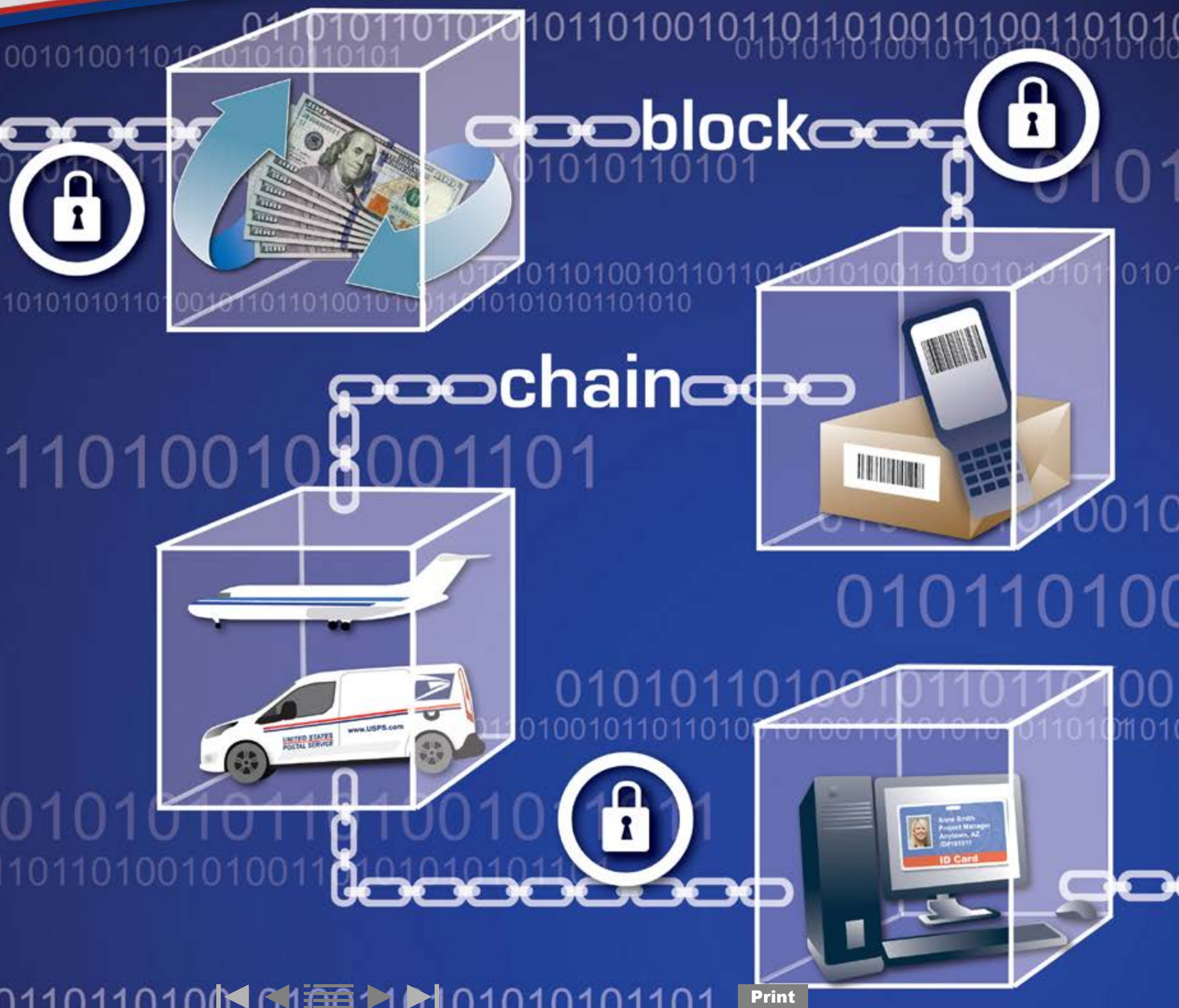
OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

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

RARC Report

Report Number
RARC-WP-16-011

May 23, 2016



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Executive Summary

Blockchain technology allows peers to exchange money directly without the need for a traditional financial intermediary, lowering the cost and increasing the speed of transactions. However, it is proving to be much more than a way to transfer monetary value. At its core, blockchain technology is a way to transfer any kind of information in a fast, tracked, and secure way.

The technology is only in the early stages of development and it is hard to recognize its full potential at this formative stage. However, developers are beginning to explore blockchain solutions outside of financial services. These new applications include property transfers, the execution of contracts, authentication services, network and device management, and records management.

Despite their novelty, blockchain applications are gaining mainstream traction. Major banks, such as Citibank and JPMorgan Chase, and government entities, such as the U.K. and Estonian governments and Australia Post, are experimenting with how blockchain technology can help them keep better records and provide services that are more efficient. The Postal Service could likewise stand to benefit from monitoring and experimenting with this technology.

The U.S. Postal Service Office of Inspector General (OIG) contracted with Swiss Economics, a consulting firm with interest and expertise in blockchain technology, to better understand the technology and its features, as well as identify areas of potential interest for the Postal Service.

Highlights

Blockchain technology has the potential to disrupt services that traditionally require intermediaries.

Originally created to transfer financial value, specifically within the context of the peer-to-peer currency known as Bitcoin, blockchain is now viewed as having the potential to be an efficient and secure way to transfer any kind of information.

Mainstream banks, governments, and other companies are starting to experiment with how they can use blockchain technology in financial applications and in new application areas such as property transfers, authentication services, and records management.

Because blockchain technology may disrupt areas in which the Postal Service currently does business, it may be wise to begin studying its impact and experimenting with its future possibilities.

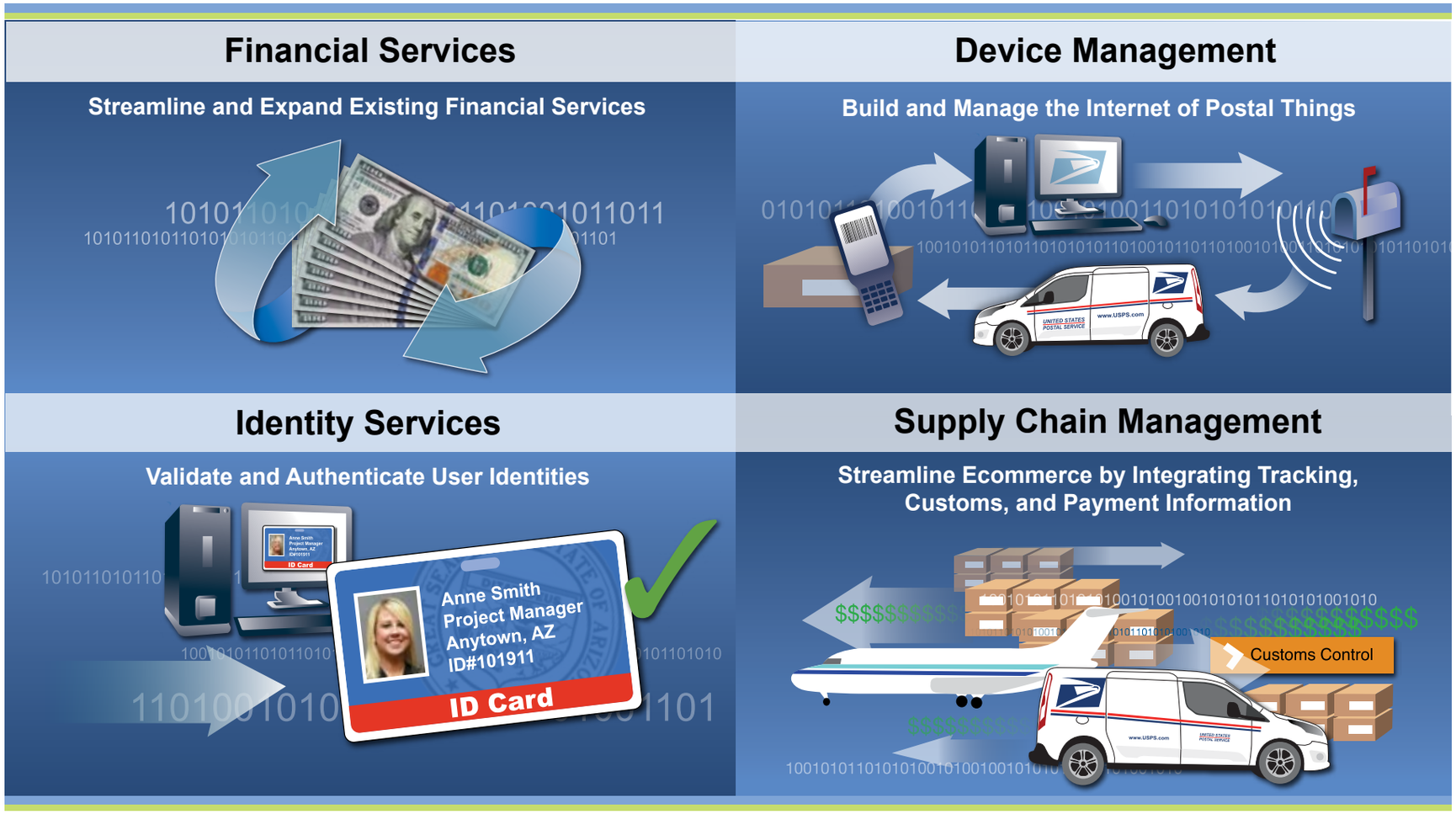
This paper proposes that blockchain technology could impact the Postal Service's business in several ways. For example, blockchain is already disrupting the global financial services industry — an industry the Postal Service is involved in through services such as money orders and international money

transfers. Additionally blockchain is an enabling technology that could allow the Postal Service to improve its operations and expand its services through emerging applications such as identity management and supply chain management. This paper takes an exploratory look at the technology and suggests that it may be wise for the Postal Service to engage in further examination of, and even experimentation with, this technology in order to gain a better understanding of its potential impacts.

The Postal Service could improve its existing services by beginning to experiment with the financial applications of blockchain. Specifically, the creation of a financial platform using blockchain could leverage the technology to offer improved financial services such as money transfers. The platform could allow the Postal Service to streamline the back-end of this current service, making the service faster and cheaper for both the Postal Service and its customers. It could also be especially useful for international money transfers due to the technology's borderless nature.

