AUGUST 2018

ARMOR™

REPORT

BLOCKCHAIN (R)EVOLUTION

EXPLORING THE PAST, PRESENT, AND FUTURE OF BLOCKCHAIN TECHNOLOGY

INTRODUCTION

Blockchain technology is generating a great deal of excitement as organizations consider its potential implications. Companies announcing blockchain-related initiatives have seen their stock prices spike, and the technology has ushered in talk of new levels of security, data fidelity, and an immutable digital ledger that can serve everything from supply chain data to financial transaction records.

Since its early applications in cryptocurrency, blockchain implementations have focused on keeping data secure by ensuring integrity. But the journey of blockchain technology now stretches far beyond Bitcoin. For businesses, blockchain implementations can change the game in terms of providing a secure way to store and track transactions, and they have sparked significant investment and interest, particularly in the financial services industry.

As can be expected however, the growing interest in blockchain technology has impacted both the legitimate and illicit economies. Due to its decentralized nature, cryptocurrency and the anonymity it can offer have been leveraged by cybercriminals for years. Beyond that, the growing popularity of cryptocurrency among the public has made it more than just a payment mechanism. It is now a target, as attackers are increasingly deploying cryptomining software onto computers surreptitiously to make money.

Looking ahead, innovation is certain — both for cybercriminals and corporations. In this paper, we will examine the past and present uses of blockchain technology, provide an inside look at the growing focus on cryptomining by attackers, and offer predictions of how the technology will have an impact on both the corporate world and the underworld.

THE PAST

BLOCKCHAIN 101

Let's start by defining exactly what blockchain technology is. Put simply, a blockchain is a digital ledger of records supported by a distributed network of computers. Each block typically has a cryptographic hash of the previous block — or record — as well as a timestamp and transaction data. By leveraging a peer-to-peer network architecture, blockchain technologies benefit from having no centralized point of failure or vulnerability. The network uses a protocol for inter-node communication as well as for validating any new blocks.

Since every block is timestamped, hashed, and linked to the other blocks, it is extremely difficult for anyone to modify the records in the chain after they have been stored without being detected. Altering any one block would alter all subsequent blocks, which requires the agreement of the majority of the network. The rules for validating new blocks are known as consensus mechanisms and can take three forms:

- **Proof-of-work:** this model requires that cryptominers perform some sort of computational puzzle in order to publish a new block on the blockchain, and it involves significant resources and computing power.
- **Proof-of-stake:** in this approach, blocks are not mined – instead, the creator of the next block is chosen in a deterministic way, through combinations of random selection and various factors.
- **Proof-of authority:** in this model, transactions are verified and approved by accounts known as validators.

Proof-of-work and proof-of-stake models are often used in public blockchains such as bitcoin, whereas proof-of-authority is most often associated with private blockchains that require an invitation from administrators. Combined with the transparency of blockchain data, these consensus mechanisms effectively keep cybercriminals from fraudulently adding new data.

