PARADIGM TECHNOLOGY

_____

The Blockchain Revolution is Here: What do you need to know?

INTRODUCTION

Imagine a world where you don't have to pay costly legal fees to get a contract executed; a world where you no longer need a bank to be an intermediary for a transaction. Imagine a world where every single device with an on/off switch is connected to each other and identity theft is a thing of the past. A world based on trust.

Sound ridiculous? Think again.

Blockchain technology is revolutionizing the world as we know it. Some say its impact on our lives could be as profound as the internet. While currently most associated with cryptocurrency, that is only scratching the surface of its capabilities, and it is only a matter of time before its impact is felt on everything from how doctors track and store our medical records to how our identities are securely and safely verified at airports.

In the simplest of terms, a Blockchain is a decentralized peer-to-peer network that allows two parties to deal directly with each other without the need for an intermediary. They rely on unique cryptographic codes that provide a fully transparent, chronological order of events that is indisputable and visible to all users on the network, while at the same time protecting the identities of those involved. The benefits to this type of network are the potential cost savings they offer by cutting out a middle man, enhanced user trust as well as alleviating time delays caused by waiting for a transaction to be verified.

There is no question that there is still much to be learned about Blockchain. But one thing is clear: Whether you are running a business or just a forward thinking individual, learning more about it now will better prepare you for the world to come.

Blockchain and Cryptocurrency are not the same things:

Over the last eight years cryptocurrency has become a digital asset that serves as a medium of exchange using cryptography to secure currency transactions. As Bitcoin has risen in prominence and expanded it's presence worldwide, a healthy dose of intrigue and skepticism has emerged in financial markets. The recurrent pattern of Bitcoin, whether it is the value, security breaches or concerns about worldwide adoption have, to this point, dominated the conversation. As a result, people who are uncomfortable with or skeptical of the long-term viability of cryptocurrency tend to dismiss its long-term relevance.

There is a disproportionate lack of knowledge of the underlying architecture of cryptocurrency (Blockchain). In large part, this is due to the fact that Bitcoin was one of the first applications created to run on a Blockchain network, and it quickly became the most well-known application associated with it. That, along with the fact that cryptocurrency is attempting to completely change the world's financial markets in the same way the internet completely changed our lives decades ago[1].

While the purpose of this paper is to discuss Blockchain, not cryptocurrency, it is first important to explain what cryptocurrency is and how it works. To do so, we will use Bitcoin as an example.

Bitcoin was established in 2008 by an unknown programmer or group of programmers operating under the name Satoshi Nakamoto. It was in essence established as a response to the worldwide financial crisis at the time and the general lack of trust people

had for centralized financial services and banks. The underlying purpose was to cut out these centralized services, associated fees and time delays these entities require. As people have come to understand the potential benefits of such a system, more have bought in. Bitcoins are now being accepted world-wide as a way to buy tangible goods and services, from food to plane tickets to real estate.

The Bitcoin Network works similar to a stock exchange. When someone buys bitcoins, they gain access to the Bitcoin platform and are therefore able to buy and sell coins as they see fit. There are numerous ways to buy and sell bitcoins. Two parties can directly trade with each other using an intermediary to facilitate the connection. You can also go through an online exchange, where you are selling to the exchange, not a specific person. Finally, there are peer-to-peer trading marketplaces that allow bitcoin owners to obtain goods with bitcoins by exchanging them to people who want to obtain the coins using credit/debit cards[2].

However, Bitcoin's capabilities are still limited, and many economists and lawyers have concerns about its underlying system and method of regulation[3]. In addition, since bitcoins have no intrinsic value in that there is no physical form that can be redeemed at a bank or cashed out, the coins are worth whatever price the buyer and seller agree upon. Thus, the tangible value of the coins is extremely volatile. There are also a number of security vulnerabilities that exist, which will be discussed later.

A Blockchain is a peer-to-peer network that allows two parties to deal directly with each other without the need for a middleman. There is no central repository or single administrator on a Blockchain, which means they are entirely decentralized. They are public ledgers of all transactions/events on the network, which means all people within the network can see every transaction, thereby establishing trust. However, while every transaction is visible to the network, the identity of the parties involved remains private. Each transaction has a unique cryptographic code, which only the parties involved have access to.