In the long-term, the Postal Service's experimentation with blockchain technology in financial applications could naturally expand into other applications enabled by the technology. In this paper, the OIG outlines three other areas of potential interest to the Postal Service: identity services, device management, and supply chain management.

Summary of Potential Postal Blockchain Applications



Source: OIG.

Table of Contents

Observations

Introduction

In 2008, the mysterious "Satoshi Nakamoto" introduced a new form of digital currency, called Bitcoin, to the world.[1] Bitcoin aims to revolutionize the world of payments by creating the world's first "peer-to-peer electronic cash system" that allows individuals to exchange value without the need for an intermediary institution.[2] Attracted by the potential benefits of fast, inexpensive, and private transactions, users around the world now exchange millions of dollars' worth of Bitcoin every day.[3] Despite this, Bitcoin has struggled to gain a foothold in the global marketplace. Seven years after its introduction, only about half of Americans had heard of Bitcoin, let alone felt comfortable using it.[4] The future of Bitcoin is still unknown.

The technology underlying Bitcoin, however — known as blockchain — might be here to stay. Similar to how now-defunct Napster changed how we share and listen to music over peer-to-peer digital platforms, blockchains have the potential to change how we transfer money and information even if Bitcoin itself does not last.

Blockchain has lately spurred a great amount of interest and ideation among mainstream players. This past year we have witnessed the development of an entire ecosystem of new companies offering hundreds of different blockchain applications.[5] However, the technology is still in the early stages of development; it is hard to recognize and appreciate its full potential at this formative stage.

The U.S. Postal Service Office of Inspector General (OIG) contracted with Swiss Economics, a consulting firm with interest and expertise in blockchain technology, to better understand the technology, its features, and possible postal applications.

Blockchain Technology: Definition and Development

Blockchain as a Mechanism to Transfer Value

Blockchain technology was originally created as a way to transfer value, specifically within the context of the digital currency Bitcoin — money in the form of data streams.[6] As such, primary uses of blockchain technology include payments and other financial transactions. Blockchain enables peer-to-peer transactions by removing the need for a trusted intermediary verifying the transactions — a role that is needed when peers do not know or trust each other.[7] Blockchain makes this possible by being a decentralized public ledger. This public ledger is not so different from the ledger that traditional financial institutions maintain, with a record of who owns what. The difference is that there is no bank or other single third party keeping the ledger and verifying the transaction — no one entity controls the ledger. Instead, the network, as a whole, verifies the transactions through a decentralized "consensus mechanism."[8]

---

1 The identity of Satoshi Nakamoto has always been shrouded in mystery. Recently, Australian computer scientist and businessman Craig Wright has claimed to be the creator of Bitcoin. However, there are still those who do not believe that Mr. Wright is in fact Bitcoin's creator. See Greenberg, Andy and Gwern Branwen, "Bitcoin's Creator Satoshi Nakamoto is Probably This Unknown Australian Genius," *Wired*, December 8, 2015, https://www.wired.com/2015/12/bitcoins-creator-satoshi-nakamoto-is-probably-this-unknown-australian-genius/; "Craig Steven Wright Claims to Be Satoshi Nakamoto. Is He?," *The Economist*, May 2, 2016, http://www.economist.com/news/briefings/21698061-craig-steven-wright-claims-be-satoshi-nakamoto-bitcoin; Butcher, Mike, "Major Questions Arise of Craig Wright's Claim to Be Satoshi Nakamoto," TechCrunch, May 2, 2016, http://techcrunch.com/2016/05/02/major-questions-arise-over-craig-wrights-claim-to-be-satoshi-nakamoto/.

2 Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf.

3 Blockchain.info, "Estimated USD Transaction Volume," https://blockchain.info/charts/estimated-transaction-volume-usd.

4 eMarketer, "Usage and Awareness of Bitcoin Among Internet Users in Select Countries," February 2015.

5 "Bitcoin Trends in the First Half of 2015," *Coinbase*, July 15, 2015, https://blog.coinbase.com/2015/07/15/bitcoin-trends-in-1h-2015/.

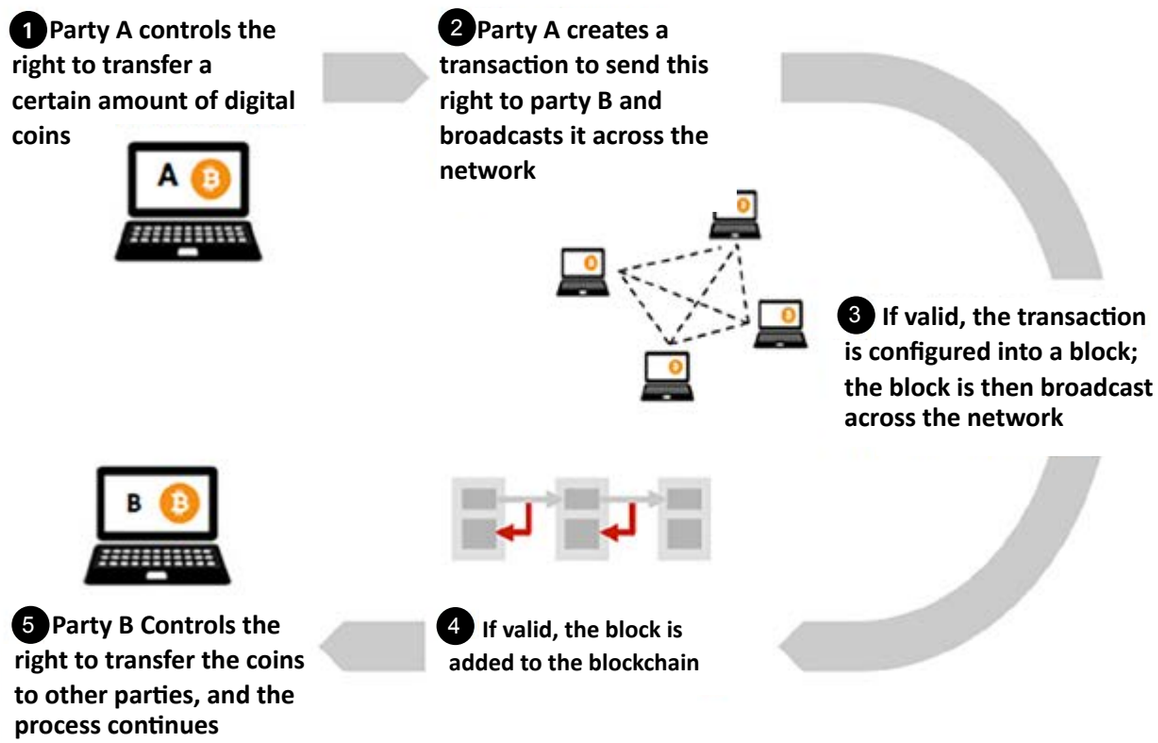
6 Although some people are referring specifically to the Bitcoin blockchain when they use the word "blockchain," for the purposes of this paper the word blockchain refers to blockchain technology in general. This paper will use "Bitcoin" or "Bitcoin blockchain" when referring to Bitcoin specifically.

7 Blockchains are "a way for people who do not know or trust each other to create a record of who owns what that will compel the assent of everyone concerned. It is a way of making and preserving truths." "The Great Chain of Being Sure About Things," *The Economist*, October 31, 2015, http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.

8 A consensus mechanism is the set of rules governing the process of agreement within a system. In the case of Bitcoin, consensus needs to be reached regarding which

The technology is called “blockchain” because individual transactions are grouped into what is called a block.[9] Members of a public peer network seek to verify the block, and each of these verifiers in the network retains a copy of the ledger on their hard drive. Blocks then build upon each other, with the data in each block being irrevocably linked to the blocks before it — hence the “chain.” As such, each “coin” on the blockchain is a string of data that identifies every transaction that coin was ever involved in — a sort of historical record.[10] Imagine holding a $100 bill in your hand and not only seeing the cold hard cash, but also a chain of information identifying every trade that $100 bill was ever involved in. Because of this linkage of blocks and transactions, it is prohibitively impractical and computationally very difficult to modify a block once created and confirmed.[11] This helps to keep the system secure while eliminating the need for an intermediary. Figure 1 below illustrates a blockchain transaction.

Figure 1: A Blockchain Transaction



Source: Swiss Economics.

transactions are valid. For more information on how a blockchain works, including a detailed description of the Bitcoin blockchain as well as different types of consensus mechanisms, please see Appendix A. “How Bitcoin Mining Works,” *Coindesk*, December 22, 2014, http://www.coindesk.com/information/how-bitcoin-mining-work.

9 Blocks are created through the consensus mechanism. In the case of Bitcoin, miners are the members of the network that are creating blocks. This requires a substantial amount of computing power.

10 The coin is the unit of account that denotes value the way a dollar denotes value. It has a unique identity that is tracked along a blockchain. For more information on the components of a blockchain system, see Appendix A.

11 IBM Institute for Business Value, *Empowering the Edge*, 2015, http://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf, p. 6.

Although the blockchain that most people are familiar with is Bitcoin, there are many different blockchains. At the highest level, these blockchains fall into two groups: public and private.[12] In a **public blockchain**, the right to alter the ledger by participating in the consensus mechanism is *open to anyone*. Transactions are publicly available for anyone to read. Bitcoin and Ethereum are two prominent public blockchains.[13] In a consortium or **private blockchain**, the right to alter the ledger by participating in the consensus mechanism is *restricted to pre-selected individuals or institutions*.[14] Transactions may either be publicly available or restricted to a select number of participants. Ripple is a prominent example, and private blockchains are also of growing interest for business use.

The Development of Blockchain Technology

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.[15] Just as the Internet relies on services such as browsers and email clients to help consumers access its capabilities, blockchain technology's utility and continued development will rely on innovation by new service providers.

Since the blockchain mechanism was originally conceived as a financial exchange tool for Bitcoins, much of the innovation activity so far has been in financial applications. It is important to note, however, that a coin on a blockchain could easily represent more than Bitcoins or money. It could represent a house, a car, a stock, or even a vote or an identity. Arguably, a coin could represent any kind of information or any piece of data. It is this realization that is sparking growth in this sector, including the development of new applications and increased interest in this technology by major players.