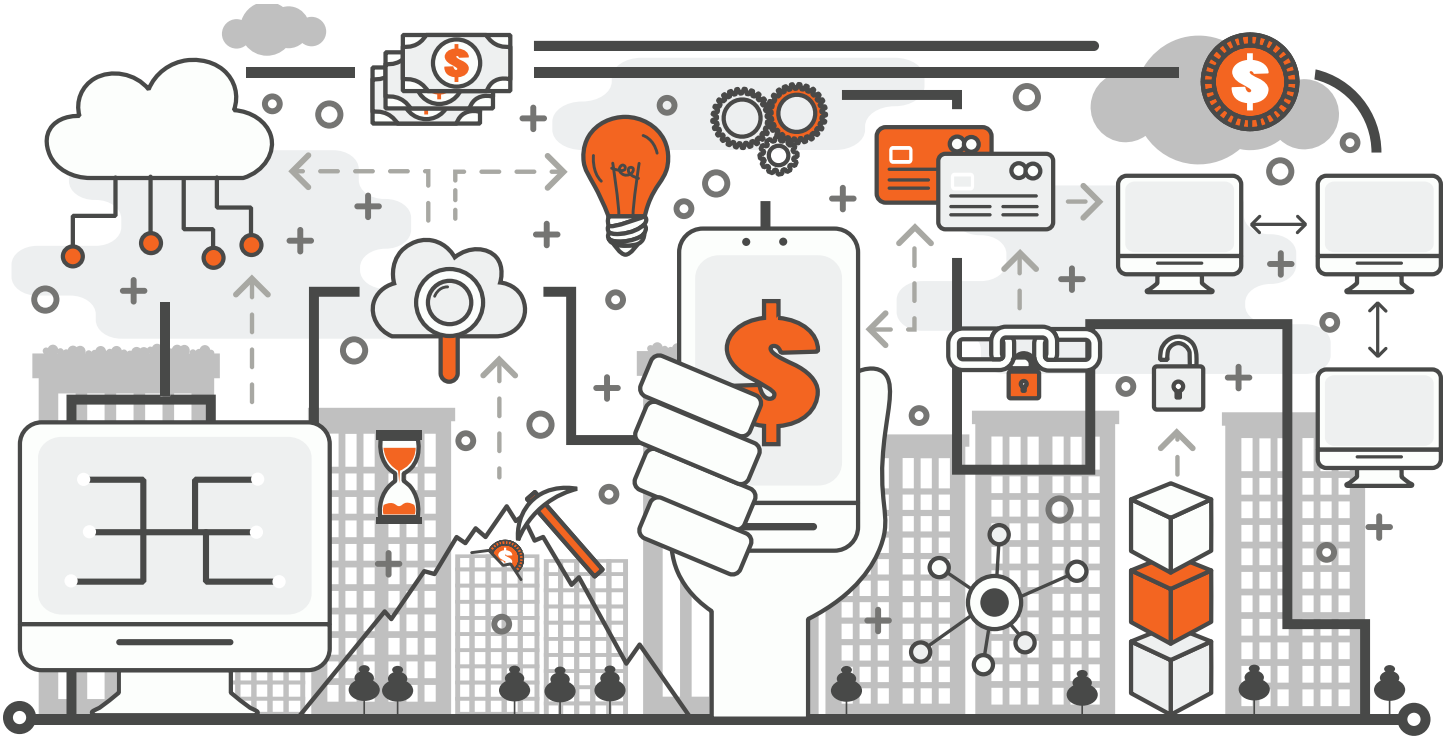
WHAT IS BLOCKCHAIN?

It is a digital ledger of records supported by a distributed network of computers. Each block typically has a cryptographic hash of the previous block – or record – as well as a timestamp and transaction data.

The origin of the blockchain is a bit of a mystery. Though early work on a cryptographically secured chain of blocks can be traced back to research published in 1991 by Stuart Haber and W. Scott Stornetta[1] , a person or group going by the name Satoshi Nakamoto[2] is credited with making the first blockchain a reality for use as the public transaction ledger of Bitcoin. When Bitcoin was released in 2009, the technology allowed it to become the first digital currency to address the problem of double-spending — the prospect of the same digital token being used more than once — without the help of a trusted authority or central server.

As noted earlier, there is more than one type of blockchain. Public blockchains such as Bitcoin are open, allowing anyone to access and view the ledger. Additionally, anyone can validate transactions via the established consensus mechanism as well as propose new blocks for the ledger. Due to their openness, public blockchains can grow large and require a significant amount of computation power to maintain the ledger. This openness also has a potential drawback caused by a lack of privacy protecting transactions.

While public blockchains may have a governance structure, they do not have a central authority. However, public blockchains do. Also called permissioned blockchains, administrators limit who has access to the ledger and enforces the rules. In some cases, because users are operating with a higher level of trust, the consensus mechanisms of private blockchains do not require as much computing power.



BLOCKCHAIN 2.0

Because blockchain first entered the public consciousness through its association with Bitcoin, the relationship between blockchain and cryptocurrency is sometimes misunderstood. Blockchain is not cryptocurrency – it is the underlying technology that allows cryptocurrencies to work. Likewise, cryptocurrencies like Bitcoin, Monero, and others should not be confused with blockchain. They are but one example of how blockchain technology can be applied.

A few years ago, a new class of applications of blockchain technology, known collectively as Blockchain 2.0, began to emerge. This second generation of blockchain implementations enables users to create more sophisticated smart contracts. Smart contracts are computer protocols that verify, facilitate, and enforce the terms of an agreement between a buyer and seller. Use of more sophisticated smart contracts opens the door for more uses of blockchain technology for businesses, such as automating actions like creating and paying invoices that may normally be performed by a third-party service.

The evolution of blockchain technology also led to increased development of decentralized applications (DApps). DApps are applications that are run by many users on a decentralized network with trustless protocols. They typically reward users with a token for providing computing power and are designed to avoid any single point of failure. DApps use smart contracts to execute commands on a blockchain and allow for more complex uses of the technology.