Every few minutes, every transaction made on the network during that time period is grouped together in a block. Each block is added on top of the previous blocks, creating an indisputable chronological order of events for all to see. Each node (computer connected to the Blockchain network) gets a copy of

the Blockchain and automatically downloads upon joining the network.

The public nature and unique cryptographic codes associated with the network and transactions make it almost impossible to hack, greatly reducing security vulnerability. As previously stated, currently the most prominent use of Blockchain technology is cryptocurrency. But that is changing—and fast. New applications are being developed, and getting involved now would provide your organization a distinct competitive advantage in the future. Let's take a look at how:

Smart Contracts

Smart Contracts are automated computer programs that are uniquely coded and programed to enforce the elements of any contract when stated conditions are met. For example, if the contract says Company A will send a particular set of products to Company B when certain conditions or payments are made, a Smart Contract will automatically notify the supply chain to carry out those terms in a transparent and chronological manner. There are many benefits to these types of contracts.

First, they reduce costs by cutting out the need for a middleman such as a lawyer to develop and execute the contracts. In addition, the terms of these contracts are unbreakable since they rely on trust established by being executed on a public network. The associated cryptographic codes make it impossible to change the terms of a contract without the other parties being made aware of these changes. These contracts are also more efficient and quicker to execute since the terms are automatically enforced as are the associated action triggers. Perhaps even more important than reduced costs and increased efficiency is the reduction of legal battles that can often come about by hard copy contracts written out by third parties. Vague wording and terms in these contracts make it easier for legal disputes to arise. Consequently, they are more likely to cause the need for legal remediation.

Smart Contracts are already being used by companies across various sectors, from banking to real estate to retail.

Digital Identification/Fraud/Data Breach Prevention

Fraud and identity theft are constant threats in this day and age. The recent hacks of Equifax, Sony and HBO reinforce this. In fact, according to a report dually published by The Identity Theft Resource Center and CyberScout in July, data breaches have been increasing at a record setting pace in 2017[4]. Per the report, there were 791 instances of data breaches in the first half of 2017, up 29% from the same time in 2016. By the end of the calendar year, it is projected that there will be more than 1,500 breaches; there were 1,093 breaches in 2016, which is the current record.

Unfortunately, there are currently no guaranteed solutions to this problem, and it is possible this fear could negatively impact the economy as people grow weary of the perils of using current identity verification methods to use services and make purchases, especially online. Thus, it is vital for companies everywhere to seek more secure methods of identity verification to avoid such a crisis. Doing so would undoubtedly increase public trust levels, and leveraging Blockchain technology may prove to be the ideal solution.

According to Ameer Rosic, founder of Blockgeeks, in a blog post written for Due.com in November 2016, "Blockchain technology offers a solution to many digital identity issues, where identity can be uniquely authenticated in an irrefutable, immutable, and secure manner. Current methods use problematic password-based systems of shared secrets exchanged and stored on insecure systems. Blockchain-based authentication systems are based on irrefutable identity verification using digital signatures based on public key cryptography[5]."

It is possible that one day soon, Blockchain-based applications will be used as a means of identity verification for everything from government-issued IDs and passports to online log-ins for retail and banking services. Being among the initial group of companies to implement such applications could provide a huge advantage over the competition.

Insurance

Blockchain will have an impact in the finance sector in ways far beyond cryptocurrency. One such example is the insurance space. Currently it is a dull

and time consuming process as claims must be processed manually from various data sources and checked against legacy policies, which increases the risk of human error. Blockchain technology has the potential to make the process much more efficient and accurate because of the transparency and encryption, which allows insurers to better identify ownership of assets to be insured[6].

In a report published by McKinsey & Company Financial Services in July 2016, multiple areas of impact are identified for insurers, including improving customer engagement and enabling cheaper offerings in emerging markets[7]. The speculated impact on customer engagement is tied into a number of things, including the storing of personal data and the aforementioned Smart Contracts. A customer-controlled Blockchain of personal data could alleviate the frustrating process of re-verifying data every time said customer comes into contact with the insurance company. This doesn't mean that all personal data is stored on the Blockchain, just certain verifiable transactions and events (Example: A doctor appointment on a certain date). This benefit is largely tied into data security and fraud prevention, which is detailed further below.

