HOW BLOCKCHAIN WILL CHANGE THE ECONOMY

Peyton McGinnis

Freshman English

Mr. Twitch

24 May 2017

Peyton McGinnis
Mr. Twitch
Freshman English
24 May 2017

How Blockchain will Change the Economy

Thesis: Blockchain is the newest revolution in cyber security and will fundamentally change how the economy functions.

I. The main security attribute of Blockchain is its distributed ledger.
   A. No one person controls transactions.
   B. The ledger is replicated amongst many other systems in the specific Blockchain group.
   C. When one ledger is updated, every other copy is instantaneously updated.

II. Smart contracts allow for automatic transactions
   A. Met negotiations between two parties can auto-execute a contract, triggering a transaction.
   B. These contracts can be programmed accordingly to the requirements of the negotiation through different programming platforms built on top of Blockchain.

III. Blockchain does not require a third party or intermediary to verify transactions.
   A. Records of past transactions are entered into all ledger copies, allowing for automatic verification and auditing programmatically.
   B. The elimination of these mediators would allow for transaction reversals, no extra fees upon transactions, and faster transactions.

Peyton McGinnis

Freshmen English

Mr. Twitch

24 May 2017

How Blockchain will Change the Economy

Since the introduction of TCP/IP as the protocol for the Internet, the world has changed in many ways, one of which is digital currency. Digital currency allows the storing of money as computerized information, and the ability to send money to other people on the Internet. But since this revolution in the industry of finance, many “hacks” have been formed to exploit applications storing the currency, granting the “hackers” free money. “The 2017 Identity Fraud Study, released by Javelin Study & Research, found that $16 billion was stolen from 15.4 million U.S. consumers in 2016” (Information 1). Different preventions for cyber theft have been developed; one example is encryption algorithms. “Encryption algorithms” are computer programs that change a value into a secure configuration that can only be decoded if the user knows the “key” that “decrypts” it (Shelton 2). Various algorithms have been developed, such as RSA and AES encryption, but these algorithms do not always prove themselves to be foolproof, as none truly is. But a new technology has come about that has reached a point of perfection in security closer than any other application: Blockchain.

Blockchain’s security comes from its distributed ledger. A “distributed ledger” is where transaction records and information can be accessed by any user connected to a blockchain

(Iansiti 2). A “blockchain” is every transaction “between two parties” that is stored on a shared database (2). Every system on the blockchain has a copy of the ledger (PSCU 4). All copies of the ledger on a blockchain are updated with the new transaction information when a transaction is performed (Iansiti 7). Transaction information is stored as a “block” (Mazonka 3). A “block” is an encrypted hash containing transaction information (1). Once a new block is pushed to the blockchain, it cannot be changed or removed (Iansiti 7). This raises the question of, “is pushing fake blocks into the ledger to gain profit possible?” The answer is no. Blockchain’s software has algorithms to prevent the entering of “counterfeit” blocks into the global blockchain group (PSCU 4). Whenever a transaction is made, it is also verified against every other ledger in the group, allowing another layer of prevention for common issues such as double spending (Nakamoto 1). Blockchain ledgers are also transparent to connected systems (Iansiti 2). This allows easier verification and the ability for anyone to view past transactions and information for different uses (Satyavolu 6).

Blockchain environments can be set up to either be open to any user or to a closed group that grants access to the ledger. In open groups, any user can join the blockchain (PSCU 5). Bitcoin, a purely digital currency that runs off of Blockchain, is the best example of an open group; it does not have a central server that a user connects to in order to perform a transaction (5). This allows person-to-person payments to be made with little resistance (Nakamoto 1). However, one can also set up a “permissioned” Bitcoin ledger (McMeekin 2). In closed group or “permissioned” blockchains, users can only join if they have been granted access by an administrator or other member of the blockchain (PSCU 5). Organizations can

implement a private blockchain within the company, or with external entities for transactions and communication (Iansiti 10).

"Smart contracts" have the power to be one of the most applicable utilizations of blockchain technology. Smart contracts "automate payments and the transfer of currency or other assets as negotiated conditions are met" (12). Organizations can set agreements between each other for what business they are conducting and program the agreement into the contract. This program cannot be edited by either party once it is sent (Satyavolu 4). When the agreement is met, the program can verify it and make a transaction using the blockchain both organizations are connected to. Because smart contracts offer great flexibility and customizability, "programmable ledgers" have the power to reach all sorts of corporations' needs (Iansiti 2).