CYBERCRIMINALS EMBRACE CRYPTOCURRENCIES

Developers in the legitimate world innovated; the world of cybercrime began to pay attention. It should come as no surprise that cryptocurrencies would be used on the black market to pay for goods and services — or, in the case of ransomware, as a way for victims to pay to retrieve access to their data. When Bitcoin first appeared, the anonymity it provided senders and receivers made it perfect for them to profit from their activities and stay undetected. This trend has continued, as new currencies, which place greater emphasis on user privacy, have emerged. Privacy-centric currencies such as Monero became another primary method of payment for more security-conscious attackers.

The ability to receive payments with reduced risk, resulted in an uptick in both ransomware attacks as well as DDoS attacks with ransom demands attached. In 2014 for example, a group called DD4BC hit targets around the world with threats of DDoS attacks if a ransom was not paid in Bitcoin. Another group known as the Armada Collective appeared in 2015 and during the past few years have targeted organizations throughout the world.[3]

Over time, attackers have surpassed looking at cryptocurrency as a payment mechanism. Today, attackers are pursuing cryptomining, targeting initial coin offerings by companies looking to raise capital, and even using blockchain domains for infrastructure.

THE PRESENT

DEVELOPMENT BOOM

Today, both the world of cybercrime and the legitimate economy are responding to some of the promises blockchains offer. According to estimates from Gartner, the business value-add of blockchain technology will grow to more than $176 billion by 2025 and exceed $3.1 trillion by 2030.[4]

According to advisory firm Deloitte, the blockchain's ecosystem is growing, with the development of new platforms, applications, and partnerships increasing. Many companies are collaborating with blockchain start-ups, and many are opting to join consortiums such as Enterprise Ethereum Alliance and R3 that support the development of decentralized business platforms and applications.[5]

Though the explosion of cryptocurrencies has put the focus on developing uses for blockchain technology in the financial services industry, the potential applications go much further. Companies like IBM and others have emerged with solutions dealing with everything from supply chain management to managing authoritative music copyright information using blockchain technology.

With each successful use case, the potential of an immutable, secure digital ledger of data becomes clearer. The Brave Browser, for example, touts itself as a privacy-oriented browser that plans to offer users the chance to opt in to a blockchain-based digital advertising platform. According to the company, users will be able to use the Basic Attention Token, a utility token based on the Ethereum technology, as a unit of account between advertisers, publishers, and users on the platform.

According to estimates from Gartner, the business value-add of blockchain technology will grow to more than **$176 billion by 2025 and exceed $3.1 trillion by 2030**

Development of blockchain technologies beyond the realm of cryptocurrency is at an inflection point, and it remains to be seen which applications will take hold and prove valuable to businesses.

For organizations considering blockchain-backed solutions, it is important to remember that traditional relational databases can provide similar (though not identical) functionality. While deciding, think about:

1. Consider whether the disintermediation of third parties is a primary benefit that you are chasing. For cryptocurrencies, the ability to facilitate payment without the need of a third party to clear the transaction is a clear benefit of the blockchain. For many organizations there may not be a need to remove a third-party from the equation.

2. The number of business-ready applications is still relatively small. For many organizations, this means that a blockchain based solution may require internal development and support. This will, in many cases, mean that the use of traditional relational databases with strict security controls and replications/backup configurations is a more cost-effective and tested solution.