Smart Contacts would have a tangible impact on insurance claims through its automated function of events caused by certain triggers. A good example could be the recent natural disasters that occurred in 2017. If a homeowner in an area at a greater risk for a hurricane has a reimbursement payment tied into one of these events taking place, a Smart Contract would automatically trigger this payment and save these customers from dealing with more stress at a time where that would be greatly appreciated. This would not only increase customer engagement, but also help in emerging/new markets since certain regions require unique plan offerings based on geography and location.

Internet of Things:

In the simplest of terms, "Internet of Things" is essentially the interconnection through the internet of computing and everyday objects, enabling them to send data back and forth to each other and sync up. This not only refers to technological objects such as cellphones, but everyday household objects like

washing machines and lamps. Essentially, if something has an on/off switch, it can be connected. Esteemed analysis firm Gartner estimates that, by 2020, there will be up to 26 Billion interconnected devices[8]. The purpose is to streamline information to help us in our everyday lives, and this can involve anything from understanding traffic patterns to helping people with everyday disabilities live a more normal life[9].

Clearly a world where everything is connected creates a huge amount of security concerns, which is what Blockchain technology will help solve. Given its transparency, decentralized and cryptographic nature; and the enhanced security against data breaches it provides, Blockchain is a more scalable way of providing more robust security than traditional methods.

In a 2016 report published by Ahmed Banafa, a tenured professor and lecturer who has specialized in IoT, he says that the current enterprise model of cloud storage to connect devices will not be able to keep up with the projected growth of the IoT ecosystem, both because of the rapid growth and the cost increases. He further hypothesizes that Blockchain may be the "missing link" to establish the security standards required, and to truly connect devices to one another, establish secure communication and track transactions and usage while lowering the cost for the industry as a whole. It would also eliminate the possibility for a single point of failure. So, while it is certainly not without its issues (such as processing delays, legal/compliance concerns and a lack of skills in the job market), it is being looked at as a building block for the future of the industry[10].

Blockchain and Security

One of the great ironies of Blockchain is that many of the issues these platforms are made to resolve, such as peer-to-peer trust established without a middleman and identity authentication, are also the areas where the greatest security vulnerabilities exist.

To illustrate this, let's look at it from a real world perspective. Let's say you are looking to buy tickets to a sporting event or concert. Currently there are three main options: Buy from a private broker; visit a ticket exchange website like Stubhub or go onto a site like Craigslist. Each has their pros and cons.

When buying from a broker, you are able to establish trust by meeting with the individual face-to-face. In this situation you are able to ensure the tickets are real and establish trust in a traditional method. But you are also paying an added cost to the broker, who is looking to profit from the transaction. Option two is going through an online ticket exchange, which has similar pros and cons as using a bank to manage a financial transaction: You are paying a fee to a middleman in exchange for processing the transaction.

Now let's consider option three, Craigslist. In some ways it could be classified as an extremely primitive Blockchain in that it relies on peer-to-peer trust. But how can you be sure you are buying authentic tickets, or that the seller is someone who can be trusted? Since all users are not notified of others' transactions, how can you hold the other party accountable, or prove that you paid for a service that was never provided?

A Blockchain answers most of these questions through unique cryptographic codes, establishment of chronological events and transaction notifications to the entire network.

However, unlike a Blockchain, other Craigslist buyers and sellers are not notified of a transaction, meaning there is a much higher likelihood of fraud.

But a Blockchain is not bulletproof. A solid network architecture is required and, because of the amount of electricity and energy each node requires to function properly, they are also expensive to operate. Consequently, each node must be configured in such a way that a backup plan is in place to maintain proper communication and function within the network should a node (or multiple nodes) go off line or malfunction in any way.

One way to address this issue is to put the most powerful nodes in areas of the Blockchain that require the most connections and connecting less powerful nodes to these nodes to ensure proper function[11]. As such, regions with cheaper energy costs are in a better position to make up the majority of a Blockchain network because it is more efficient to have more powerful nodes in these areas. This increases the risk of black market centralization, potentially neutralizing the transparent establishment of trust the Blockchain is intending to create.