New Applications and Services

Developers are beginning to create and market novel uses of blockchain, which has the potential to disrupt any sector that uses intermediaries to verify or track the transfer of information. Some of the major application areas include financial services, the transfer of property, the execution of contracts, authentication services, network and device management, and records management.[16] This has led the Institute of Electrical and Electronics Engineers to suggest that "the possibilities are endless and that money is only the first, and perhaps the most boring, application enabled by Bitcoin technology."[17] Table 1 describes common application areas pursued by many of the startups in the space.

---

12 Christian Jaag of Swiss Economics, in discussion with the author, December 14, 2015, and Buterin, Vitalik, "On Public and Private Blockchains," *Ethereum Blog*, August 7, 2015, https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

13 Ethereum is a blockchain-based platform designed specifically for use in smart contracts. Smart contracts are blockchain transactions that are automatically carried out under the right circumstances by building conditional language into the transaction. "What is Ethereum," https://www.ethereum.org/; and "The Great Chain of Being Sure About Things," *The Economist*.

14 This right to alter could also be limited to just one individual or party, to create a truly private blockchain. This type of blockchain, though, would essentially be very similar to a traditional database.

15 Brock Pierce, presentation "Bitcoin might fail but the blockchain is here to stay – Full WIRED Retail talk," YouTube video, posted by "*Wired UK*," December 9, 2014, https://www.youtube.com/watch?v=jbu6I-8mNUo.

16 GrowthPraxis, cited in Let's Talk Payments, "Blockchain Use Cases: Comprehensive Analysis & Startups Involved," July 29, 2015, http://letstalkpayments.com/blockchain-use-cases-comprehensive-analysis-startups-invoved/. Categorization by OIG.

17 Morgan E. Peck, "The Future of the Web Looks A Lot Like Bticoin," *IEEE Spectrum*, July 1, 2015, http://spectrum.ieee.org/computing/networks/the-future-of-the-web-looks-a-lot-like-bitcoin. In addition to the Institute of Electrical and Electronics Engineers expressing interest in the new applications of this technology, experts in the field of Bitcoin and blockchain, such as Mike Hearn and Chris Ellis, are interested as well. "Bicoin 2012 London: Mike Hearn," YouTube video, from the London Bitcoin Conference 2012, posted by "QueuePolitely," September 27, 2012, https://www.youtube.com/watch?v=mD4L7xDNCmA and Jay Cassano, "What are Smart Contracts? Cryptocurrency's Killer App," *Fast Company*, September 17, 2014. Likewise, IBM is investing in the future of non-financial applications of blockchain. Robert McMillan, "IBM Adapts Bitcoin Technology for Smart Contracts," *Wall Street Journal*, September 16, 2015, http://www.wsj.com/articles/ibm-adapts-bitcoin-technology-for-smart-contracts-1442423444.

Table 1: Startup Activity in the Blockchain Space

Type of Service	Intermediaries Replaced	Sample Companies in the Market
Financial Services: services involving the exchange of money that can now be performed on a blockchain. Such services include money transfers, remittances, and payments	Banks, credit card companies, money transmitters, clearinghouses, and other intermediaries in the financial industry	Bitpay, Coinbase, Kraken, BitPesa, coins.ph, LocalBitcoins, bitso, bitt, Bitcoin Venezuela, expresscoin, Counterpart
Smart Contracts: verification and enforcement of agreements negotiated between two or more parties, such as escrow services or wills, is written into the blockchain	Lawyers, sharing economy platforms (such as AirBnb or Uber)	SmartContract, Codius, New System Technologies, Bitnplay; UbiMS, BitHalo, Lighthouse
Smart Property*: tracking ownership of physical and non-physical property, such as cars, real estate, stocks, and other assets through a blockchain	Lawyers, stock markets, real estate and other sales agents	Symbiont, Mirror Labs, Secure Assets, BitShares, equityBits, DXMarkets, MUNA, Everledger
Authentication Services: use of information in addition to a user's public wallet address, such as a home address or social media profile, to verify and authenticate a user's identity and activity on a blockchain. Services include identification verification and proof of ownership	Government agencies, such as motor vehicle departments or the Social Security Administration, and other identity brokers	Onename, Bitnation, BlockCDN, Colu, MyPowers, TRST.im, Blockai, Bitproof, ascribe, Artplus, Stampery, Chainy Link, Proof of Existence
Records Management: the maintenance of official records and registers in a transparent, secure, and auditable manner by using a blockchain. Includes the management of health records, government records, and voting	Hospitals that manage patient records, governments	BitHealth, Agora, BitCongress, Follow My Vote, BTC Blockchain Apparatus
Network and Device Management: allowing connected objects to communicate with each other directly over a blockchain. This enables decentralized Internet of Things management and network storage	Centralized cloud computing, human intervention required to manage devices	Chimera IOT, Storj; ePlug, Filament, Tilepay

* Smart property transactions may utilize smart contracts, and some participants in the field see smart property as a subset of smart contracts, https://en.bitcoin.it/wiki/Smart_Property.

Source: OIG Analysis and Growth Praxis.

Big Players are Beginning to Adopt Blockchain

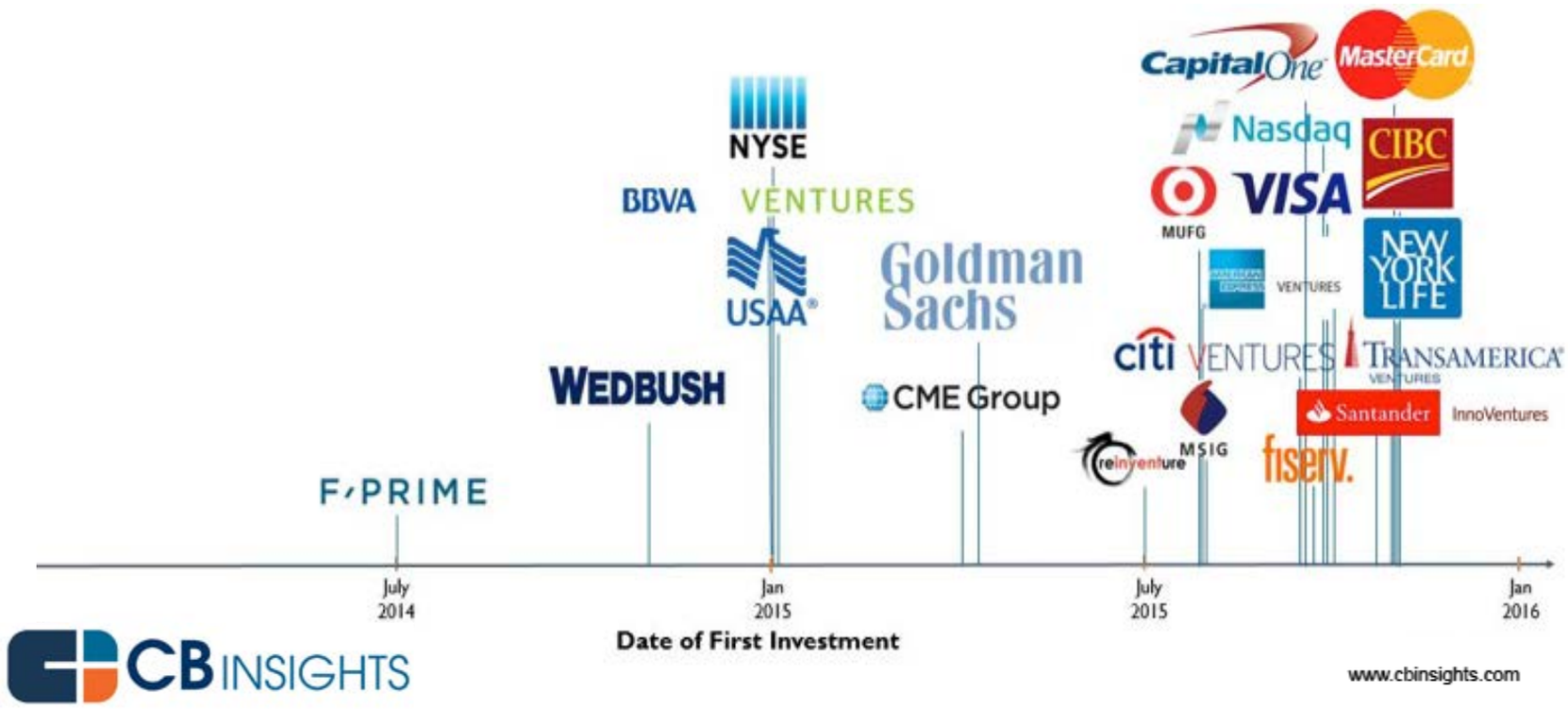
In addition to an increasing array of diverse applications being developed by start-ups, there is an increased use of blockchains by major mainstream players. In January 2014, *Overstock.com* became an early beneficiary of blockchain technology by becoming one of the first major companies to enable payment in Bitcoin on its website.[18] It has since received approval to issue stock through the Bitcoin blockchain.[19] Since then many major players have announced plans to use blockchain, invest in blockchain startups, or at the very least research how the technology could affect their business.

18 After Overstock announced it would accept Bitcoin, many other major companies followed suit including Microsoft, Dell, and Expedia. Bheemaiah, Kariappa, "Block Chain 2.0: The Renaissance of Money," *Wired*, http://www.wired.com/insights/2015/01/block-chain-2-0/.

19 Patrick M. Byrne, "Overstock CEO: Why We're Accepting Bitcoins," *CNBC*, January 7, 2014, http://www.cnbc.com/2014/01/07/overstock-ceo-why-were-accepting-bitcoinscommentary.html and Yessi Bello Perez, "SEC Approves Overstock's Plan to Issue Blockchain Securities," *Coindesk*, December 16, 2015, http://www.coindesk.com/sec-approves-overstocks-proposal-to-issue-securities-on-the-blockchain/.

As one would expect, a number of the interested companies are in the banking and financial services sector (see figure below). UBS has opened a research lab to explore the application of blockchain to their financial business.[20] Citibank is testing different uses of blockchain in their lab and has gone so far as to experiment with their own coin: CitiCoin.[21] JPMorgan Chase, America's largest bank, has just begun to investigate how blockchain could be used, for example, to deal with data errors in the bank's loan funds.[22] Additionally, the stock exchange Nasdaq revealed that it will soon record trades in privately held companies on a blockchain-based system.[23]

Figure 2: Timeline of Major Financial Institutions' Activity in the Blockchain Space



Source: CB Insights.