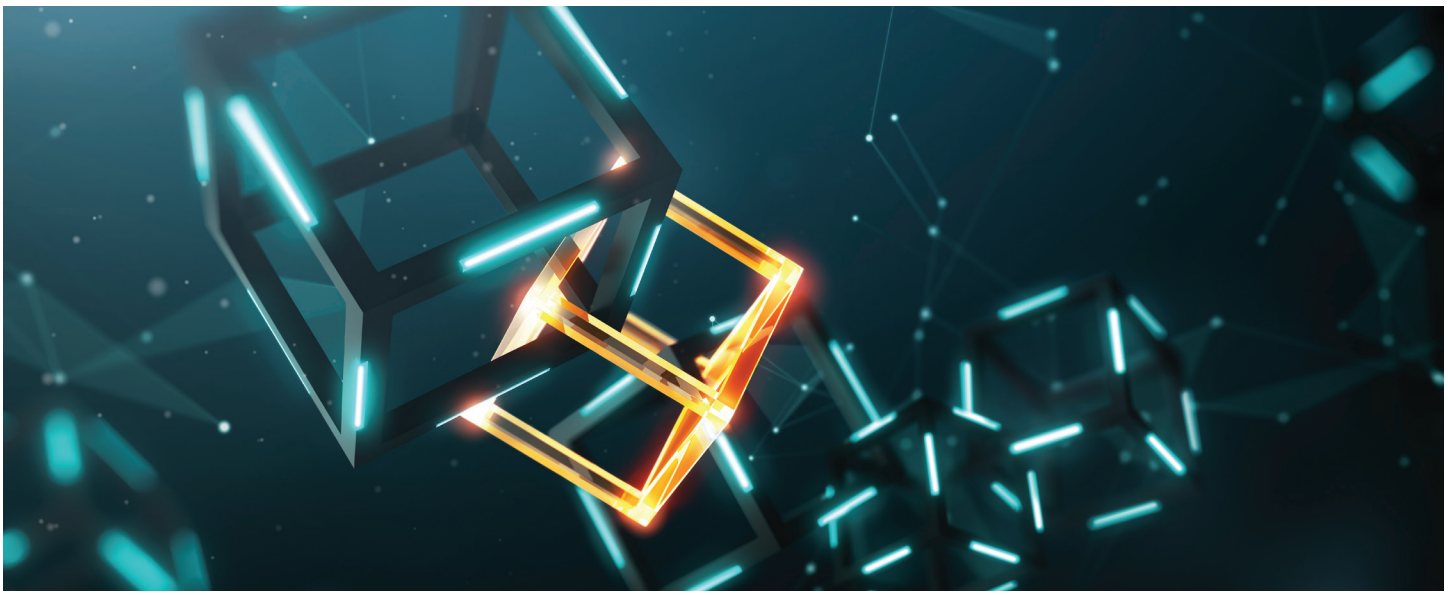
3. How important is fault tolerance? While organizations can achieve relatively good fault tolerance with traditional relational databases, blockchain-based solutions are better. If this is your primary concern, then a blockchain-based solution may make sense (but remember point 2).

4. What about data confidentiality? If confidentiality is important, then using a private blockchain is preferable to a public one.

5. Lastly, traditional relational databases will likely have better performance than any blockchain-based solution. Therefore, if speed/performance is key, current blockchain solutions may not cut it.

Meanwhile, the number of cryptocurrencies is exploding. According to some estimates, there are more than 1,600 cryptocurrencies as of this writing.[6]

Bitcoin started it all, but a number of other cryptocurrencies have emerged. Some of these currencies, such as Monero, Dash, and Zcash have sought to distinguish themselves from Bitcoin with additional layers of privacy for users. For example, with Bitcoin, if an identity is ever connected to a wallet address, the entire history of the person's transactions can



be uncovered. This leads privacy-conscious users to have more than one wallet address to mask their transaction history. Monero, however, solves this problem by keeping wallet and transaction information totally private.

"Even if someone knew about specific anonymous funds that you control, they cannot tell if or when you spend those funds," Monero explains on its website. "They cannot tell whom you've sent those funds to, because it will look to the world as if people may be using your funds in their own transactions all the time. (This is achieved through a cryptographic mechanism called a ring signature)."[6]

FROM MONEY LAUNDERING TO MINING

This increased emphasis on privacy has also attracted some bad actors. Armor's Threat Resistance Unit (TRU) has noticed more attackers abandoning Bitcoin in favor of currencies like Monero. An example of this can be found in the WannaCry ransomware attacks of 2017. According to media reports, the criminals behind the malware converted their profits from Bitcoin to Monero as they attempted to cash out.[7] In order to do this, they took advantage of Bitcoin exchange ShapeShift to launder their proceeds. More of this activity will happen in the future as cybercriminals and others look to hide their transactions.

Currently, there have been a number of arrests linked to exchanges laundering money. For example, in April 2018, Europol announced that it had arrested 11 people and identified 137 suspects potentially involved in a criminal network using cryptocurrencies and credit cards to launder money from illegal drug sales.[8] In another case, an Arizona man operating a peer-to-peer Bitcoin exchange business was convicted in March 2018 of laundering more than $164,000 for undercover federal agents.[9]

The popularity of cryptocurrency has impacted the illicit economy in another way – the growth in cryptojacking. Cryptojacking occurs when someone gains access to someone else's system and uses its resources to mine cryptocurrency. For example, in January 2018, researchers at Proofpoint noted the growth of the Smominru botnet, a cryptomining operation that is estimated to have made millions of dollars.[10] In another notable example, hackers compromised the cloud environment of car manufacturer Tesla as part of a cryptojacking operation.[11]

During a 45 day-period in 2018 (April 25 – June 8), Armor recorded 70 signature-based anti-malware events related to cryptomining malware across 4 customers. Roughly 50% of these events were determined to be Drupalgeddon 2 and 3 related and 50% were ApacheStruts2 related. The event-to-target ratio of these events indicates the attacks were likely automated.

