Stevens Institute of Technology

# Blockchain and Cybersecurity

Group 3 - Wei Chen, Deep Chokshi, John Encke, Miao Hong, Fangzhou Liu, Yuanjin Zhao

CS573

Prof. Ed Amoroso

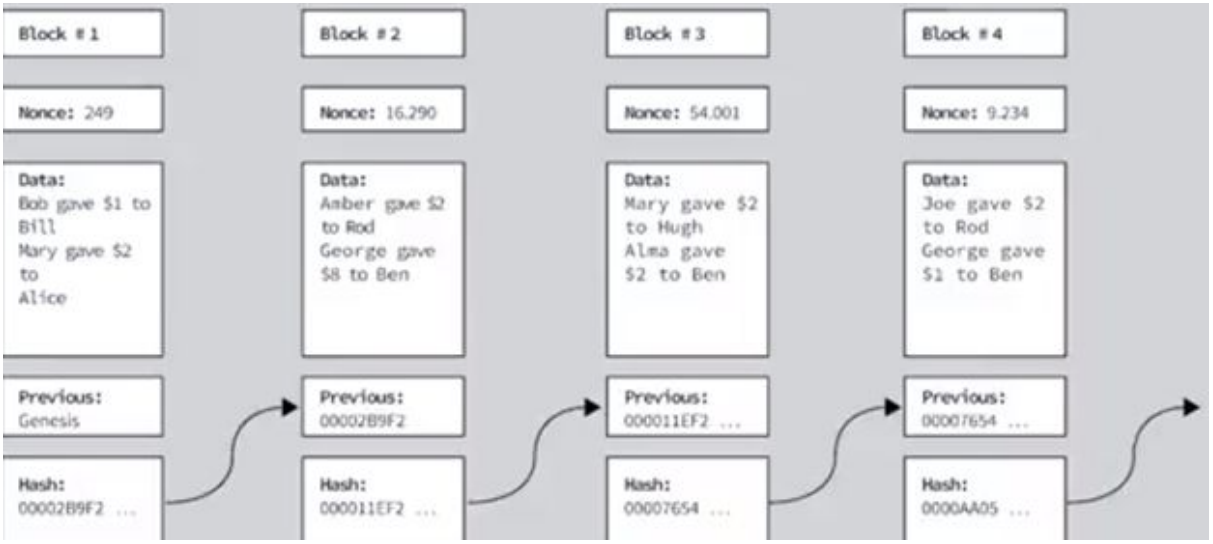
3 December 2018

**Abstract**

Blockchain is one of the biggest emerging technologies currently on the market. After its creation and successful application in Bitcoin, many industries are currently attempting to find other applications for this distributed ledger technology. This paper explores its applications in the scope of cybersecurity. We start with an introduction to the technology, followed by a discussion of the strengths and weaknesses associated with blockchain. Then we take a look at vendor applications of blockchain. Finally, we conclude by making recommendations on how blockchain technology should be applied in the future.

**An Introduction to Blockchain by Deep Chokshi**

A Blockchain is a type of diary or spreadsheet that contains record about transactions that are almost impossible to hack. Each transaction produces a hash which is a sequence of numbers and letters. in that first four letters must be zeroes. Transactions are entered in the order in which they have transpired. The order is very important because every hash depends on the former transaction's hash and even a sparse modification in a transaction generates a completely new unique hash. The nodes check to make sure a transaction has not been changed by scrutinizing the hash of all the blocks. If a transaction is authorized from a majority of the nodes, then it can be written into a block. Each and every block points to the previous block's hash and together make the Blockchain. A Blockchain is effective as it is spread over many computers, which are also called as nodes, each of which has a copy of the Blockchain.




