claims process and improves the health care experience for all stakeholders.
   Author: Culver K.
   Organization: Unaffiliated
4. **Blockchain: Opportunities for Health Care [PDF – 787 KB].** Presentation of an implementation framework and business case for using Blockchain as part of health information exchange to satisfy national health care objectives.
   Authors: Krawiec RJ, Barr D, Killmeyer K, Filipova M, Nesbit A, Israel A, Quarre F,

Fedosva K, Tsai L.
Organization: Deloitte Consulting LLP

5. **A Case Study for Blockchain in Healthcare: "MedRec" Prototype for Electronic Health Records and Medical Research Data [PDF - 591 KB].** A decentralized record management system to handle electronic health records, using Blockchain technology that manages authentication, confidentiality, accountability and data sharing.
   Authors: Ekblaw A, Azaria A, Halamka J, Lippman A.
   Organizations: MIT Media Lab, Beth Israel Deaconess Medical Center
6. **The Use of a Blockchain to Foster the Development of Patient-Reported Outcome Measures [PDF – 195 KB].** Use of the Internet of Things in combination with Blockchain technology for Patient Reported Outcome Measures (PROMs).
   Author: Goldwater JC.
   Organization: National Quality Forum
7. **Powering the Physician Patient Relationship with 'HIE of One' Blockchain Health IT [PDF-162 KB].** 'HIE of One' links patient protected health information (PHI) to Blockchain identities and Blockchain identities to verified credential provider institutions to lower transaction costs and improves security for all participants.
   Author: Gropper A.
   Organization: Unaffiliated
8. **Blockchain: The Chain of Trust and its Potential to Transform Healthcare – Our Point of View [PDF- 249 KB].** Potential uses of Blockchain technology in health care including a detailed look at health care pre-authorization payment infrastructure, counterfeit drug prevention and detection and clinical trial results use cases.
   Organization: IBM Global Business Service Public Sector
9. **Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records [PDF – 270 KB].** Use of Blockchain as a novel approach to secure health data storage, implementation obstacles, and a plan for transitioning incrementally from current technology to a Blockchain solution.
   Author: Ivan D.
   Organization: Unaffiliated
10. **ModelChain: Decentralized Privacy-Preserving Health Care Predictive Modeling Framework on Private Blockchain Networks [PDF – 272 KB].** ModelChain is a framework used to adapt Blockchain to enable privacy-preserving health care predictive modeling and to increase interoperability between institutions.
    Authors: Kuo T, Hsu C, Ohno-Machado L.
    Organizations: Health System Department of Biomedical Informatics, University of California San Diego, La Jolla, CA Division of Health Services Research & Development, VA San Diego Healthcare System.
11. **Blockchain for Health Data and Its Potential Use in Health IT and Health Care Related Research [PDF – 1.5 MB].** A look at Blockchain based access-control manager to health records that advances the industry interoperability challenges expressed in ONC's *Shared Nationwide Interoperability Roadmap*.
    Authors: Linn L, Koo M.
    Organization: Unaffiliated
12. **A Blockchain-Based Approach to Health Information Exchange Networks [PDF-402 KB].** A Blockchain-based approach to sharing patient data that trades a single

centralized source of trust in favor of network consensus, and predicates consensus on proof of structural and semantic interoperability.
Authors: Peterson K, Deedvanu R, Kanjamala P, Boles K.
Organization: Mayo Clinic

13. **Adoption of Blockchain to enable the Scalability and Adoption of Accountable Care [PDF-500 KB].** A new digital health care delivery model that uses Blockchain as a foundation to enable peer-to-peer authorization and authentication.
Author: Prakash R**.**
Organization: Unaffiliated
14. **A Blockchain Profile for Medicaid Applicants and Recipients [PDF – 190 KB].** A solution to the problem churning in the Medicaid program that illustrates how health IT and health research could leverage Blockchain-based innovations and emerging artificial intelligence systems to develop new models of health care delivery.
Authors: Vian K, Voto A, Haynes-Sanstead K.
Organization: Blockchain Futures Lab - Institute for the Future
15. **Blockchain & Alternate Payment Models [PDF - 601KB].** Blockchain technology has the potential to assist organizations using alternative payment models in developing IT platforms that would help link quality and value.
Author: Yip K.
Organization: Unaffiliated

Source: http://wayback.archive-it.org/3926/20170128063822/https://www.hhs.gov/about/news/2016/08/29/onc-announces-blockchain-challenge-winners.html

Blockchain Technology: Possibilities for the U.S. Postal Service

At its core, blockchain technology is a way to transfer any kind of data or information in a fast, tracked, and secure way without the need for an intermediary institution. Initially developed to allow peers to directly exchange digital currency faster and at lower cost, blockchain is now yielding a variety of promising new solutions beyond financial services. It is difficult to understand the full potential of these new applications at this formative stage, but they include property transfers, the execution of contracts, authentication services, device management, and records management.

- Blockchain technology is a new way to transfer any kind of data or information in a fast, tracked, and secure manner without need for an intermediary.
- Major companies, such as Citibank and Australia Post, are beginning to research and experiment with this technology in order to provide new and more efficient services.
- The Postal Service could benefit from use of this technology – particularly regarding financial services, identity services, supply chain management, and device management – and should consider exploring and experimenting with it.

Despite their novelty, these applications are beginning to gain traction with major companies and government entities, from Citibank and JPMorgan Chase to the Estonian government and Australia Post. These organizations are researching or experimenting with blockchain technology in order to keep better records and provide new and more efficient services.

The U.S. Postal Service Office of Inspector General contracted with Swiss Economics in order to better understand blockchain technology's features and capabilities, as well as identify potential areas of interest for the Postal Service.

One major area is financial services. The Postal Service could use blockchain technology to improve the back-end of its financial products, such as international money transfers and money orders. A blockchain-based financial platform could digitize and streamline the services, making them faster and cheaper for both the Postal Service and its customers. In the long-term, blockchain technology could also be useful to the Postal Service in other areas such as identity services, supply chain management, and device management.

While blockchain was originally developed as part of digital currency, people are realizing that at its core, it is a way to transfer any kind of information in a fast and private way and that it can be useful for any kind of information or value transfer that typically involves an intermediary. This realization has spurred intense development activity in the market. In fact, people in the field are comparing it to the early stages in the development of the Internet, and there are similar levels of capital investment in startups related to blockchain services and applications as there was in the development of the Internet in the mid-1990s. Just as the Internet relies on services such as browsers and email clients to help consumers access its capabilities, blockchain

Thank You for previewing this eBook

You can read the full version of this eBook in different formats:

- HTML (Free /Available to everyone)
- PDF / TXT (Available to V.I.P. members. Free Standard members can access up to 5 PDF/TXT eBooks per month each month)
- Epub & Mobipocket (Exclusive to V.I.P. members)

To download this full book, simply select the format you desire below