45 DAY-PERIOD IN 2018

(April 25 – June 8)

- **Armor** recorded 70 signature-based anti-malware events related to **cryptomining malware** across 4 customers
- Roughly **50%** of these events were determined to be **Drupalgeddon 2** and **3** related and **50%** were **ApacheStruts2** related
- The event-to-target ratio of these events indicates the **attacks** were likely **automated**

Armor analysts discovered IP addresses associated with Monero, Electroneum, and Ubq mining pools coded into the malware samples. Additionally, Drupalgeddon2 indicators of compromise (IoC), Apache Struts2 IoCs, and malware domains were detected via network monitoring. The geolocation of repositories hosting cryptomining malware, mining pools, and other associated malware downloads were globally distributed. While there is insufficient evidence to attribute the activity to any specific threat actor or botnet, it was observed that a majority of the IP-based indicators are associated with regional internet registries in Eastern Europe, namely Romania.

In each case, the events that have included cryptomining malware have been determined by Armor analysts to be the result of unpatched web application vulnerabilities. Known, targeted customers include the healthcare, materials (metals and mining), financial, and information technology industries as well as non-profits. Outside the vulnerable applications, no trends or anomalies have been observed that would indicate that a particular vertical is being targeted. However, the attacks highlight the importance of patching vulnerable applications. In addition, organizations may want to consider working with security vendors to block the IP addresses of mining pools.

10-20
ACTIVE MINERS

Coinhive notes that 10-20 active miners on a website can turn a monthly profit of **0.3 XMR — or $97** *(as of February 22, 2018)*. An army of zombified systems translates to more illicit payouts.

A scan of the headlines reveals other tactics as well. Drive-by downloads are another means of attack used to compromise computers. A number of security firms have reported incidents of the cryptocurrency mining service Coinhive being placed on compromised websites in order to hijack the computers of anyone visiting the sites.

"Just like how ransomware matured, we're starting to see the use of notorious exploits and methods for deploying fileless malware to install miners," explains Trend Micro. "Coinhive notes, for instance, that 10-20 active miners on a website can turn a monthly profit of 0.3 XMR — or $97 (as of February 22, 2018). An army of zombified systems translates to more illicit payouts. A cryptocurrency-mining malware we found last year, which exploited EternalBlue for propagation and abused Windows Management Instrumentation (WMI) for persistence, is an example of this."[12]

What is clear is that hackers are increasingly interested in pursuing cryptocurrency as a target as opposed to using it just as a means of payment. By way of example, in December 2017, attackers hit NiceHash, a cryptocurrency cloud mining marketplace and reportedly stole tens of millions of dollars in Bitcoin.[13] In April 2018, attackers were able to temporarily redirect visitors to MyEtherWallet.com (MEW) to a phishing site and steal money.[14]

Even initial coin offerings (ICOs) are being targeted. According to a December 2017 report by consultancy Ernst & Young, phishing is the most common form of funds theft during ICOs and hackers steal up to $1.5 million in ICO proceeds per month. Scammers either request a funds transfer to their wallet or steal private keys to investors' wallets.

FUTURE

LOOKING TO THE FUTURE

It is fair, given the history of technological evolution, to expect the development of legitimate and illegitimate uses of blockchain technology to continue to grow in parallel. So where does all this leave us? Already, reports have emerged of cybercriminals beginning to use blockchain domains for infrastructure. Researchers at FireEye, for example, noted several examples of this in recent research, citing situations where malware was configured to use .bit domains.[16] Meanwhile, blockchain technology offers a number of attractive potential use cases that can bolster cybersecurity and improve data management. With this in mind, here are some predictions Armor has for the future.

Attackers Take Advantage of Emerging Blockchain Solutions: Just as attackers have been quick to leverage blockchain-based cryptocurrencies, there is a whole generation of potential technologies on the horizon that are enabled by some of the same foundational blockchain concepts that have enabled cryptocurrencies to date. One example of a new technology that is the result of synergy between blockchain concepts and other battle-tested technologies is the InterPlanetary File System (or IPFS) concept, which is a distributed file system that enables the creation of completely distributed applications. As adoption of this technology increases, it is likely there will be threat actors who find ways to leverage this technology for command and control or data exfiltration.