The Bitcoin Blockchain is decentralized and is not controlled by one central authority. While conventional currencies are issued by central banks, Bitcoin has no central authority. Instead, the bitcoin Blockchain is maintained by a system of people known as miners. These miners are people running purpose-built computers that are actually competing to solve complex mathematical enigmas in order to make a transaction go through. For example, there are many people are making bitcoin transactions nowadays. Each transaction originates from a wallet that has a private key. This is a digital signature and gives a mathematical confirmation that the transaction has come from the owner of the wallet. Presently imagine lots of transactions are taking place over all around the world. These individual transactions are arranged together into a block, which is designed and bound by strict cryptographic rules. The block is assigned out to the bitcoin network, which is made up of people operating high-powered computers. These computers compete to validate the transactions by trying to solve complex mathematical issues.

Blockchain's decentralized, public & cryptographic nature empowers people to trust each other and transact peer-to-peer, making the need for intermediaries obsolete. This also

brings unprecedented security benefits. Hacking attacks that generally impact largely centralized organizations like banks would be practically impossible to pull off on the Blockchain. For example, if hacker desired to hack into a selective block in a Blockchain, a hacker would not only need to hack into that particular block, but all of the proceeding blocks going to back the entire archives of that Blockchain where they would need to do it on every entry in the network, which could be more than millions, simultaneously.

**Strengths of Blockchain Technology by Yuanjin Zhao**

Blockchain runs on a distributed network, also takes advantage of breakthroughs in encryption, and uses complex algorithms to verify the ownership and accuracy of data. Each of those functions is an element of a powerful, advanced cyber security strategy. Combining them through blockchain technology is expected to make progress for the cyber security industry. There are three aspects of cybersecurity that blockchain has the most likely to enhance or improve.

*1. Blockchain can help prevent access fraud*

One of the biggest problems with identity and access management is that users may use weak passwords that are can be easily cracked by hackers. They may use the same password in multiple applications, allowing the hackers to access sensitive information after cracking the code in one application.

The password usually running on the Public Key Infrastructure (PKI) model, and this model relies on the Central Authority (CA) to publish, revoke, and store key pairs. The key pair record the pair of the private key corresponding to the public key, and the public key is for verifying the person who use private key to access certain data and information like email, account.

If use blockchain, we can create a distributed PKI model. Instead of a CA managing key pairs, we can store that data on the blockchain. Blockchain security advocates believe that CA manages passwords is a centralized databases and systems, this will be more vulnerable to be hacked. For example, if a hacker want to access the system, he only need to ack a single, centralized point of entry, but for the blockchain, As it runs on a distributed network, and store data distributed, hacker have to access multiple points of entry at the same time to hack the network.

*2. Blockchain can help deter certain cyber attacks*

Malware and viruses are the most common types of cyber attacks, DDoS attacks also not far behind. It usually attempt to crash online services by bombarding them with traffic from many different sources at once. There is also a survey shows that over a third of businesses had been the target of a DDoS attack.

Websites crash when subjected to DDoS attacks because DNS is stored on a system that's only partially decentralized. Once hackers gain access to the centralized part of DNS, they can crash the site. If we operate DNS on a blockchain would fully decentralize the system, meaning that this can avoid the flood of traffic that crashes sites. It also means that if a hacker want to gain access to multiple nodes in the system at the same time in order to implement the attack, it would be much harder, more expensive, and more time-consuming for the hacker.

*3. Blockchain can ensure the integrity of data*

In the last part, we have introduced the security that data storage in distributed system. Also the blockchain technology also offers safeguards to ensure that data will not be destroyed or lost.

Data can never be removed from a blockchain. New or edited data is added on top of old blocks. Every time a block is added to a chain, it has a digital signature and time stamp, therefore each data is fully traceable. So if a hacker were somehow able to change data on the chain, you would be able to see when they did it and which account they did it from.

Also, if a hacker change the data on the blockchain, those changes would be detected very quickly, because every time a data is changed, the rest of the chain will verify these changes. False data, or data altered without permission, would alert the whole chain that there was an error, and the false data would be excluded from the system, keeping your data intact.