Ironically, the best way to mitigate this risk—and the thing that is most likely to cause the biggest public backlash, is through the same type of information that would be utilized to solve the data/fraud prevention issue mentioned in the previous section: personal data and biometrics[12]. Since we've already identified the security risks surrounding password authentication, it is obviously not a solution to this issue. Biometrics refer to the measurement and statistical analysis of a person's physical and behavioral characteristics. This technology is mainly used for identification and access control. In Layman's terms, it refers to an individual's physiological characteristics such as DNA and fingerprints and behavioral characteristics such as gait, gestures and voice. This information is then cross-referenced against a database with stored, confirmed authentic data, thereby providing a more secure means of identification than password verification. On the surface this may seem like something you might see in a futuristic Sci-Fi movie like *The Matrix*. It may even seem as an invasion of privacy.

The process of obtaining and storing this information on a Public Blockchain will probably scare the general public and require a lot of education to help people feel more secure and comfortable with it. A comprehensive Blockchain will require a digital representation of a person's identity, meaning that not only will the biometric information be stored in cyber space permanently, but it will also be stored on nodes across various Blockchain networks[13].

And yet, in reality, biometrics actually are beneficial for an individual. Whereas passwords and credit information are prone to fraud and theft, biometric information, particularly physiological traits, are completely unique to an individual. One could also make the argument that, with data and identity theft being as prevalent as it is, an individual's information is already permanently available in cyberspace; the difference being that in one scenario hackers are able to lurk in the dark, in the other there is a traceable transparency that makes it infinitely harder to truly "steal" an identity.

Nevertheless, the complexity and lack of knowledge about biometrics and the potential benefits and consequences are something any organization must consider when deciding on investing in a Blockchain, since there will undoubtedly be some employees who are uncomfortable allowing this sort of

information to be stored on a Blockchain network forever.

An effort is already underway to standardize the process of using biometrics for identity management on a Blockchain. According to John Callahan, CTO of Veridium, a company that specializes in biometrics-based authentication solutions, standards and documentation such as Decentralized Identity Documents are being created, although they are in their nascent phases and confined to specific Blockchains[14]. He adds that a future Blockchain will require open communities of information across different Blockchain networks in order to achieve interoperable identity standards, and predicts that, once achieved, biometrics will be the key to linking a person to their identity claims.

Tying this all into the ticket purchase scenario above, and it becomes the key to establishing trust in dealing with total strangers no matter where they are physically located and closing the Blockchain loop. It allows for the convenience of purchasing tickets online, the removal of a middleman and added costs and the essential trust and transparency that classified advertisement websites like Craigslist are unable to provide.

Private Blockchains:

While Public Blockchains have the greatest potential to impact our daily lives, there is another version being developed that may be better suited, in the short term, for government entities and private businesses: Private Blockchains.

While fundamentally using the same type of architecture as a Public Blockchain, instead of having no central authority figure, control is given to a central entity within a Private Blockchain. This entity is then able to control permissions so not everyone on the Blockchain has access to read every transaction[15].

This type of Blockchain is controversial, since the biggest advantage of Blockchain technology is supposed to be the establishment of transparent peer-to-peer trust. This advantage is greatly compromised when control is given to a central figure, no matter how trusted that figure is by everyone on the network.

Some argue that this type of Blockchain is no different than other distributed ledger technology

already in the market, especially since the central authority has the power to reverse a transaction. Others say it is a great way for an organization to initially start implementing a Blockchain strategy.

In a 2016 article written by Justin O'Connell published by *Bitcoin Magazine,* Lisk CEO Max Kordek says he sees a few use cases for Private Blockchain, primarily because traditional institutions, "won't switch to a completely Public Blockchain from one day to another." Kordek goes on to say that they represent a step to a more cryptographic future, and that the biggest advantages they have over traditional centralized databases are the cryptographic auditing and known identities[16].

It is also worthwhile to note that a Private Blockchain maintains some of the advantages of a Public Blockchain, such as the establishment of the chronological order of events/transactions that take place, and that transparency is maintained for those who are granted permission to be a part of the Blockchain. So, while there are certainly benefits to Private Blockchain, they are only useful if those on the network trust the central figure to maintain the integrity of the system.

The Future of Blockchain: How can Paradigm be a Solution Partner?:

One of the biggest challenges preventing the widespread implementation of Blockchain technology is the scarcity of the job market. Put simply, the supply of talent is unable to match the demand of implementation.

