

ING 112A ASSESSMENT II: INTEGRATING SPECIFIC INFORMATION (25%)
QUESTION SHEET

Date: April 17, 2022 Time: 10:00 – 11:30

Warning: Appropriate disciplinary action will be taken against you if you share this document with third parties.

- **Read the paragraph below on the topic of cryptocurrencies.**
- **Read the 4 source excerpts and 2 graphs provided.**
- **Find relevant specific information in the sources in relation to the ideas stated in the paragraph.**
- **Select 1 sentence from one of the sources to use as a direct quotation by conforming to APA rules.** (6 pts)
- **Select 1 piece of specific information from one of the sources and paraphrase it by conforming to APA rules.** (10 pts). Choose only ONE of the two blanks to insert the paraphrase (Sentence 4 or 5).
- **Select one of the graphs and interpret it by conforming to APA rules** (9 pts). Choose only ONE of the two blanks to insert the graph interpretation (Graph 2 or 3).
- **You must provide the answers on the answer sheet and submit it to Ninova only.** (Late homework will not be accepted by email.)
- Only use an online dictionary/thesaurus. **Other internet sources/applications** (e.g. Google translate, paraphrasing tools) must **NOT** be used.
- It is your responsibility **not to share your homework with another student in addition to not having someone else do your homework.**
- If your paraphrase and graph interpretation match someone else's with a high similarity report, this will be evaluated as plagiarism and you will be given a ZERO.

The digital revolution has become one of the major driving forces of the world, manifesting itself in diverse areas ranging from technological innovation, science, and education to economy. Among these domains, economy is undisputedly the most prominent one. A breakthrough in digitalization involving monetary transactions began for the first time in 2009 with the implementation of digital currency, an electronic form of physical currency, called Bitcoin. **[1] Quotation** _____. The difference between traditional currency issued by a government, and digital currency is that its operation is decentralized and not supported and maintained by any government, enabling transactions to be completed exclusive of the requirement of third parties. The recognition and popularity of digital currency as a lucrative source of investment have increased exponentially in the past few years. **[2] Graph** _____. Digital currency is also referred to as cryptocurrency due to being secured by cryptography; however, in recent years, there has been an escalation in various illicit actions. **[3] Graph** _____. There are a number of reasons that denote cryptocurrency as high-risk. One of the difficulties is the necessity of mining, which is a highly complex computer activity for the verification of blocks of transactions and the generation of new coins that require excessive power consumption as well as technological proficiency. Another limitation is the fact that there are no personal identities associated with the individual accounts. Due to the absence of a regulatory party, both tracking a breach and ensuring the compensation of the loss are challenging tasks to accomplish; thus, this has led to an increase in fraud cases. For example, **[4] Paraphrase** _____. Additionally, the vulnerability of cryptocurrency is evident in a multitude of expansive criminal activities. These may arise from terrorists aiming directly at countries, organized crime groups conducting unlawful acts, or hackers seeking ransom. For instance, **[5] Paraphrase** _____. For the long-term viability of cryptocurrency, and its global acceptance, such serious complications should consequently be addressed.

SOURCES

Source: M. Daileh. Common cryptocurrency frauds, 2022, page 2

The rising value of cryptocurrencies promises huge returns for investors and cryptocurrency mining "fortunes". With cryptocurrency, a central bank is no longer required because Bitcoin, the currency, can be produced by anyone running a full node, a program that fully validates transactions and block. It is believed Bitcoin will do to banks what email did to the postal industry. The procedure is far from being simple, though. Learning how digital currency works is like learning a new language; it is incredibly difficult at the beginning, but once it clicks, it will stick with a person forever. However, in this lawless and unregulated crypto world, the risk of becoming a victim of fraud is very high as defrauders often have an advantage because there are few to no regulations governing the cryptocurrency market for investors, compared to the traditional stock market. From October 2020 through March 31, 2021, reports of crypto-related fraud skyrocketed to nearly 7,000 people reporting losses of more than \$80 million. There has been a 12-fold increase in the number of fraud related reports compared to the same period a year ago and a nearly 1,000% rise in reported losses. One common crypto fraud is Ponzi Schemes which is a type of investment scam where victims are tricked into investing in a non-existent project or "get-rich-quick scheme". Falsifying data is easy when the money is virtual anyway. Pump and dump is another type of fraud whereby defrauders encourage investors to buy crypto assets in little-known cryptocurrency projects, based on false information. Moreover, there are fake apps in which defrauders falsify legitimate cryptocurrency apps and upload them to app stores. If installed, it could steal personal and financial data.