**Weaknesses of Blockchain Technology by Miao Hong**

1. No privacy

In the blockchain public chain, each participant is able to obtain a complete data backup, and all transaction data is public and transparent. Each node contains the information of the whole block. It is impossible to hide some data secretly. As more and more nodes come to the block, more and more participants will know the information. If you want to know the account and transaction information of some commercial organizations, you can know all his wealth, important assets and trade secrets, etc. There is no privacy.

2. Security issue

A major feature of blockchain technology is that it is irreversible and unforgettable, but only if the private key is secure. The private key is generated and kept by the user and is not attended by a third party. Once the private key is lost, it cannot do anything with the assets of the account. With the development of new computing technologies such as quantum computers, the future asymmetric cryptographic algorithms have certain cracking possibilities, which is also a potential security threat to blockchain technology.

3. Deferred data validation

In the financial blockchain, the time for data validation is relatively long. Take Bitcoin as an example. The validity of the currently generated transaction is affected by the network transmission. The bitcoin transaction is really about 10 minutes each time, and it takes an hour for 6 confirmations. Therefore, the transaction data of the blockchain is delayed.

4. Supervision

The decentralized, autonomous nature of the regulatory blockchain dilutes the concept of state regulation. However, all innovations need to meet regulatory requirements. The regulation of the blockchain, in a certain procedure, promotes the commercial application of the blockchain and better provides compliance protection. On the other hand, due to the lack of regulatory oversight, scams and market manipulation are commonplace, the regulatory authorities and the establishment of laws have lagging behind for this new technology, may also destroy the blockchain. So it should be careful to do it.

5. Cannot be falsified or revoked

This is both an advantage and a disadvantage. There is no regret in the blockchain. You can hardly change the data of the blockchain. It is mainly reflected in: if the transfer address is incorrectly filled, it will directly cause permanent loss and cannot be revoked; if the key is lost, the same will cause permanent losses irreparable. In reality, if your bank card is lost or your password is forgotten, you can still go to the bank's business office and your money is still there.

As a kind of innovation, blockchain can produce subversive effects in specific areas. In the face of the advantages and disadvantages of blockchain, it is necessary to do something to avoid weaknesses and use its capabilities. So whether the blockchain can be the underlying

technology of a new generation of financial infrastructure is still a problem.

**Current Applications of Blockchain I by Wei Chen**

*(1) Bitcoin*

Blockchain has been mostly recognized and admitted by society as a top-notch technology which can undergird Bitcoin and some other cryptocurrencies. The first application of blockchain is Bitcoin, established in 2009 by a mysterious person (or a mass of people) with the name "Satoshi Nakamoto" The original purpose of releasing Bitcoin is to let it act as a new variety of database, open to public (open-source) and transact without the third-party institutions like banks or governments. Following up with Bitcoin, AIX (an an open operating system from IBM that is based on a version of UNIX) and Ethereum (an open-source, public, blockchain-based distributed computing platform and operating system featuring smart contract functionality) came up into public's sight. It works as an replacement to today's currencies, with the financial industry trying to analyze and discover a method of how to use technology to trade these cryptocurrencies.

Cryptocurrencies can not only be purchased by vendors like bitcoin but also can be bought by normal people. However, a larger number of the people "mine" for them without having to put down any money. The mechanism of mining is to utilize computers to figure out complicated algorithms in order to validate the next block and verify previous transactions.

Some interesting news concerning "crypto kings" in their crypto castles, becoming richer by investing in Bitcoin and other cryptocurrencies. This hype has triggered many people to switch between the term Bitcoin and blockchain whatever they want to.

We should aware that blockchain is not Bitcoin. Here is the analogy for comparison: blockchain is to Bitcoin as the internet is to Facebook—it is the mechanism on which Bitcoin runs, giving Bitcoin its utility. Blockchain will do for transactions what the internet did for communications, allowing you to track everything to a T.

