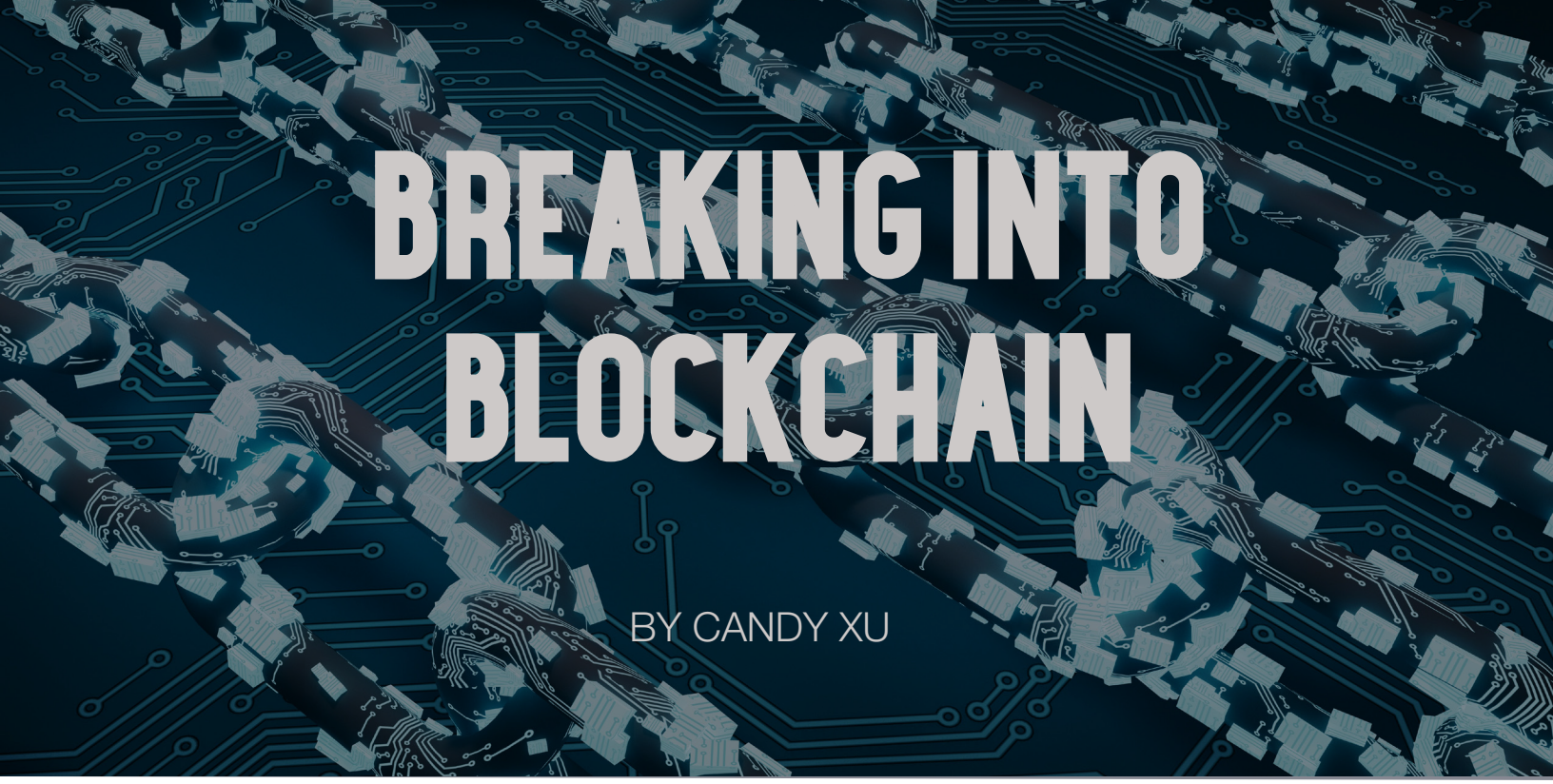

BREAKING INTO BLOCKCHAIN

BY CANDY XU

On May 12, 2017, at roughly 12:30 p.m. British Summer Time, England's National Health Service (NHS) was invaded by WannaCry, a ransomware attack. To this day, this cyberattack remains the largest one affecting the NHS.[1,2] An estimate of nearly 20,000 patient appointments were cancelled, and 595 general practices were infected.[2] Soon, news about this attack raced to headlines, and with it, so did Bitcoin, a relatively new type of currency. The attackers had encrypted computer files, making them unreadable to human users, and proceeded to demand 300 dollars worth of bitcoins for decrypting each computer. This demand for an exchange through Bitcoin brought the seemingly mysterious cryptocurrency to the foreground of the public sphere.