Improved Authentication Services: Using a distributed public key infrastructure for device/user authentication where management of certificate data is carried out on the blockchain represents an opportunity for businesses to eliminate passwords. However, there is a challenge ensuring the identity information entered into a blockchain is accurate and vetted, since it is immutable. Companies such as Civic and Remme.io are already doing work in the area of identity and access management. Expect continued development of solutions around this topic.

Next-Level Data Integrity Services: Perhaps the biggest area for potential development tied to blockchain is data integrity. Efficient data integrity monitoring of large datasets can allow detection of unauthorized configuration

changes across a network to identify early indications of insider threats, threat actors, and even alert on human error. While File Integrity Monitoring has been around a long time, there are some who believe these technologies enabled by a blockchain will enable advanced data integrity capabilities.

Improved Data Management: Rather than copies of sensitive information being held by various individual companies, it could be stored on a blockchain. Then, by applying existing cryptographic principles to that, companies could be authorized to access select pieces of information as needed. This would mean that the companies would no longer need to maintain individual copies of the data, reducing the potential entry points for attack.

Attackers Look for Opportunities: As noted earlier, attackers are already taking advantage of blockchain domains for infrastructure, and that trend will continue. Namecoin allows for human-friendly .onion addresses, which makes it a great fit for threat actors that have used TOR in the past. As more and more traditional systems get blockchain/DApp equivalents, attackers can be expected to pay attention to compromising those as well. Mistakes related to key management, common coding errors, and other vulnerabilities will be exploited.

CONCLUSION

There are a number of challenges that need to be addressed before widespread enterprise adoption of blockchain technology truly begins. The first is a general knowledge factor. Many executives still don't feel they know enough about blockchain and are still figuring out how to assess the possibilities the technology presents. Even one of its greatest strengths – its relative immutability – can pose a challenge if mistakes are made during the data entry.

Before adopting blockchain-based applications, enterprises need to properly assess their readiness for the technology and whether they have a proper use case for it. Shiny object syndrome in IT can lead to aggressive adoption of new technologies, but it also introduces integration challenges and wastes time, money, and effort. But as organizations assess the technology, it is equally important for them to be on guard for cybercriminals looking to exploit it. Security remains an arms race, and where legitimate developers go, cybercriminals will not be far behind.

SOURCES CITED

1. Stuart Haber, W. Scott Stornetta, "How to time-stamp a digital document", https://link.springer.com/article/10.1007/BF00196791, January 1991.
2. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf.
3. Radware, https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/bottom-line-rdos-rises/; June 23, 2017.
4. Gartner Inc., "Forecast: Blockchain business value, worldwide, 2017–2030," March 2, 2017.
5. Deloitte, "Blockchain: A technical primer", https://www2.deloitte.com/insights/us/en/topics/emerging-technologies/blockchain-technical-primer.html, February 2018.
6. Monero, "How does Monero's privacy work?", https://www.monero.how/how-does-monero-privacy-work.
7. Forbes, "WannaCry Hackers Are Using This Swiss Company To Launder $142,000 Bitcoin Ransoms", Thomas Fox-Brewster, Aug. 3, 2017.
8. https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking
9. https://www.justice.gov/usao-az/pr/arizona-based-peer-peer-bitcoin-trader-convicted-money-laundering
10. Proofpoint, "Smominru Monero mining botnet making millions for operators", https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators, January 31, 2018.
11. RedLock, "The Cryptojacking Epidemic", https://blog.redlock.io/cryptojacking-tesla, February 20, 2018.
12. Trend Micro, "Cryptocurrency-Mining Malware: 2018's New Menace?", https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-malware-2018-new-menace/, February 28, 2018.
13. Business Insider, "Thieves stole potentially millions of dollars in bitcoin in a hacking attack on a cryptocurrency company, Dec. 6, 2017.
14. Ars Technica, "Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency", https://arstechnica.com/information-technology/2018/04/suspicious-event-hijacks-amazon-traffic-for-2-hours-steals-cryptocurrency/, April 24, 2018.
15. Ersnt & Young, "EY research: initial coin offerings (ICOs)", http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/%24File/ey-research-initial-coin-offerings-icos.pdf, December 2017.
16. FireEye, "How the Rise of Cryptocurrencies is Shaping the Cyber Crime Landscape: Blockchain Infrastructure Use", https://www.fireeye.com/blog/threat-research/2018/04/cryptocurrencies-cyber-crime-blockchain-infrastructure-use.html, April 18, 2018.

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167