*(2) Bitcoin Blockchain PTP Process (Procure-To-Pay process)*

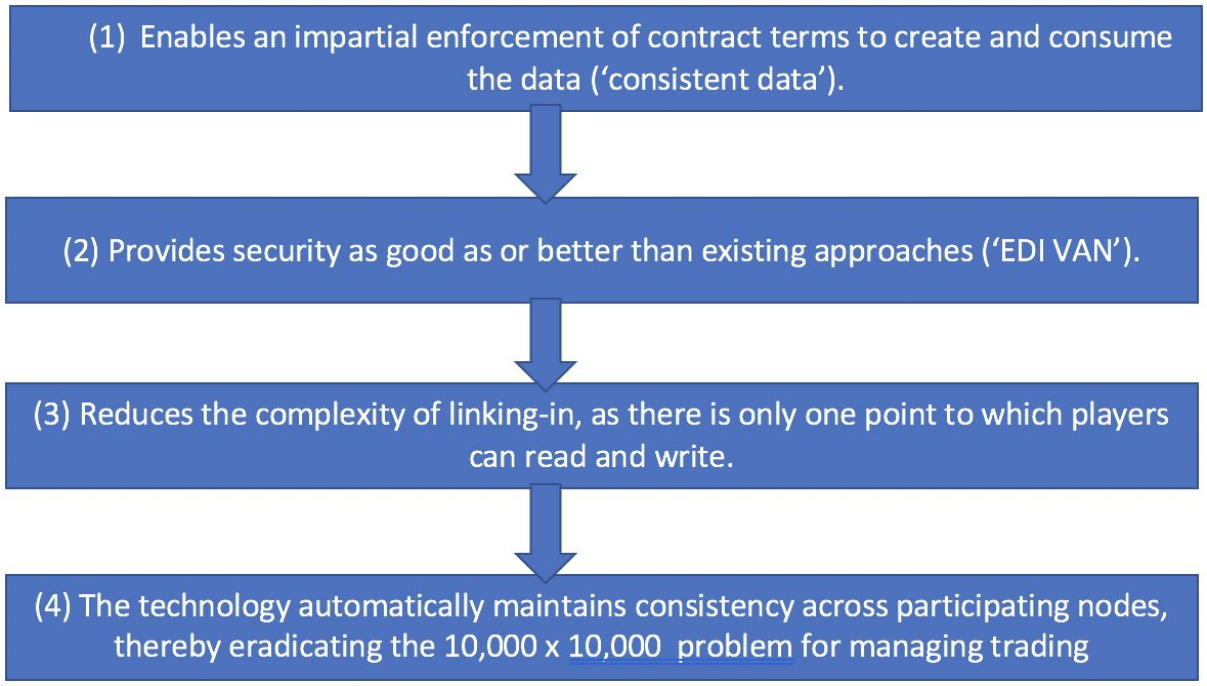
Here is the PTP Process flow chart used in Bitcoin vendor:


**Figure: PTP Process Graph**

*(3) Applied in a Single System via Supply Chain*

Blockchain is a single system of record. The most prominent feature is that only one access point has to be generated for each partner while the chain itself is reproduced across all partner 'nodes'. A unique implementation for each partner in the system, that has originally forbidden EDI-based verifications, or at least EDI-based rich transaction sets, is not necessary.

To reduce data redundancy across trading partners in a supply chain, a technical solution has been proposed: integrating blockchain with smart contracts. To realize "integrating blockchain with smart contracts", a flow chart are conceived:




Surprisingly, to supply chain operations, substantial cost reductions and efficiency benefits occurs while contracts are applied to basic applications of blockchain technology in supply chain. There are two options for this. One is to connect with suppliers and customers phase through read/write to one point for millions of participants, while the other is the

'ongoing communication' phase by enormously reducing transaction volumes and irregularities.