Different software platforms have been designed to allow programming on top of blockchain for contracts, such as Ethereum (PSCU 11). Ethereum is "a permission-less blockchain-based digital currency that comes with a full programming language" (11). Ethereum's programming language is called Solidity, but you can also use more common languages such as C++, Python, Rust, and Go to program Ethereum applications. Because both blockchain and Ethereum are purely software, they can be programmed to fit the needs of users and organizations alike to automate negotiations (Iansiti 12).

Blockchain technology could change the position of financial mediators such as banks and credit unions (12). Transactions involving digital currency almost always go through an intermediary (Nakamoto 1). They exist so that transactions can be handled without disputes

and to prevent hacks such as double-spending (1). The issue arises when one actually considers what banks and credit unions do: they are responsible for storing *your* assets, and they do not let the actual holders of the assets perform their own transactions (Mazonka 1). If asset-storing changed, asset-holders would be able to store their money on their own system (1). This results in a few significant changes. First, some banks put fees on transactions, credit and debit cards, and holding a checking account for using their services (Nakamoto 1). "The cost of mediation increases transaction costs, limiting the minimal practical transaction size and cutting off the possibility for smaller transactions" (1). Another reason is that person-to-person payments would also result in faster transactions. Blockchain allows transactions to be made directly over the Internet between two people. "There is no need for third-party intermediaries to verify or transfer ownership" (Iansiti 7). Both of these conditions present a single conclusion to transaction processing: automation (PSCU 13). Human intervention in some transactions to verify transfers would no longer be necessary; algorithms and software could verify transactions (Iansiti 3). Even "audit functions may be largely automated and self-reporting" (PSCU 13). Higher-performing blockchain based business models could overtake older archetypes of financial institutions (Libert 5).

Blockchain has brought a transformation in the realm of security and financial automation. With all of these automations in the financial industry that would not have been possible before, it brings about many changes that will affect the worldwide economy. Recently, the city of Dubai announced that a "city-wide effort" would be done to implement Blockchain into its economy (Lohade 1). We are already seeing effects of this technology

around the world. “It is only a matter of time before the broader financial services and banking industries shift to blockchain and network-based approaches” (Libert 4).

Works Cited

Department of Justice. Cybercrime against Businesses, 2005. Washington: GPO, 10 Oct 2008. Accessed Online. Date Accessed 19 Apr 2017.

Iansiti, Marco and Karim R. Lakhani. "The Truth about Blockchain." Harvard Business Review. Jan 2017: n. pag. Print. Date Accessed 19 Apr 2017.

Insurance Information Institute. "Identity Theft and Cybercrime." 2017. Date Accessed 19 Apr 2017.

Internet Crime Complaint Center. 2013 Internet Crime Report. Washington: GPO, 2013. Accessed Online. Date Accessed 19 Apr 2017.

Mazonka, Oleg. "Blockchain: Simple Explanation." (n.d.): n. pag. 2016. Web. Date Accessed 19 Apr 2017.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Web. Date Accessed 19 Apr 2017.

PSCU. "Blockchain and the Credit Union: The Asset Transfer Revolution." 2016. Date Accessed 19 Apr 2017.

RSA. "2016: Current State of Cybercrime." 2016. Date Accessed 19 Apr 2017.

SecurityScorecard. "2016 Financial Industry Cybersecurity Report." 2016. Date Accessed 19 Apr 2017.

Shelton, Barry K. "Introduction to Cryptography." Information Security Today. Internet. Date Accessed 19 Apr 2017.

Lohade, Nikhil. "Dubai Aims to Be a City Built on Blockchain." The Wall Street Journal. 25 Apr 2017: n. pag. Print. Date Accessed 21 May 2017.

McMeekin, Paul. "How the Blockchain Will Disrupt Banking." CFO. 5 May 2016: Internet. Date Accessed 21 May 2017. http://ww2.cfo.com/applications/2016/05/blockchain-will-disrupt-banking/

Libert, Barry and Megan Beck and Jerry Wind. "How Blockchain Technology Will Disrupt Financial Services Firms." Knowledge@Wharton. 24 May 2016: Internet. Date Accessed 21 May 2017. "http://knowledge.wharton.upenn.edu/article/blockchain-technology-will-disrupt-financial-services-firms/"