Outside the financial services sector, some additional blockchain applications are beginning to gain traction — particularly with governments. In the records management space, the U.K. Government is starting to research a role for blockchain in keeping registers, and government representatives in Honduras are working with a startup called Factom on a prototype of a blockchain-based land registry.[24] The Liberal Alliance in Denmark was the first major political party to vote using the technology, in an internal election, and similar systems were later used in Norway and Spain.[25] Citizens of Estonia will soon be able to manage their health records and who has access to them via a blockchain-based database.[26] In the area of identity management, the Estonian Government has announced that residents

20 Rachel King, "UBS Working with Blockchain Prototypes," *Wall Street Journal Blog*, October 2, 2015, http://blogs.wsj.com/cio/2015/10/02/ubs-working-with-blockchain-prototypes/.

21 John Biggs, "Citibank is Working on Its Own Digital Currency: Citicoin," *TechCrunch*, July 7, 2015, http://techcrunch.com/2015/07/07/citibank-is-working-on-its-own-digital-currency-citicoin/ and Ian Allison, "Codename Citicoin: Banking Giant Built Three Internal Blockchains to Test Bitcoin Technology," *International Business Times*, July 1, 2015, http://www.ibtimes.co.uk/codename-citicoin-banking-giant-built-three-internal-blockchains-test-bitcoin-technology-1508759.

22 Das, Samburaj, "JPMorgan Begins Blockchain Trials," *Cryptocoins News*, January 2, 2016, https://www.cryptocoinsnews.com/jpmorgan-begins-blockchain-trials/.

23 "The Great Chain of Being Sure About Things," *The Economist.*

24 Emily Spaven, "UK Government Exploring Use of Blockchain Recordkeeping," *CoinDesk*, September 1, 2015, http://www.coindesk.com/uk-government-exploring-use-of-blockchain-recordkeeping/; Greece has also expressed interest in such a land registration system. "The Great Chain of Being Sure About Things," *The Economist*.

25 Daniel, Matthew, "Blockchain Technology: The Key to Secure Online Voting," *Bitcoin Magazine*, June 27, 2015, https://bitcoinmagazine.com/articles/blockchain-technology-key-secure-online-voting-1435443899.

26 Ian Kar, "Estonian Citizens Will Soon Have the World's Most Hack-proof Health-care Records," *Quartz*, March 3, 2016, http://qz.com/628889/this-eastern-european-country-is-moving-its-health-records-to-the-blockchain/.

with an “e-Resident” digital identity will be able to use blockchain to notarize marriages, births, contracts, and more.[27] IBM is building a coin-less blockchain for smart contracts and hoping it will help move the technology into the mainstream.[28] Finally, Australia Post recently announced that it is exploring the role of blockchain technology as a tool for digital identity management.[29]

Case Study on Blockchain Investments: Goldman Sachs

Leading multinational investment banking firm Goldman Sachs is one of many financial firms taking notice and making serious investments in blockchain technology in attempts to decipher its possible uses and cost-saving potential.

According to a recent report from Goldman Sachs, blockchain’s potential extends far beyond Bitcoin. The report says, “from banking and payments to notaries to voting systems to vehicle registrations to wire fees to gun checks to academic records to trade settlement to cataloguing ownership of works of art, a distributed shared ledger has the potential to make interactions quicker, less-expensive and safer.”

The bank is one of many of the world’s top financial firms participating in R3CEV, an initiative to develop distributed ledger technologies for financial services and processes. This consortium of the largest global banks is looking to create standards and protocols for blockchain undertakings in order to reduce the cost of financial transactions. R3CEV has hired people to help from Google, IBM, Barclays, and others.

In addition to participating in this initiative, Goldman Sachs is making moves to further understand the full potential of the blockchain. It recently filed a patent for a cryptographic currency, known as SETLcoin, which allows for peer-to-peer exchange of securities. The application for the patent details the ways the tokens can be marked and exchanged. Goldman Sachs is also an investor in Circle, a blockchain payments startup that received $50 million in funding in 2015.

Source: The Goldman Sachs Group Global Investment Research, “Emerging Theme Radar: What if I Told You…,” December 2, 2015.

Strengths and Weaknesses of Blockchain Technology

Blockchain transactions are quite different from typical transactions. They have unique attributes that offer users a number of potential benefits. These benefits are what have sparked the interest in this technology and innovation in this area. On the other hand, as with any new technology, there are still many challenges associated with blockchain that are important to consider. The OIG collaborated closely with Swiss Economics to outline the benefits and shortcomings of blockchain technology. These strengths and weaknesses emerged within the context of financial applications of blockchain, but they also apply to other application areas.

Strengths

Lower Cost of Transactions

Due to the decentralized nature of blockchains, users have the ability to make online transactions for a fraction of the fees charged by current intermediaries such as financial or legal institutions. Credit card companies charge a fee per transaction for processing,

27 The Estonian e-Residency program provides individuals with a government-issued digital identity that allows users to sign legal contracts, run an Estonian company, and file taxes online. For more information on this program, see https://e-estonia.com/e-residents/about/. See also Ian Allison, “Bitnation and Estonian Government Start Spreading Sovereign Jurisdiction on the Blockchain,” *International Business Times*, November 28, 2015, http://www.ibtimes.co.uk/bitnation-estonian-government-start-spreading-sovereign-jurisdiction-blockchain-1530923.

28 Robert McMillan, “IBM Adapts Bitcoin Technology for Smart Contracts” and IBM, *IBM Blockchain is open for business*, http://www.ibm.com/blockchain/index.html.

29 Keen, Lucille, “Australia Post to Use Blockchain to Store Identities,” *Australian Financial Review*, March 16, 2016, http://www.afr.com/technology/australia-post-to-use-blockchain-to-store-identities-20160316-gnk6w5.

which is a cost that is usually borne by merchants but which can also be passed along to buyers through higher prices or an additional fee for purchasing with a credit card.[30] Remittance service providers charge senders an average of 8 percent to transfer money to family overseas.[31] In the financial services sector alone, Spanish bank Santander estimates that blockchain technology could save banks around the world $15-20 billion annually in settlement, regulatory, and cross-border payment costs.[32] Outside of the financial services sector, IBM has suggested that blockchain can help reduce infrastructure and maintenance costs of scaling the Internet of Things by allowing connected devices to "share computing resources without dependency on a central cloud or server, thereby optimizing resource utilization and cost."[33] Other cost savings of the technology are only just beginning to be investigated.

Faster Transactions

Blockchain transactions are processed much more quickly than most traditional data transfer systems, usually in a matter of minutes. With blockchain, time is saved by the elimination of intermediary institutions such as clearinghouses that make sure banks or others parties have matching records.[34] This feature is especially significant when it comes to payments, which can take hours, days, or even weeks to process. For example, when trading stocks or bonds, it usually takes 3 days for a transaction to settle and for the participants to have their funds available.[35] This is true even for electronic transactions where the information exchange may be immediate, but it may take 3 days to receive payment.[36] Real estate sales are also costly and time-intensive, often taking weeks to schedule a time for closing with thousands of dollars in closing costs. With smart property, selling a house could be as simple as transferring a coin. Other applications, such as not having to present yourself in-person to vote or notarize a document could save time and increase the convenience of these processes. Blockchain allows for faster, more efficient, and more customizable transactions.

Geographical Freedom of Transactions

Transactions across a blockchain are not bound to geographical limits. Given the virtual nature of the system, it does not matter whether an individual sends data to a neighbor or to someone on the other side of the world. In addition, as blockchains do not use intermediaries, which are bound by country-specific regulations, transactions can cross national borders with less friction. This makes blockchain well suited for international transactions.

Irreversibility of Transactions

Blockchain-based payments are irreversible; once a payment is issued, it can only be reversed by asking the receiver to pay the same amount back in another transaction. This feature is ideal for lowering transaction risk for a payment recipient, allowing merchants to be sure that buyers cannot cancel a payment after the sale of a good or service (the way they can with credit card purchases). This alleviates fraud risks and payment security costs for merchants.[37] On the other hand, buyers may not view this as an advantage. This is because conventional card- and bank-based payment providers, acting on behalf of the buyer,

---

30 For example, PayPal charges a 3 percent fee for their flat rate pricing, but fees can be higher depending on the type of transaction, https://www.paypal.com/webapps/mpp/brc/demystifying-credit-card-processor-fees.
31 The World Bank, *Remittance Prices Worldwide*, March 2014, https://remittanceprices.worldbank.org/sites/default/files/RPW_Report_Mar2014.pdf.
32 Santander Innoventures report, *The Fintech 2.0 Paper: Rebooting Financial Services*, June 2015, http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf, p.15.
33 IBM Institute for Business Value, *Empowering the Edge*, p. 4.
34 Steven Melendez, "The Future of Bitcoin Isn't Bitcoin: It's Bigger Than That," *Fast Company*, October 13, 2015, http://www.fastcompany.com/3051679/innovation-agents/the-future-of-bitcoin-isnt-bitcoin-its-bigger-than-that.
35 Ibid.
36 U.S. Securities and Exchange Commission, "About Settling Trades in Three Days: T+3," https://www.sec.gov/investor/pubs/tplus3.htm.
37 Payment irreversibility may especially strengthen ecommerce due to reduced overall transaction risk. Christian Jaag and Christian Bach, "The Effect of Payment Reversibility on E-commerce and Postal Quality," in *Handbook of Digital Currency*, (2015), pp. 139-152.

can reverse transactions in order to protect buyers against fraud, such as being overcharged or if a good is defective.[38] However, the irreversibility feature is not only beneficial to merchants. It applies to other application areas as well; including the transfer of property where there would be no way, for example, for someone selling a house on a blockchain to reverse the transaction and get the deed back after receiving payment. This feature would also mean that records could not be tampered with, altered, or undone after they have been created, making blockchain a highly transparent and auditable records management tool.