To avoid unnecessary reconciliation, miscommunication, and poor enforcement of joint contract standards, which will create an order-of-magnitude opportunity for those who adopt, we need the shift to a common blockchain journal of data for all parties.

*(4) Blockchain in banking, insurance and finance services*

Since 2015-2016, large financial service providers, for example, FinTechs took many initiatives in blockchain for finance. Distributed ledger technology is among others used and/or tested for insurance applications such as claims management and for banking applications where digital identity and smart contracts are just a few use cases that fit in myriad financial operations. Other areas like the transfer of funds and financial transactions are also in the vicinity of the root of blockchain.

The IBM blockchain-based cross border payment solution that the company announced on October 16th, 2017, is a symbol of exponential development in banking. The mission statement of this solution is to figure out cross-border payment challenges and provides real-time clearing and settlement.

More than a dozen institutions and banks were involved in the deployment and development process. Cross-border payments are undeniably a core use case as in 2017 also SWIFT, Mastercard and the R3 consortium took initiatives, the latter two and IBM did so in October 2017.

One of many applications that can be very useful in specific banking applications is Digital identity. It makes the way we onboard customers changed and resolves the identity problem and enabling full mobile onboarding.

Based on the data from IDC Worldwide Semiannual Blockchain Spending Guide PR in January 2018, blockchain lends itself to a number of common use cases including regulatory compliance, cross-border payments & settlements, custody and asset tracking, and trade finance & post-trade/transaction settlements within the financial sector.

Based on Juniper Research, a current dependence on paper-based legacy storage systems and/or a high volume of transmitted information are beneficial to many companies.

*(5) The Internet of Things and Blockchain Technology*

Blockchain is the symbol of missing link to tackle privacy and reliability concerns in IoT. The Integration of IoT and blockchain is viewed and effectively balanced for countless reasons, ranging from smart contracts and IoT data monetization models across complicated chains of connection where trust is vital.

Based on the background of the Internet of Things, blockchain applications come out. some vendors have particular methods to empower the use of blockchain for IoT to increase trust, save costs and accelerate transactions. The fact that several vendor and industry initiatives have been processed with novel solutions and actual deployments cannot deny IBM's pioneer effect. IoT is all about contracts, trust and transactions in a distributed environment. For comparison, Blockchain is the missing link to tackle privacy and reliability concerns in IoT as the IEEE's Ahmed Banafa writes.

One point should be mentioned is that blockchain and IoT combination also refers to assorted other technologies (e.g. AI), industries (e.g. insurance and telematics) and activities (e.g. supply chain management, security). In other words: IoT and blockchain needs to be viewed and operated in exact details and isn't just a matter of how blockchain can motivate IoT and help resolve challenges we see in IoT.

*(6) Supply chain management, logistics and blockchain*

From manufacturing or even the design of a product to purchasing it in a retail store or online is a long process.

By tracing and recording all manually and automated transactions, again endless applications arise, for example in respects to where the product was made. With respects to the utilization of blockchain in supply chain management, logistics, transportation and so forth, several existed project come into our sight.

If there is one chief section of global business where there is a high amount of transactions, an ecosystem with many participants (certainly in cross-border trade) and still a high reliance on paper “in a fast evolving and highly interconnected ecosystem it’s everything related to end-to-end supply chains”.

Therefore, based on IDC’s blockchain spending predictions, it is not surprising that blockchain spending is leveraged to be the most tremendous in the distribution and services sector on a global level.

With blockchain, logistics and the various stakeholders in transactions, most people are actually have full understanding of connected supply chain ecosystem where speed and accuracy matter more than ever before. It depends on the supply chain, ranging from outbound logistics and all the way (with several forms of transportation) to distribution or export with even more intermediaries, forms of transportation, freight forwarders, container shipping, import and inbound logistics.

For the sake of really function we need to have blockchains enclosing all these stakeholders and the many others we left out of this streamlined ecosystem picture, or definitely and at the very least in a global supply chain context interoperability would be key as stakeholders like customs, to to name just one also have their systems.