BITCOIN AND BLOCKCHAIN

Bitcoin is a type of decentralized digital currency first introduced in Satoshi Nakamoto's white paper in 2008.[3] Unlike physical currencies, digital currencies are available in electronic form and can be exchanged around the world. The growing popularity of Bitcoin has brought with it a new interest in the technology supporting it, namely blockchain. Blockchain, introduced as the backbone of the Bitcoin system in Nakamoto's white paper, had been in existence far before the advent of Bitcoin.[3] Many of Bitcoin's features such as the security and transparency of its transactions largely come from blockchain's characteristics.

Blockchain is a distributed database that supports transactions between participants and keeps records of all the transactions it mediates.[4] It is analogous to a paper ledger on which each party can record their activities using a permanent pen; users document their own independent transactions, and everyone comes to consensus based on these records. These qualities exemplify blockchain's data integrity and transparency, since no one can alter the data in the chain, and all activities through a blockchain are publicly visible.[5] Blockchains are also known for being formidably secure. Since each new block consists of the hash of the previous block, if an attacker were to mutate a published block, all blocks after it would be malformed (Fig. 1). Malicious activity will thus be immediately noticed, contributing to the tamper-evident nature of the blockchain system.

However, no system is perfectly secure, and blockchain is not an exception. Attackers have been finding ways to break this system and have indeed been successful in many cases. The DAO, a decentralized autonomous company operating blockchain-based smart contracts, was hacked and lost 50 million dollars to an unknown attacker in June 2016.[6] Bitfnex, an exchange platform in Hong Kong, also lost 72 million dollars worth of bitcoins in a similar attack two months later.[6]

"Unlike physical currencies, digital currrencies are available in electronic form and can be exchanged around the world. Blockchain, introduced as the backbone of the Bitcoin system in Nakamoto's white paper, had been in existence far before the advent of Bitcoin."