Increased Privacy of Transactions

Currently, completing an ecommerce transaction or enacting a legally binding contract requires participants to disclose their personal information to another party, such as an ecommerce platform. Transferring information across a blockchain is similar to paying with cash: there is no need to disclose any personal information such as a person's name, address, credit history, or credit card number. Individuals only disclose their wallet information, which is an alphanumeric "address." In addition to protecting user privacy, blockchain transactions greatly reduce the risks of identity theft and fraud that are common with other forms of transaction or payment, such as credit cards.[39]

Weaknesses

Technological Barriers

Blockchain is new and very different from most of the traditional technologies that people use. As such, in its current form, it requires above-average computer literacy to use properly, which acts as a barrier to entry for businesses and individuals that are interested in applications but do not know where to begin. This can limit access to the new technology for non tech-savvy users, and can expose them to fraud risks. Further, blockchain's decentralization means that there is no central customer care resource if users need assistance.[40]

Security Concerns

Although the Bitcoin blockchain has so far not been compromised, service providers (such as wallet providers or exchange services), are vulnerable to attacks.[41] Furthermore, the privacy of transactions seen as a benefit to many is also a security concern. Not knowing the identity of the individual on the other side of the transaction makes it difficult to resolve issues that may arise and can place users at risk for fraud.

Limited Access

At present, access to blockchain applications is provided by online exchanges. Physical touchpoints, such as Bitcoin ATMs and other physical service locations, are scarce and scattered. Service platforms are mostly new start-up firms with little reputation and lack physical exchange points.

---

38 There are possible solutions, however, that may help put buyers at ease. The transaction could use escrow, where payment is released to the merchant only after two out of three parties sign the transaction. Furthermore, private blockchains could potentially solve this problem by allowing for the reversibility of transactions by authorized users or other service providers could play a traditional intermediary's role of settling disputes. For example, *Open Bazaar* is a peer-to-peer selling platform where a moderator can be called in to settle a dispute. "Disputes," *Open Bazaar*, https://blog.openbazaar.org/openbazaar-user-tutorial/.

39 This feature has sparked a lot of discussion about the anonymity of cryptocurrency transactions that would foster the use of this payment system for illicit purposes. This is a valid concern, although cryptocurrency payments are not totally anonymous and with some investigative effort, illegal uses can be identified and prosecuted. Jerry Brito and Andrea Castillo, "Bitcoin: A Primer for Policymakers," *Mercatus Center*, December 19, 2013, http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_v1.3.pdf, p. 8. Such privacy is also offered by other encryption services or cash.

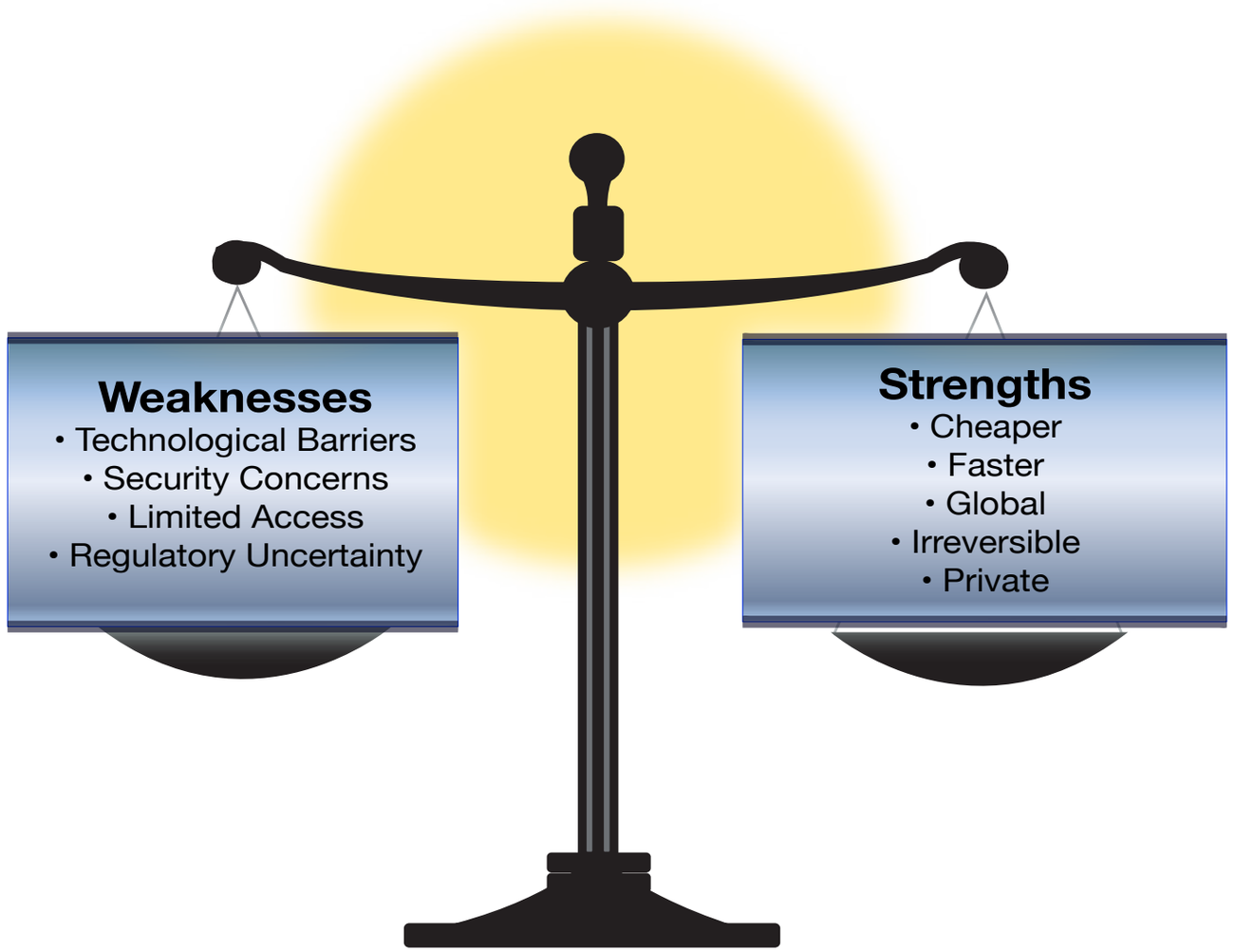
40 However, there are support forums, e.g. for Bitcoin http://www.bitcointalk.org or http://www.reddit.com/r/Bitcoin/ and other intermediaries, such as bitpay.com that seek to offer service to customers.

41 The most prominent example of such a theft is the exchange platform Mt. Gox which lost the equivalent of approximately USD 480 million in Bitcoin. The company has declared bankruptcy following this incident and it is likely that users will not be able to reclaim their assets. Carter Dougherty, and Grace Huang, "Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss," *Bloomberg*, February 28, 2014, http://www.bloomberg.com/news/2014-02-28/mt-gox-exchange-files-for-bankruptcy.html.

Regulatory Uncertainty

A lot of progress has been made in recent years, but there is still no international — or even interstate — agreement about how to regulate blockchain applications. Current regulations focus on financial applications of blockchain technology. It remains to be seen how applications such as smart contracts, smart property, and records management will be regulated. Up to this point, some government entities have emphasized instituting consumer protections while letting innovation continue to develop, but others have imposed more restrictive regulations. For example, the state of New York requires a "BitLicense" for businesses operating in this space, causing many startups to leave the state.[42] This regulatory uncertainty, coupled with speculation, has led to other problems, such as exchange rate volatility in the cryptocurrency applications such as Bitcoin.[43]

Figure 3: Strengths and Weaknesses of Blockchain Technology



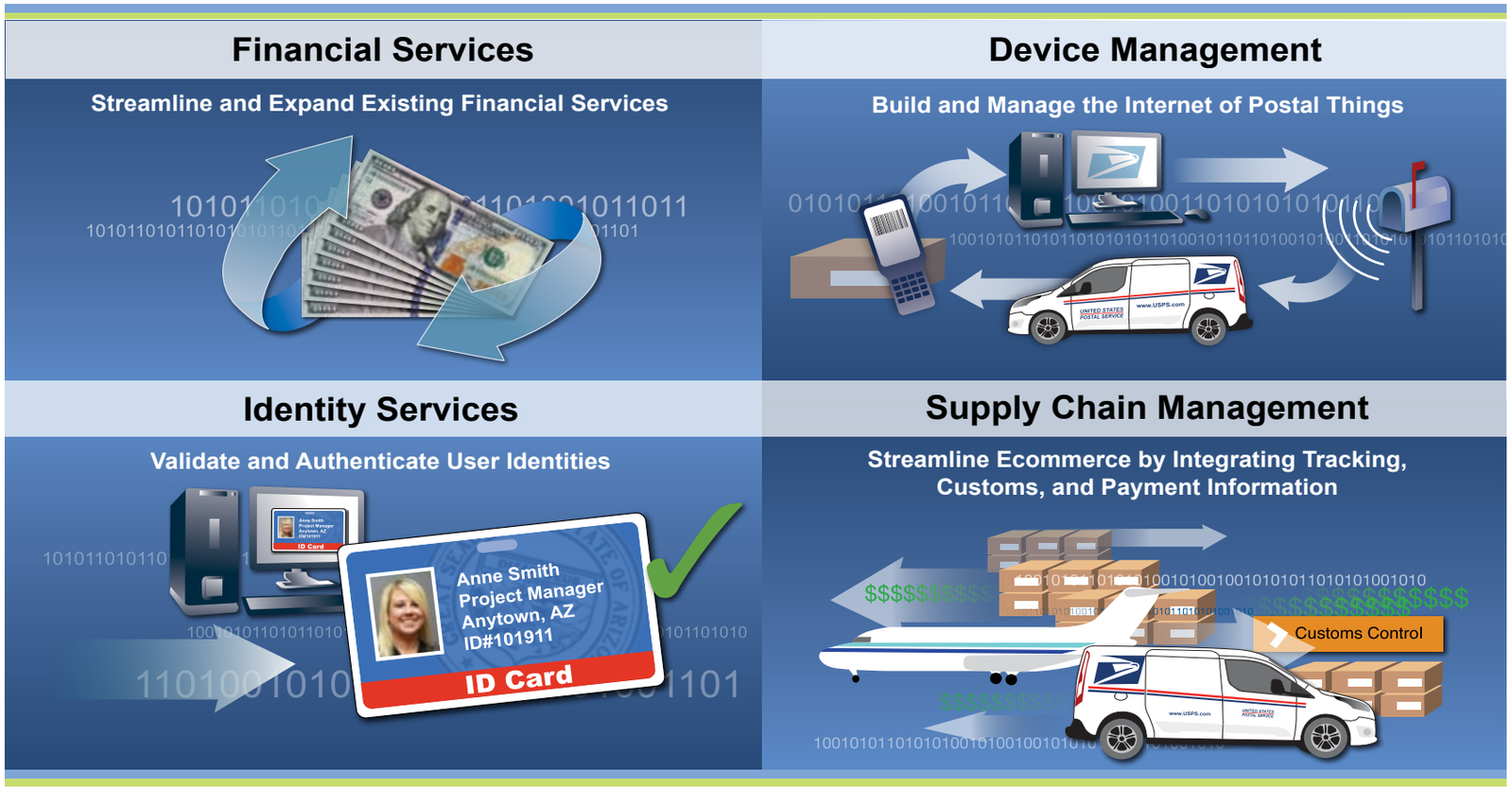
Source: OIG and Swiss Economics.