In the past few years we've seen blockchain supply chain, logistics and transportation efforts and consortiums showed up, sometimes with a more global cross-border shipping concentration and sometimes with a more specific concentration such as container release and cargo flows in ports or dispute resolution in logistics.

While these efforts are coming in realization, existing initiatives also declare new members. These also include e-commerce giants. In February 2018, for instance, Chinese retailer JD.com which is preparing to compete with Amazon in Europe and opened offices in Australia in 2018, all part of a primary international push, joined BiTA (Blockchain in Transport Alliance) that has been declaring new members since the beginning of 2018 at an stunning percentage.

A major declaration based on the background of global trade and supply chain digitization blockchain, are related to the beginning of a joint venture between container shipping giant Maersk and IBM at the end of January 2018.

IBM and Maersk launched their cooperation in the Summer of 2016 and have been concentrated on blockchain possibilities for quite some time now. A couple of companies, ports and authorities have carried on pilots with the platform and several more are planning to participate in.

Blockchain initiatives are also realize on a perhaps what less encompassing scale. However, it goes beyond the original designed goals which resolves specific authentic challenges and then moves forward to more applications and blockchain use cases in a specific logistics context. A fitted example is blockchain smart case in the port of Antwerp where real challenges in the range of maritime logistics and especially container release are dealt with.

Moving a container from one point to another is not easy, which usually involves over 30 different parties, with an average of 200 interactions between them. Traditional channels and information carriers, like fax and paper are utilized in these interactions and transactions. Paperwork is estimated to account for up to half of the cost of container transport. In order to secure container release, cross-border shipping cases and tamper-free smart contract cases or transportation document/data flows, broad improvements are possible to make supply chains smarter, more secure, faster and more efficient across use cases ranging from customs declarations and marine insurance.

**Current Applications of Blockchain II by Fangzhao Liu**

Blockchain is popular and it is still in the early stage now, but some ambitious companies already grab the chance to develop enterprise-grade solutions for the technology. For the developer, it is good that there are already variety of enterprise blockchain platforms can be used in the market. There are so much more companies has blockchain service, and here are the details of some major providers in the market.

*Amazon Web Services*

Amazon has the largest and the most reliable global facilities for building end-to-end blockchain platforms. Amazon Web Services has its own cloud service which allows customers to use AWS Blockchain Templates to run blockchain networks on it. Ethereum and Hyperledger Fabric are for customers to choose, both of them are open-source blockchain frameworks. Kaleido Blockchain Platform is also available in the AWS Marketplace, and Solution providers can also exploit it to develop projects.

*BigchainDB*

BigchainDB is a company from Berlin. Rather than attempt to improve blockchain technology, BigchainDB starts with a big data distributed database and then adds blockchain

characteristics - decentralized control, immutability and the transfer of digital assets. The company also has a production support department and hands-on consulting to help customers.

*Hewlett Packard Enterprise*

Hewlett Packard Enterprise's key competitive power is Mission Critical Distributed Ledger Technology. Based on this technology, it promises that customers can run "workloads in environments that demand 100 percent fault tolerance at mission-critical levels". The company also provides advisory, professional and operational services for blockchain design and implementation needs (Martin).

*IBM*

IBM provides a complete blockchain platform for IBM Cloud. It attempts to attract customers form AWS. The advantage of IBM's platform is that it can use sophisticated technology to slash activation time by two-thirds. The platform also includes Hyperledger Composer, a set of collaboration, open-source tools that make it easy and faster for developers to make proof-of-concepts, and Hyperledger Fabric, an open-source framework for developers to build scalable blockchain networks.

*Microsoft*

Microsoft Azure is the pioneer to bring blockchain to the cloud. Microsoft Azure Blockchain Workbench aims to simplify development and provide partners make blockchain projects on the company's Azure cloud service. Third-party applications are also authorized to access on Azure Marketplace, such as Ethereum and Hyperledger Fabric.