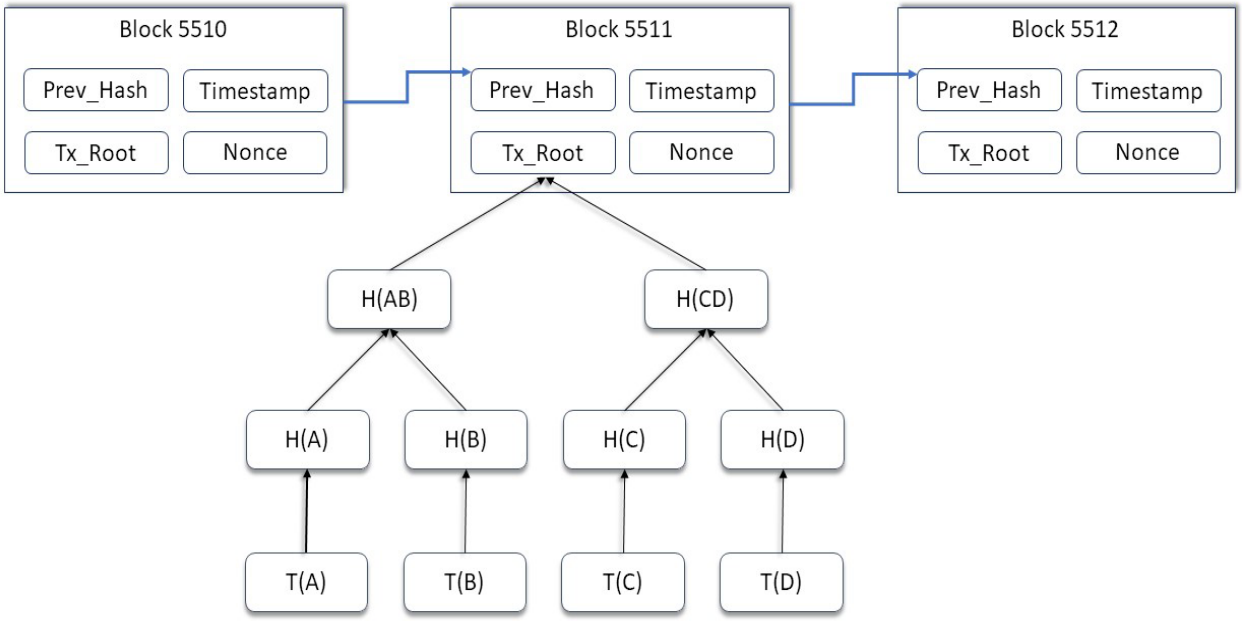

Figure 1: Block header. *Hash functions map any input to an output of fixed length.[11] Due to their special mathematical characteristics, hashing algorithms, such as SHA-256, became brilliant choices for preserving data integrity. Each block in the blockchain contains a hash value of the previous block. If one block is mutated, all the rest will be affected: hash outputs will be changed, effects easily noticed by anyone using the hashing function.*

ATTACK ON THE USER

A pair of public and private keys are vital for every Bitcoin user. When registering for an account, each party gets a private key, and this private key is in turn used to generate a public key through a hashing algorithm. The public key acts as the account name, and the private key acts as the password.[7] Since blockchains are anonymous, these keys are the only identification for each account. Thus, if a user loses their private key, everything in the corresponding account will become effectively inaccessible.

Naturally, attackers often try to obtain a user's private key in order to transfer the user's Bitcoin back to themselves. There are a lot of different methods of storing one's private key, and most of them involve using a digital wallet. Similar to a physical wallet that stores cash, a digital wallet stores public and private keys and can keep track of the current balance in certain accounts. Some of the wallets can also perform transactions and manage assets for the users. These are called "hot wallets," because they require Internet access.[8] They are also one of the primary targets for hackers because there are a lot of existing ways to attack Internet-connected applications. For example, verification of end-users often occurs in a single server. This linear architecture makes the system more vulnerable to spoofing attacks.[9]

In order to combat this type of attack, people have started to use "cold wallets," wallets that do not require an Internet connection.[8] For instance, some users have created QR codes of their private key and printed them on paper (Fig. 2). Others have opted to simply store their key on a hard drive. Nonetheless, it is still possible for attackers to steal cold wallets either physically or by hacking into computers.

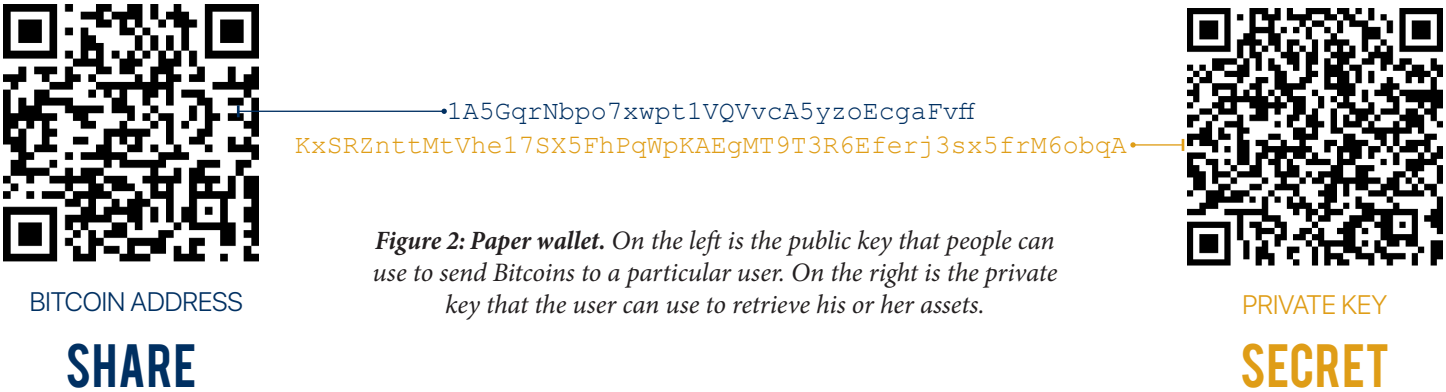

Figure 2: Paper wallet. *On the left is the public key that people can use to send Bitcoins to a particular user. On the right is the private key that the user can use to retrieve his or her assets.*