In an article posted by *Banking Technology* in August of this year, according to Joblift there were 546 Blockchain-related jobs posted in the UK since August 2016, and these jobs have been increasing by 25% each month, a huge increase compared to the 2% increase seen throughout the rest of the job market in the country[17].

The industry is expanding in the United States as well. As of November 2017, LinkedIn had 706 active Blockchain-related jobs posted, with the oldest one having been posted 10 months earlier, including approximately 600 over the previous month alone.

The demand is so great that in 2016, Kite Consulting Group started a worldwide Blockchain job site called BlockTribe[18].

While the market has, to this point, been catered to the finance sector, where banks are aggressively working towards developing their own Private Blockchain applications, other industries, including the airline industry and utilities sector, are starting to explore use of the technology to solve their own issues.

S7, Russia's largest airline, launched a Blockchain-based Ticketing Agent in July 2017. The platform is designed to reduce settlement times between the airline and the agent. It is an early attempt within the industry to use the platform to streamline the ticketing process. The airline is also exploring the viability of using Smart Contracts[19].

Meanwhile, Air France is exploring ways of using Blockchain to make the airline maintenance process more efficient and easier to track and other international airlines are also exploring ways to benefit[20].

Experiments are also being conducted in New York to explore potentially using Blockchain within the utilities sector to increase efficiency by using distributed energy resources such as solar power to deliver reliable and reusable energy sources to people[21]. A project being conducted known as the Brooklyn Microgrid aims to create a community-powered microgrid to allow for a sustainable energy network and for users to choose their preferred energy sources. Such a grid could also operate independently during a power outage to the larger grid, enabling the neighborhood to have a backup source of power[22].

Paradigm Technology is uniquely suited to be your partner in implementing a Blockchain strategy that works for you. We are a premier strategic solution provider. A true partner that empowers you to make smarter and more informed business decisions. We are committed to delivering highly customized end-to-end client solutions to meet your unique business needs.

SUMMARY

Despite popular belief, Blockchain technology is not the same thing as cryptocurrency. A Blockchain is a distributed ledger that cuts out the middle man in a transaction by relying on peer-to-peer trust; cryptocurrency is an application that runs on a Blockchain. On a Blockchain, every action that takes place is fully transparent to all users. However, each individual action is secured with unique cryptographic codes, meaning that while all the users on a Blockchain see the details of an event that took place, only the parties involved know the exact identity of the parties involved.

While cryptocurrency is currently the most prevalent use of the technology, it is starting to be utilized in other ways and further adoption is only a matter of time. Other current and projected value areas are revolutionizing the way two parties write, administer and enforce contracts (Smart Contracts); enhancing digital identity and fraud prevention and providing enhanced data protection. The technology will also contribute to the long term scalability of the Internet of Things (IoT).

Although companies across the US are starting to implement and explore the value of Blockchain across the enterprise and the domestic job market is growing exponentially, it has a stronger foothold in Europe (beyond Cryptocurrency). S7, a Russian Airline, recently introduced a Blockchain Application for ticketing, and other airlines are exploring the value of utilizing it for maintenance tracking purposes.

While there is still much to be learned about the long-term capabilities and the best ways to maintain proper security standards one thing is certain: Blockchain Technology is not going anywhere and exploring it's value now will create a distinct competitive advantage for organization's across all sectors, from insurance to healthcare to airlines and beyond.

About the Authors:

Paradigm Technology is a strategic consultancy that focuses on Digital Transformation, Analytics, Governance and Cloud. Started in 1994, we partner with clients to deliver business and technology solutions that enable our clients. Analytics & Governance are at the heart of the value we deliver. Learn more about us at www.PT-Corp.com

Jordan Jurkowitz is a Senior Talent Acquisition Manager for Paradigm and has been with the organization since 2014. He majored in Journalism/Mass Communication at the Walter Cronkite School of Journalism. Upon graduation, Jordan spent nearly two years writing for a local newspaper as well as BleacherReport.com.

PARADIGM™
technology

Bibliography:

1. Khalid, A. (2017, April 20). *What Blockchain Is, And Why Some Experts Say It's As Revolutionary as The Internet.* Retrieved From Http://http://www.wbur.org/bostonomix/2017/04/20/blockchain-explainer.

2. *How to Sell Bitcoin.* (2017, October 23). Retrieved From https://www.coindesk.com/information/sell-bitcoin/.