*Oracle*

Not only database, but Oracle also offers Blockchain Cloud Service, which is part of the company's Platform-as-a-Service offerings. Based on the service, it good for the short-term

learning curve and large scalability of network participants, and these participants are protected by Oracle Identity Cloud Service. The service also integrates with Oracle's other offerings, including ERP Cloud and Supply Chain Management Cloud. It can accelerate transactions across entire ecosystem with the power of blockchain.

*SAP*

SAP's Platform Blockchain Service is part of the company's Leonardo portfolio. The service provides an easy way to build, create and experiment on blockchain networks for customers. Developers can build blockchain extensions for existing applications. The service integrates with SAP's Internet of Things and machine-learning offerings with blockchain capabilities which is a good attractiveness.

# Works Cited

An Introduction to Blockchain by Deep Chokshi

"How Blockchain Technology Works. Guide for Beginners." *Cointelegraph*, Cointelegraph, cointelegraph.com/bitcoin-for-beginners/how-blockchain-technology-works-guide-for-beginners.

Kharpal, Arjun. "Everything You Need to Know about the Blockchain." *CNBC*, CNBC, 29 June 2018, www.cnbc.com/2018/06/18/blockchain-what-is-it-and-how-does-it-work.html.

Strengths of Blockchain Technology by Yuanjin Zhao

Anderson, Kelsie. "The Benefits of Blockchain for IT, Part 2: Cybersecurity." *The 11 Most Popular Hotel Management Software Solutions for Small Hotels Compared Comments*, June 2018, blog.capterra.com/benefits-of-blockchain-cybersecurity/.

Horbenko, Yuliia. "Using Blockchain Technology to Boost Cyber Security." *SteeKiwi*, 2018, steelkiwi.com/blog/using-blockchain-technology-to-boost-cybersecurity/.

"Impact of Blockchain on Cybersecurity." *Worldcore Blog*, 6 May 2018, worldcore.eu/blog/impact-blockchain-cybersecurity/.

Weaknesses of Blockchain Technology by Miao Hong

Marr, Bernard. "The 5 Big Problems With Blockchain Everyone Should Be Aware Of." *Forbes*, Forbes Magazine, 20 Mar. 2018,

www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/#4101e2861670.

Current Applications of Blockchain I by Wei Chen

"Blockchain Technology: Digital Trust and Distributed Ledger Technology (DLT) in Business." *i-SCOOP*, www.i-scoop.eu/blockchain-distributed-ledger-technology/.

"How Blockchain Can Bring Greater Value to Procure-to-Pay Processes." *Accenture.com*, 2016, www.accenture.com/t20170103T200504Z__w__/us-en/_acnmedia/PDF-37/Accenture-How-Blockchain-Can-Bring-Greater-Value-Procure-to-Pay.pdf.

"How Blockchain Will Simplify and Transform Blockchain." *Accenture.com*, 2018, www.accenture.com/t20180214T053948Z__w__/us-en/_acnmedia/PDF-71/Accenture-Blockchain-For-Supply-Chain.pdf.

"An Introduction to Blockchain, and What It Means for Retail's Future." *NPD Group*, www.npd.com/wps/portal/npd/us/news/thought-leadership/2018/an-introduction-to-blockchain-and-what-it-means-for-retails-future/.

Current Applications of Blockchain II by Fangzhou Liu

"Blockchain Cloud Service." *Platform as a Service | Oracle Cloud*, cloud.oracle.com/blockchain.

"Features & Use Cases of BigchainDB." *BigchainDB*, www.bigchaindb.com/features/.

Martin, Dylan. "8 Hot Blockchain Vendors Solution Providers Should Check Out." *CRN*,

www.crn.com/slide-shows/internet-of-things/300104876/8-hot-blockchain-vendors-solution-providers-should-check-out.htm/1.