42 Perez, Yessi Bello, "The Real Cost of Applying for a New York BitLicense," *Coindesk*, August 13, 2015, http://www.coindesk.com/real-cost-applying-new-york-bitlicense/.
43 Christian Jaag and Christian Bach, "Cryptocurrencies: New Opportunities for Postal Financial Services" (Swiss Economics, Working Paper 0052, June 2015), https://www.swiss-economics.ch/RePEc/files/0052JaagBach.pdf.

Potential Postal Blockchain Applications

Many of the novel applications that the blockchain community is currently exploring are in service areas where the Postal Service is already active, which might make blockchain a worthwhile technology for the Postal Service to consider. The following applications could be of particular interest to the Postal Service.

Figure 4: Summary of Potential Postal Blockchain Applications



Source: OIG.

Financial Services

The Postal Service currently offers some basic financial services, including international electronic money transfers. To provide these services through a digital format that could be cheaper and more efficient for both the customers and the Postal Service, Swiss Economics suggests leveraging blockchain technology through the creation of a financial platform, that they term a Postcoin platform. Although financial applications on the blockchain do not need intermediaries to function, having a trusted entity like the Postal Service acting to facilitate its fair, affordable, and transparent use may help address many of the challenges that currently prevent individuals and businesses from taking advantage of this technology.[44] For example, the Postal Service could provide multichannel access and assistance online at USPS.com, through the USPS mobile app, and in-person through carriers or at post offices.[45] Postcoin could not only benefit users but the international postal network, for example, by allowing for faster, direct

44 These benefits and much of the explanation of the concept of Postcoin was adapted from joint research conducted with Swiss Economics and previously presented by Swiss Economics (Jaag and Bach).

45 The trusted Postal Service could also ensure a level of stability and security that is currently lacking, and its role as an intermediary would mean customers could go to the post office for assistance when trouble arises. Additionally, the Postal Service could back Postcoin with a full reserve so that anyone holding a Postcoin could exchange it back at the local post office for currency, possibly at a fixed exchange rate — a major difference between a Bitcoin and Postcoin. Christian Jaag and Christian Bach, "Cryptocurrencies: New Opportunities for Postal Financial Services."

transactions between posts. Furthermore, embracing new payment technologies and adapting to the changing wants and needs of customers could help the Postal Service remain relevant in a market where the use of electronic money increasingly dominates.

Creation of a Postcoin Platform — Two Options

The creation of the Postcoin platform could follow two different paths. One option is to "buy in" to an existing, public blockchain. A postal operator would first have to acquire some coins. Once the post owns the coins, it could add an additional layer of information to each coin, or fraction of a coin, to mark it as representing a specific and distinct asset — in this case, a Postcoin. After exchanging money into Postcoin, users can exchange them freely and directly over the existing public blockchain. The advantage of buying into an existing and already widely used platform is that the post does not have to foot the bill for the costs to maintain the validation system or to secure the payment network.

The other option would be to create a brand new blockchain altogether. The Postal Service could use the Bitcoin protocol, another open source software, or create their own.[46] Through the creation of such an enterprise blockchain platform, the Postal Service could maintain control over the platform and its features. This would help avoid many of the shortcomings listed above, addressing security and access issues while still bringing the benefits of speed, low cost, and auditability of the blockchain.

A Global Postal Payment Platform

Although the Postal Service could develop its own platform, Postcoin would be strongest as a global postal money transfer and payment platform. Postal operators around the world have an unmatched physical presence that extends across more than 600,000 post offices worldwide, including areas where rates of financial exclusion are higher.[47] Since a global Postcoin system would need national postal operators to interoperate, the Universal Postal Union (UPU) could be the governance body for a global Postcoin platform, setting standards, determining regulations, providing support for settling accounts between posts, and setting the value of the Postcoin.[48] The UPU is well-positioned for this because it already manages a global money transfer and payment platform that is used by many countries and coordinates payments between operators for settlement of terminal dues.[49]

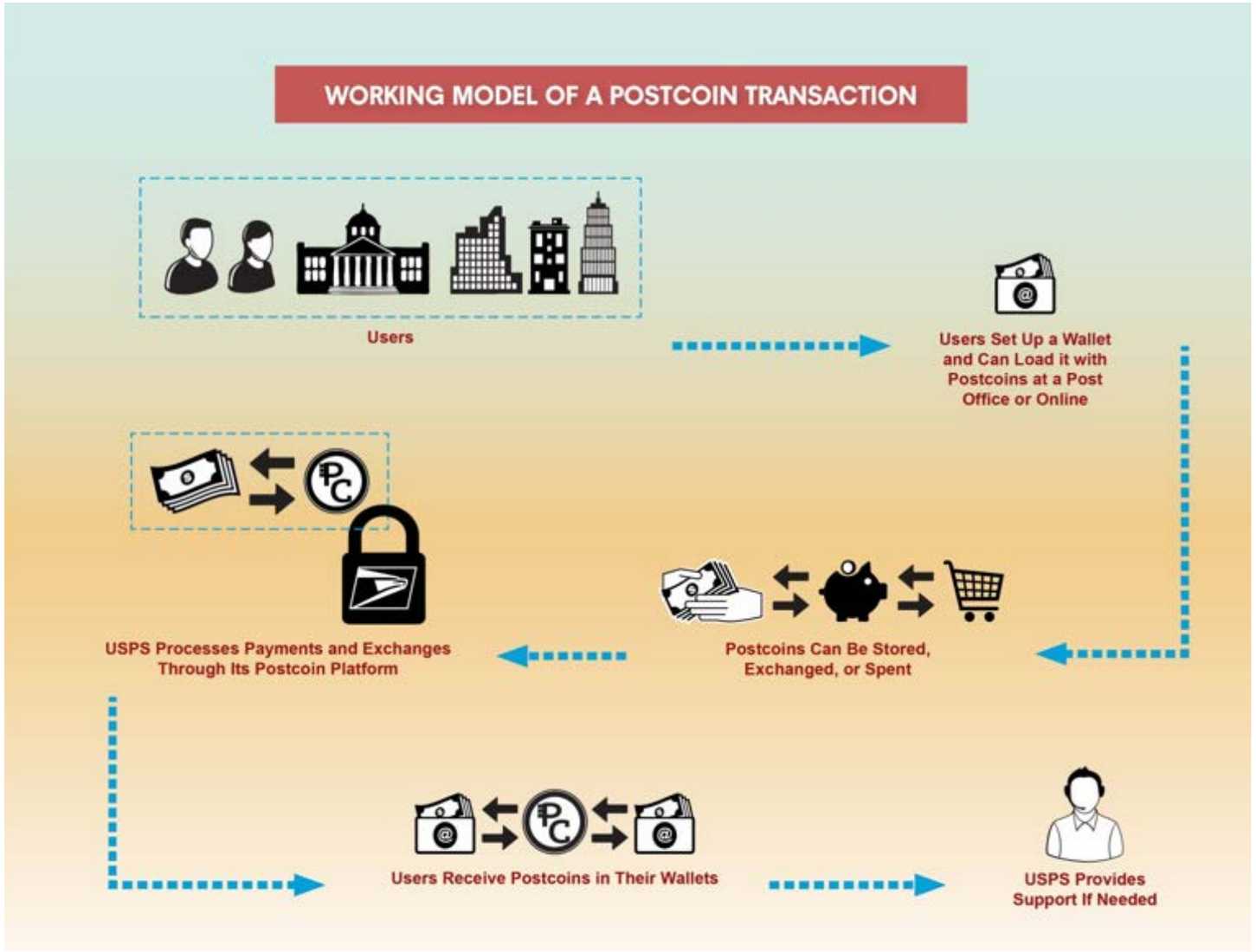
Benefits of Postcoin

The Postal Service currently has a steady money transfer business, but use of blockchain could help improve and expand that service. For example, the Postal Service currently offers international money transfers. However, these services are currently only cashable in a limited number of countries.[50] The flexibility and convenience associated with the Postcoin could potentially allow the expansion of electronic money transfer services to anyone in the world. Postcoin would not only allow these services to be conducted at a lower cost to both the Postal Service and its customers, but it might also help the Postal Service modernize and expand the reach of its financial services. Additionally, the Postcoin could be used for transactions directly between posts. This could potentially help streamline, for example, the settlement of terminal dues. The figure below illustrates how a Postcoin transaction could work.

---

46 For more information on this, see the discussion of "Other Coins Based on Bitcoin" in Appendix A.
47 Financial exclusion refers to whether citizens have access to the necessary banking and financial services they need, including savings accounts, credit, and loans.
48 José Anson, "Supporting Transactions not Pegged to National Currencies: A Role for the UPU," (presentation at OIG-UPU International Online Forum on Postal Innovation, January 2014).
49 Terminal dues refers to the system, negotiated as an intergovernmental agreement, by which posts compensate one another for the international delivery of letters, flats, or small packages up to 2 kilograms. OIG, *Terminal Dues in the Age of Ecommerce*, Report No. RARC-WP-16-003, December 14, 2015, https://www.uspsoig.gov/sites/default/files/document-library-files/2015/RARC-WP-16-003.pdf, p. 4.
50 Currently, the Postal Service's electronic money transfers are cashable only in 10 countries. In addition, these services have limits on how much money can be sent (USD 1,000 domestically, USD 700 internationally). See U.S. Postal Service's website for the Sure Money program at https://www.usps.com/shop/money-orders.htm and https://www.usps.com/international/money-transfers.htm. Postcoin would allow the Postal Service to make these services cheaper and faster and could extend their reach to more countries.