3. Ali, R., Ito, J., Narula, N. (2017, March 9). *The Blockchain Will Do to the Financial System What the Internet Did to Media.* Retrieved from https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media.

4. Identity Theft Resource Center. (2017). *At Mid-Year, U.S. Data Breaches Increase at Record Pace* [Press Release]. Retrieved from http://www.idtheftcenter.org/Press-Releases/2017-mid-year-data-breach-report-press-release.

5. Rosic, A. (2016, November 29). *6 Blockchain Applications That Go Beyond Bitcoin* [Blog Post]. Retrieved from https://due.com/blog/6-blockchain-applications-go-beyond-bitcoin/.

6. *17 Blockchain Applications That Are Transforming Society: An In-Depth Guide By BlockGeeks.* (n. d.). Retrieved from https://blockgeeks.com/guides/blockchain-applications/.

7. Lorenz, J.T., Munstermann, B., Higginson, M., Braad-Olesen, P., Bohlken, N., Ricciardi, V. (2016, July). *Blockchain in Insurance – Opportunity or Threat*. Retrieved from https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-in-insurance-opportunity-or-threat.

8. Morgan, J. (2014, May 13). *A Simple Explanation of 'The Internet of Things'.* Retrieved from https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#710bcd971d09.

9. Pott, T. (2014, August 5). *What's The Point of the Internet of Things? World Peace, natch, What did you think it was?* Retrieved from https://www.theregister.co.uk/2014/08/05/whats_the_point_of_the_internet_of_things/.

10. Banafa, A. (2016, December 21). *A Secure Model of IoT With Blockchain'.* Retrieved from https://www.bbvaopenmind.com/en/a-secure-model-of-iot-with-blockchain/.

11. Berke, A. (2017, March 7). *How Safe Are Blockchains? It Depends.* Retrieved from https://hbr.org/2017/03/how-safe-are-blockchains-it-depends.

12. Thackston, J. (2016, November 7). *Fraud and Privacy Problems on the Blockchain.* Retrieved from https://www.csoonline.com/article/3138869/security-awareness/fraud-and-privacy-problems-on-the-blockchain.html.

13. Thackston, J. (2016, November 7). *Fraud and Privacy Problems on the Blockchain.* Retrieved from https://www.csoonline.com/article/3138869/security-awareness/fraud-and-privacy-problems-on-the-blockchain.html.

14. Callahan, J. (2017, May 25). *Blockchain and Biometrics: The Future of Identity.* Retrieved from https://www.veridiumid.com/blog/future-identity-blockchain-biometrics/.

15. Thompson, C. (2016, October 26). *The difference between a Private , Public & Consortium Blockchain: A Simple Explanation for Dummies.* Retrieved from http://www.blockchaindailynews.com/The-difference-between-a-Private-Public-Consortium-Blockchain_a24681.html.

16. O'Connell, J. (2016, June 26). *What Are the Use Cases for Private Blockchains? The Experts Weigh In.* Retrieved from https://bitcoinmagazine.com/articles/what-are-the-use-cases-for-private-blockchains-the-experts-weigh-in-1466440884/.

17. *Infographic: UK's blockchain job market.* (2017, August 18). Retrieved from http://www.bankingtech.com/951362/infographic-uks-blockchain-job-market/.

18. Barnes, R. (2016, September 28). *Kite Launches Blocktribe to Assist with Blockchain Talent Acquisition.* Retrieved from https://www.financemagnates.com/cryptocurrency/news/kite-launches-blocktribe-to-assist-with-blockchain-talent-acquisition/.

19. Wolfie, Z. (2017, July 25). *A Russian Airline Is Now Using Blockchain to Issue Tickets.* Retrieved from https://www.coindesk.com/russian-airline-using-blockchain-for-tickets/.

20. Galeon, D. (2017, October 6). *One Of The World's Largest Airlines Is Looking Into Blockchain Technology.* Retrieved from https://futurism.com/one-of-the-worlds-largest-airlines-is-looking-into-blockchain-technology/.
21. Basden, J., Cottrell, M. (2017, March 27). *How Utilities Are Using Blockchain To Modernize The Grid.* Retrieved from https://hbr.org/2017/03/how-utilities-are-using-blockchain-to-modernize-the-grid.
22. Retrieved from http://brooklynmicrogrid.com/.