ATTACK ON THE CHAIN

Hackers can also directly attack the blockchain itself. One of the most famous attacks considered remarkably dangerous is the 51% attack.[10] This attack occurs during the validation of blocks when Bitcoin's blockchain system accepts the longest chain as the valid one. Mining blocks typically requires a large amount of computing power because the mining algorithms are computationally difficult (Fig. 3). It is thus possible for a particular group who owns more than 50% of the computing power to seize control of the flow of blocks.[10] They can do so by utilizing their excessive computing power to outperform all other algorithms and create the longest chain with their set of desired blocks. Once published, this chain will be accepted by the system and effectively rewrite the blockchain's history.

Besides the famous 51% attack, there have been a multitude of additional means for hacking, including the race attack, feather forking, and the eclipse attack among others. In an eclipse attack, attackers take advantage of blockchains' need to compare information with each other by taking control of a singular node and then using it to mislead the activity of other nodes. By doing so, the attacker is able to mislead other nodes into accepting false transactions or waste computing power on unnecessary comparisons.[8] However, these kinds of smaller attacks are generally considered less harmful than 51% attacks, since their scale of influence is not as large.

Although it has some vulnerabilities, blockchain remains a very secure system compared to other systems. It can be used not only for cryptocurrencies, but also for a number of other kinds of digital products. For example, Ethereum is a blockchain-based application platform that features smart contracts, while CryptoKitties is an Ethereum-based game in which players can purchase virtual cats. The development of blockchain's usage might still be in its infancy, yet these current early stages are proving to be an exciting time for people to learn about this new technology while simultaneously becoming the pioneers who push its boundaries.

Acknowlegements: I would like to express my sincere appreciation to Justin Yu for reviewing my article.

Figure 3: ASIC. *ASIC, or Application-Specific Integrated Circuit, is a type of device that is designed for the sole purpose of mining. It is currently a popular choice for miners and can perform mining algorithms more efficiently compared to other devices such as CPUs and GPUs.*

REFERENCES

1. National Audit Office. (2018). Investigation: WannaCry cyber attack and the NHS.
2. Brandom, R. (2017, May 12). UK hospitals hit with massive ransomware attack. Retrieved from https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin.
3. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
4. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation, 2*(6-10), 71.
5. Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine, 7*(2), 18-21.
6. Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, A. (2019). Exploring the attack surface of blockchain: A systematic overview. *arXiv preprint arXiv*:1904.03487.
7. Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)* (pp. 839-858). IEEE.
8. Orcutt, M. (2018, April 25). How secure is blockchain really? Retrieved from https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/
9. Yang, D., Kou, L., & Liu, A. (2017). *U.S. Patent No. 9,672,499*. Washington, DC: U.S. Patent and Trademark Office.
10. Bastiaan, M. (2015, January). Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin. Retrieved from https://pdfs.semanticscholar.org/0336/6d1fda3b24651c71ec6ce21bb88f34872e40.pdf
11. Rogaway, P., & Shrimpton, T. (2004, February). Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In *International workshop on fast software encryption* (pp. 371-388). Springer, Berlin, Heidelberg.

IMAGE REFERENCES

12. Banner: https://pixabay.com/illustrations/blockchain-block-chain-bitcoin-3750157/
13. Figure 1: https://www.flickr.com/photos/166102838@N03/30990804477
14. Figure 2: https://commons.wikimedia.org/wiki/File:A_paper_printable_Bitcoin_wallet_consisting_of_one_bitcoin_address_for_receiving_and_the_corresponding_private_key_for_spending.png
15. Figure 3: https://pixabay.com/zh/photos/farm-mining-the-ethereum-market-2852024/