Figure 5: The Working Model of a Postcoin Transaction



Source: OIG and Swiss Economics.

These enhancements to existing financial services are actionable in the short-term, and over time, the Postal Service could naturally expand into new product areas. For example, the Postal Service could offer blockchain-based escrow services, acting as the trusted and neutral third party for transactions that take place both in the real world and online. This type of service would be especially beneficial for peer-to-peer commerce.[51] Additionally, the Postal Service could offer currency exchange services. This service could allow the traveler to obtain foreign currency at ATMs or post offices at lower transaction and exchange rate fees.

In the long-term, the Postal Service's experience with blockchain technology in financial applications could further expand into non-financial application areas that would be enabled by the technology. In the following sections, we outline three other blockchain applications of potential interest to the Postal Service.

51 OIG, *Peer-to-Peer Commerce and the Role of the Postal Service*, Report No. RARC-WP-13-005, January 14, 2013, https://www.uspsoig.gov/sites/default/files/document-library/2013/rarc-wp-13-005.pdf.

Identity Services

In order to facilitate safe and transparent financial transactions across a blockchain — either a postal or a nonpostal blockchain — the Postal Service could offer identity verification services. The lack of verified identities presents a security issue, a weakness of blockchain discussed above, and places users at risk for fraud. A verified digital identity would allow users to know that the peers they are transacting with are real and have proof of ownership.

The Postal Service could verify identities in-person at a post office by using an identification card, such as a driver's license, or a biometric ID, such as a fingerprint. The Postal Service could further link that virtual identity used by the customer to operate within a blockchain system with real-world identifiers, such as a person's postal address. Customers could use these verified identities to login to secure websites, notarize documents, or participate in smart contracts.

The Postal Service already has experience identifying customers for its own services and for services that it offers to other agencies. For example, many post offices process passport applications for the Department of State, an identification process that involves verifying both proof of identity and proof of U.S. citizenship.[52] The Postal Service is also familiar with managing login information for secure government sites through the Federal Cloud Credentialing Exchange (FCCX) program.[53]

Identity services are one of the biggest areas of opportunity in the blockchain community, and the Postal Service, as a highly trusted government agency, would be well-suited for a role in identity verification.[54]

Device Management

Another potential application of blockchain technology is using it to secure and maintain the Internet of Things — the network of connected devices sensing the environment and acting upon collected data. Blockchain may be a viable way for the Postal Service to build and manage an Internet of Postal Things at a lower cost than traditional, centralized methods.[55] As the Internet of Postal Things scales and thousands of more devices are brought online, blockchain's decentralized control and verification system could potentially allow devices to more securely record and transfer data. This would also help increase the security of the overall network by removing the risks associated with single points of access, as exists in centralized networks.[56]

In addition, device management through a blockchain could strengthen the ability of devices to actually act upon the information they collect.[57] With blockchain technology, peer networks of devices would be able to "negotiate" directly with internal and external stakeholders or even other connected devices to, for example, share power resources or contract for maintenance services and part replacement. This could help reduce the infrastructure and maintenance costs of managing the whole system and increase its efficiency.[58]

---

52 U.S. Postal Service, "Passport Campaign: Postmaster Toolkit," https://about.usps.com/postal-bulletin/2004/html/pb22131/kit-textx.html.

53 U.S. Postal Service, "Federal Cloud Credential Exchange (FCCX)," https://about.usps.com/news/secure-digital/welcome.htm and U.S. Postal Service, "USPS Connect," http://about.usps.com/news/uspsds/connect.htm.

54 Alex Voto, in discussion with the author, February 4, 2016. New startups, such as Onename, are already looking into providing identity services on blockchains. See, "Blockchain ID. A Better Identity," onename, https://onename.com/. However, an identity verification service backed by the highly trusted Postal Service could be a potentially stronger market option.

55 The OIG defined and discussed the Internet of Postal Things in a previous paper. OIG, *The Internet of Postal Things*, Report No. RARC-WP-15-013, August 3, 2015, https://www.uspsoig.gov/sites/default/files/document-library-files/2015/rarc-wp-15-013_0.pdf.

56 IBM Institute for Business Value, *Empowering the Edge*, p. 1.

57 Devices are frequently already equipped with the capability to act upon the information they collect. For example, thermostats not only collect data about ambient temperature but also turn on the appropriate heating or air conditioning systems to reach a desired temperature.

58 IBM is already imagining how this could look, through the ADEPT proof of concept. While this project has so far been tested on a very limited scale, researchers at IBM's Institute for Business Value were able to demonstrate that a washing machine was able to contract with third parties to request service calls, order refills of detergent and replacement parts, and negotiate power usage during non-peak times. See IBM, "Empowering the Edge: Use Case Abstract for the ADEPT proof-of-concept," 2015, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&htmlfid=GBE03666USEN&attachment=GBE03666USEN.PDF.

Imagine if postal vehicles and sorting equipment could manage their own tracking, monitoring, and maintance. For example, a vehicle could monitor the performance of its brake pads, determine when one is about to wear out, find out if that part is still under warranty, create a contract with the manufacturer to install a replacement part, and then pay for the brake pad and service — all autonomously. In general, "predictive maintenance" of vehicles has already demonstrated cost savings in other industries, and would help to reduce both regular and overtime hours at postal Vehicle Maintenance Facilities. Predictive maintenance alone could potentially help the Postal Service save 7 percent of current fleet costs, and increasing the level of automation through use of blockchain could create further efficiencies.[59]

Supply Chain Management

A final application that might also prove useful for the Postal Service is better supply chain management: using blockchain to identify packages and mail in the same way individuals can be identified. As mentioned previously, blockchain removes the need for trust between parties, allowing it to coordinate the activities between parties more efficiently. The Postal Service has a number of customers, partners, contractors and other stakeholders that it coordinates with, including: other posts, customs agencies, shipping partners (UPS and FedEx), long-haul trucking drivers, mailers, and recipients. Using blockchain to manage interactions between these different entities could speed up shipments, particularly international ones.

Imagine if each mailpiece was embedded with a sensor that could keep track of its own chain of custody while executing smart contracts for payment and customs clearance. Each mailpiece, whether a parcel or letter, could be uniquely identified on a blockchain and have the ability to create transactions, allowing for the timely sharing of information and processing of payments. It would currently be prohibitively expensive to tag every piece of mail with a sensor. However, it may be possible that the Postal Service could initially use the blockchain approach on high-value shipments in its early adoption stages and then rely on downward pressure on the cost of sensors to expand the feasibility of wider use over time.[60]

This application would allow the Postal Service to keep an auditable chain of custody and embed additional shipment and tracking information to facilitate customs clearance and faster delivery. Furthermore, payment processing could be integrated directly into the shipping process — and paying in a digital currency would lower costs for online merchants and facilitate ecommerce while also allowing people without bank accounts to participate.

This approach is already being tested in the private sector: one of the current experiments on the Ethereum blockchain involves invoices that are automatically paid when a shipment arrives.[61] There could be great potential for such an application in the cases of dropshipping, worksharing, or settlement of international terminal dues.

In essence, blockchain technology allows for close linkages between the financial, logistics, and delivery parts of commercial transactions with the power to unify payment and delivery in one seamless experience.[62] Posts could become a single intermediary between merchants and customers, allowing them to reduce coordination needs, offer more efficient ecommerce solutions, contribute to the growth of ecommerce (particularly cross-border ecommerce), and increase their market share and revenue.

---

59 OIG, *The Internet of Postal Things*.
60 John Cohn, in discussion with the author.
61 "The Great Chain of Being Sure About Things," *The Economist*.
62 The UPU already considers crypto-payment systems as a potential way to simplify the complex system of international transactions as they offer the possibility to synchronize financial and physical (logistics) transactions. José Anson, 2014.

Conclusion

Blockchain, as a decentralized information and value transfer platform, has the potential to disrupt sectors that rely on intermediaries to perform verification or tracking activities. It is currently gaining a lot of buzz as developers apply it to more and more use cases and as global companies and governments explore its possibilities. As the technology reaches what Gartner calls the “plateau of productivity,” we will discover which applications will be the most suitable for blockchain technology. In particular, the use of blockchain technology could prove to be beneficial in specific applications that cross national borders or require the interaction and agreement of multiple untrusted parties. In addition, benefits could rise from the technology’s ability to help lower costs, speed up transactions, and introduce a level of automation into processes.

The Postal Service could benefit from blockchain technology in the short term by studying the technology and possibly experimenting with blockchain-based solutions for financial services. The Postal Service already offers some financial services, including money orders and international money transfers, where blockchain could be an enabling tool, allowing the Postal Service to offer these services more efficiently. Over time, this experience and experimentation with blockchain could naturally expand into other areas, such as identity services, device management, and increased control over the ecommerce supply chain. Because this technology is likely to be a disruptor in areas of the Postal Service’s business, monitoring the development of this technology and beginning to experiment with its possible applications could benefit postal operations and customers.

Appendices

Click on the appendix title to the right to navigate to the section content

Appendix A: The Blockchain Mechanism Detailed

As mentioned in the paper, blockchain technology was invented with the creation of Bitcoin, the first decentralized "cryptocurrency," in 2008.[63] Bitcoin is a specific open source protocol designed to transfer a specific digital coin, a Bitcoin, which represents value. The main innovation of Bitcoin is that it makes it possible to digitally send something of value (be it money, property, or information) directly between individuals (peer-to-peer) without an intermediary institution. In order to see how exactly Bitcoin accomplishes this goal, the OIG worked with Swiss Economics to detail how Bitcoin works.

How Bitcoin Works

The peer-to-peer digital transactions that Bitcoin enables, such as payments, were impossible in the past because of the problem of double-spending. If, for example, one person sends an e-mail to another, both end up with a copy of the e-mail. This is beneficial for communication, but does not work for money; a certain unit of money must be unique or it loses its value. If a dollar could easily be copied, it would not be associated with value anymore. For a payment to be valid, it must be clear that the recipient is the sole owner of that dollar (or Bitcoin) and that the sender no longer has rights to use it.

Video 1: How Bitcoin Works

Bitcoin resolves this problem by using a decentralized public ledger that Bitcoin users verify through cryptography. When a transaction occurs between two users, the software broadcasts the number of Bitcoins transferred, the public addresses involved, and the time of the transaction. When a user transfers a Bitcoin, the transaction information is recorded in the public ledger and becomes proof of the new ownership. This ledger is similar to the double-entry ledgers used in the financial industry currently, where the traditional intermediary (such as a bank) debits and credits sender and recipient appropriately. Everyone in the network agrees that this public ledger is the only legitimate record of Bitcoin transactions. Because of this mechanism, each coin contains its complete transactional history. This public ledger has become known as blockchain, and the word blockchain can refer to the Bitcoin blockchain specifically or any similar public ledger system.

Transactions are bundled in a block and only added to a blockchain after the network validates it. So-called miners are nodes that bundle transactions in a block and receive the associated transaction fees and some new Bitcoins as a reward. In order for a block to be valid, miners have to show a "proof-of-work" consisting of solving a cryptographic problem. The difficulty of the cryptographic problem is regularly changed to ensure that blocks are created at a regular interval (every ten minutes on average). Because of the computing power required for mining, currently, each miner does not usually represent an individual but a collective of individuals pooling their computing power together.[64]

In addition to miners, there are other nodes throughout the network. Nodes hold a copy of the full blockchain and help to verify blocks. They also verify transactions and pass them on to other nodes. While both miners and other nodes are involved in the verification of blocks, the difference between the two is that nodes only verify blocks after blocks have been created, whereas miners create blocks (a process that requires special mining hardware). The network is also comprised of users, participants in the system that hold wallets and trade Bitcoins on the Bitcoin blockchain but do not create or verify blocks or transactions.[65]

---

63 Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System."
64 As time has gone by, the computing power required to solve a block has grown enormously, meaning it has become more difficult to create a block.
65 Christian Jaag from Swiss Economics, in conversation with the authors, January 6, 2016.

Bitcoin as a Form of Currency

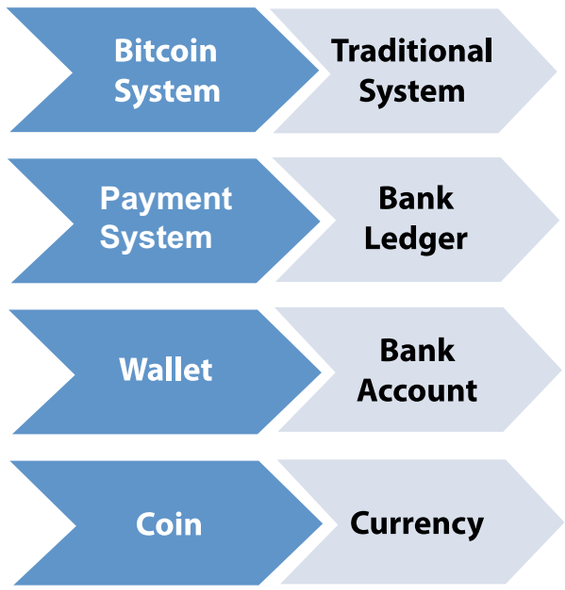
Bitcoin was created to be a purely digital form of cash — money in the form of data streams — that can be traded directly from person to person without intermediaries to the transaction. Like cash, Bitcoin is quick, direct, inexpensive, irreversible, and confidential. Also like cash, users can acquire Bitcoin in exchange for a national currency the way one might exchange Dollars for Euros through a number of companies that provide exchange services online. Unlike cash, Bitcoin is location independent and issued by the network of its users instead of by a national bank.[66] Bitcoins receive their value from their usefulness and the confidence of those participating in the system.[67] While some consider Bitcoin to be a new form of currency, others say that it is not yet widely enough used nor a stable enough store of value to be considered a currency.

Three different components comprise the Bitcoin working model and enable it to perform as a kind of digital cash:

- **The payment system:** Bitcoin provides a system for payments between users through a digital transaction that is distributed over a peer-to-peer network, posted on the public ledger, and verified by the network.
- **The wallet:** Usually stored on a user's mobile phone or computer, a wallet enables use of Bitcoins by storing the information needed to receive and spend Bitcoins.[68]
- **The coin:** The Bitcoin is the unit of currency that denotes value the way a dollar denotes value. It has a unique identity that is tracked along the blockchain and stored in user's wallets.

This working model is not extremely different from the way the financial industry is set up currently.

Figure 6: The Bitcoin System Compared to the Traditional System



Source: OIG.

66 Christian Jaag, and Christian Bach, "Cryptocurrencies: New Opportunities for Postal Financial Services."
67 The supply of Bitcoin is limited, and as the demand for units of Bitcoin increases so does its value (which is usually expressed in comparison to the US Dollar).
68 In the case of a cryptocurrency like Bitcoin, a wallet contains alphanumeric "keys" that are needed to sign transactions. Bitcoin uses both public and private keys for transactions. These keys could also be written down on a piece of paper for safe, long-term storage in a non-electronic form. In order to send and receive cryptocurrency, however, the keys need to be accessible electronically.

Other Coins Based on Bitcoin

The Bitcoin protocol is open source, meaning anyone can access it to see how it works and copy the software for their own uses. Consequently, there are now many alternative coins, or "altcoins," which are other cryptocurrencies that utilize blockchain technology and are based on the same underlying principles of Bitcoin with minor adjustments. Some examples of popular altcoins include Litecoin which is essentially an identical protocol but with a different proof of work, a shorter validation time, and a greater supply of coins; and Peercoin, which mainly differs in the validation mechanism for blocks as it not only considers computing power but also the amount of coins in possession by the miner. There are hundreds of altcoins in existence, but Bitcoin is by far the most widely used blockchain-based currency.

In addition to altcoins, other new blockchains have been designed for different applications beyond just financial applications. For example, Omni Layer aims at facilitating the creation and trading of smart properties and user currencies as well as other types of smart contracts. Omni Layer thereby serves as a binding between Bitcoin, smart properties, and smart contracts created on top of the Omni Layer protocol. Another similar example of innovation on the Bitcoin protocol is the concept of colored coins, which offer greater functionality by allowing users to tag (or "color") certain Bitcoins to represent a specific asset. This tag can be identified even after many transactions. These innovations have led to the discussion of trading assets and smart property via the Bitcoin protocol.[69] Further advancements include open payment systems like Ripple or distributed application platforms like Ethereum, a blockchain-based platform designed specifically for use in smart contracts.

Although the Bitcoin blockchain was the first use of blockchain, the term blockchain technology now refers to the technology underlying Bitcoin, altcoins, and these other similar systems.

Consensus Mechanisms

One of the changes that some altcoins have made is in the type of consensus mechanism used. In order for a transaction to be included in a blockchain, the network must reach consensus as to whether a transaction (or block of transactions) is valid. There are many ways to reach consensus; the Bitcoin's mechanism is only one. A few of these "consensus mechanisms" are explored below.

- **Proof-of-Work**: This is the consensus mechanism that requires miners to solve cryptographic problems, as described above. In addition to Bitcoin, Litecoin and Ethereum use proof-of-work consensus.[70]

- **Proof-of-Stake**: Members of the network who own a certain amount of coins or have owned coins a certain amount of time are allowed to verify blocks. Users that do not have enough "stake" in the system, either by amount or by time, are not allowed to create blocks. Ripple is a system that uses proof-of-stake consensus.[71]

- **Proof-of-Importance**: Only a user with a certain level of importance, as defined by the number of transactions a user participates in and whom he transacts with, can verify a block. NEM is a blockchain-based system that uses proof of importance consensus.[72]

It is also possible to use multiple consensus mechanisms jointly. For example, the altcoin Peercoin uses both proof-of-work and proof-of-stake.[73]

---

69 Tim Swanson, "Smart Property, Colored Coins, and Mastercoin," *CoinDesk*, January 22, 2014, http://www.coindesk.com/smart-property-colored-coins-mastercoin/.
70 However, there are plans for Ethereum to move to a proof of stake mechanism.
71 Bryant Gehring, "The Ripple Ledger Consensus Process," *Ripple*, February 20, 2015, https://ripple.com/knowledge_center/the-ripple-ledger-consensus-process/.
72 See video at www.nem.io.
73 "Frequently Asked Questions," *Peercoin,* https://peercoin.net/faq.

Additionally, there are other, simpler consensus mechanisms being used in the development of private blockchains for enterprise. For example, a blockchain might use multi-signature consensus, where each transaction must get a certain amount of approval (such as eight out of the 10 participating entities must agree), or round robin voting where each participant votes whether a transaction is valid and a simple majority wins.[74] Companies like Gem and Tendermint are working to utilize these less-expensive forms of consensus within the blockchain environment for enterprise. For example, Tendermint's blockchains verify transactions when a block is signed by a quorum of validators.[75]

74 Emily Vaughn in discussion with the author.
75 "The Tendermint Socket Protocol (TMSP), *Tendermint*, December 19, 2015, http://tendermint.com/posts/tendermint-socket-protocol/.

Appendix B: Management's Comments

RANDY S. MISKANIC
CHIEF INFORMATION SECURITY OFFICER
AND DIGITAL SOLUTIONS VICE PRESIDENT

UNITED STATES POSTAL SERVICE

May 19, 2016

ALLISON GLASS
RISK ANALYSIS RESEARCH CENTER
U.S. POSTAL SERVICE, OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Blockchain Technology: Possibilities for the U.S. Postal Service (RARC-WP-XX-XXX)

Thank you for the opportunity to review and comment on the Blockchain Technology Report. This whitepaper on Blockchain technology provides an excellent high-level overview of some of the opportunities. The Postal Service will continue to examine Blockchain technology in our innovation activities for identity management, supply chain management and secure electronic communications. As highlighted in the report, we will need to be cautious in specific implementations to account for technology barriers, security concerns and regulatory uncertainty. We will evaluate the use of Blockchain for each of the use cases and further review the available opportunities while considering the impact of the technology and financial restrictions.

The report and management response do not contain information that should be exempt from disclosure under the Freedom of Information Act.

Responsible Official:
Chief Information Security Officer & Digital Solutions, Vice President

Randy S. Miskanic

cc: *Manager, Corporate Audit Response Management*

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-4021
WWW.USPS.COM

OFFICE OF
INSPECTOR
GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms.
Follow us on social networks.
Stay informed.

For media inquiries, contact Agapi Doulaveris
Telephone: 703-248-2286
adoulaveris@uspsoig.gov