Source: T. Sadon. Evaluation of potential cryptocurrency development in terrorist financing, 2021, page 23

Domestically and internationally, the focus on terrorist financing strengthened greatly, mainly after the 9/11 incident. Internationally, the United Nations, World Bank, IMF, and FATF have focused on the issue of terrorist financing, and even on the role of cryptocurrency in terrorist financing in recent years. Between 2016 and 2017, illegal crypto transactions linked to terrorism had risen from 12 to 25 cases. Terrorist organizations use cryptocurrency to trade drugs, weapons, and other items on the black market. Similarly, terrorists can ask for funding and donations for extremist organizations, without revealing their identity. Militant Bahrin Naim, the planner of the terrorist attacks in Jakarta in 2016, used Bitcoin for virtual payment to transfer funds to the armed elements and finance terrorist activities. The money was used to fund a suicide attack at the Police Headquarters in Java. In addition, there are also many anecdotes about terrorists using cryptocurrency in blackmail schemes online.

Source: Rand Corporation. Crypto in organized crime: Money laundering from drug dealing, 2022, page 7

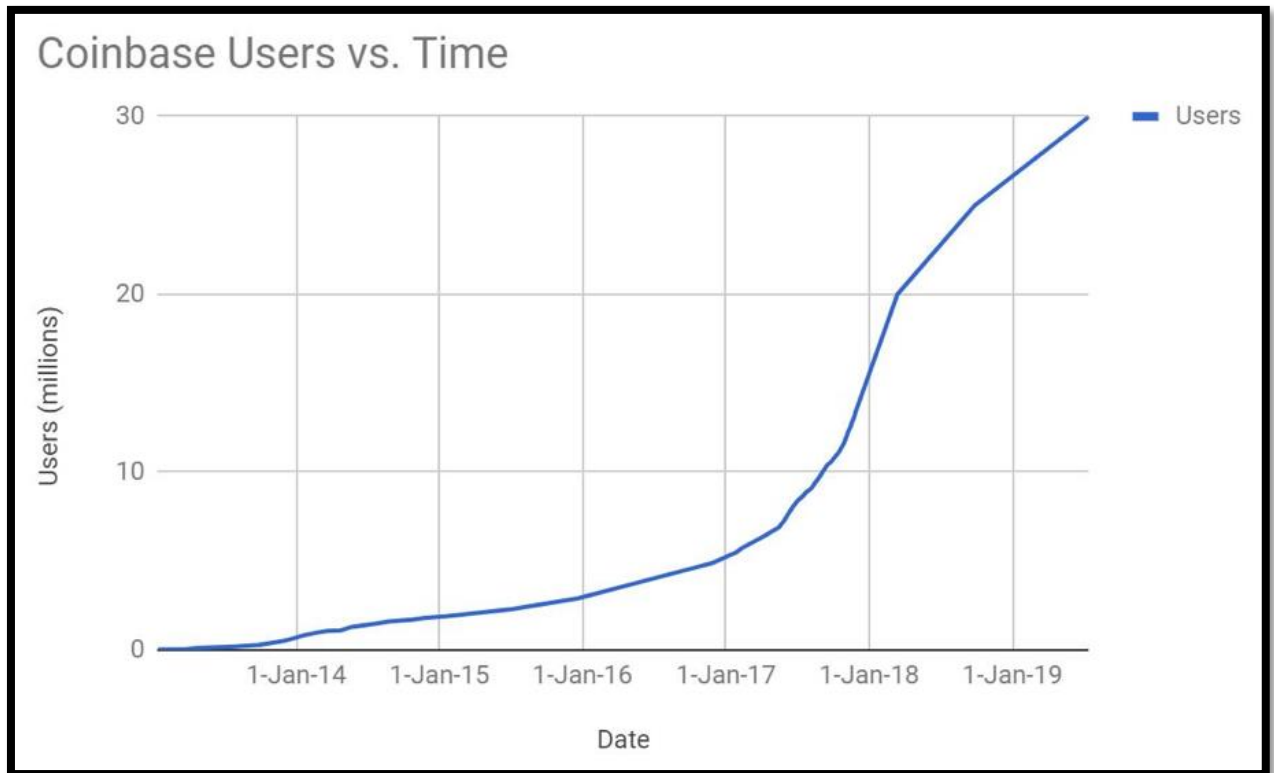
Most cryptocurrency is laundered through a limited number of services. For example, particular exchanges are favoured by criminals. Whilst the vast amount of cryptocurrency usage and exchange is for legitimate reasons, organised criminals have identified the benefits that cryptocurrency provides them. There are parts of the cryptocurrency structure that are being exploited to launder criminal cash, particularly from drug dealing. Blockchain data company Chainalysis tracks cryptocurrency wallets controlled by criminals such as ransomware attackers, malware operators, scammers, human traffickers, dark net market operators, and terrorist groups. By following flows of cryptocurrency from addresses associated with criminal activity, Chainalysis was able to estimate the amount "laundered". Criminals laundered \$8.6bn of cryptocurrency to cover up money gained from drug dealing in 2021, up by 30% from the last year.

Source: M. Wilson, J. Souter. The digital gold rush-bitcoin in connection with ransoms, 2021, page 5

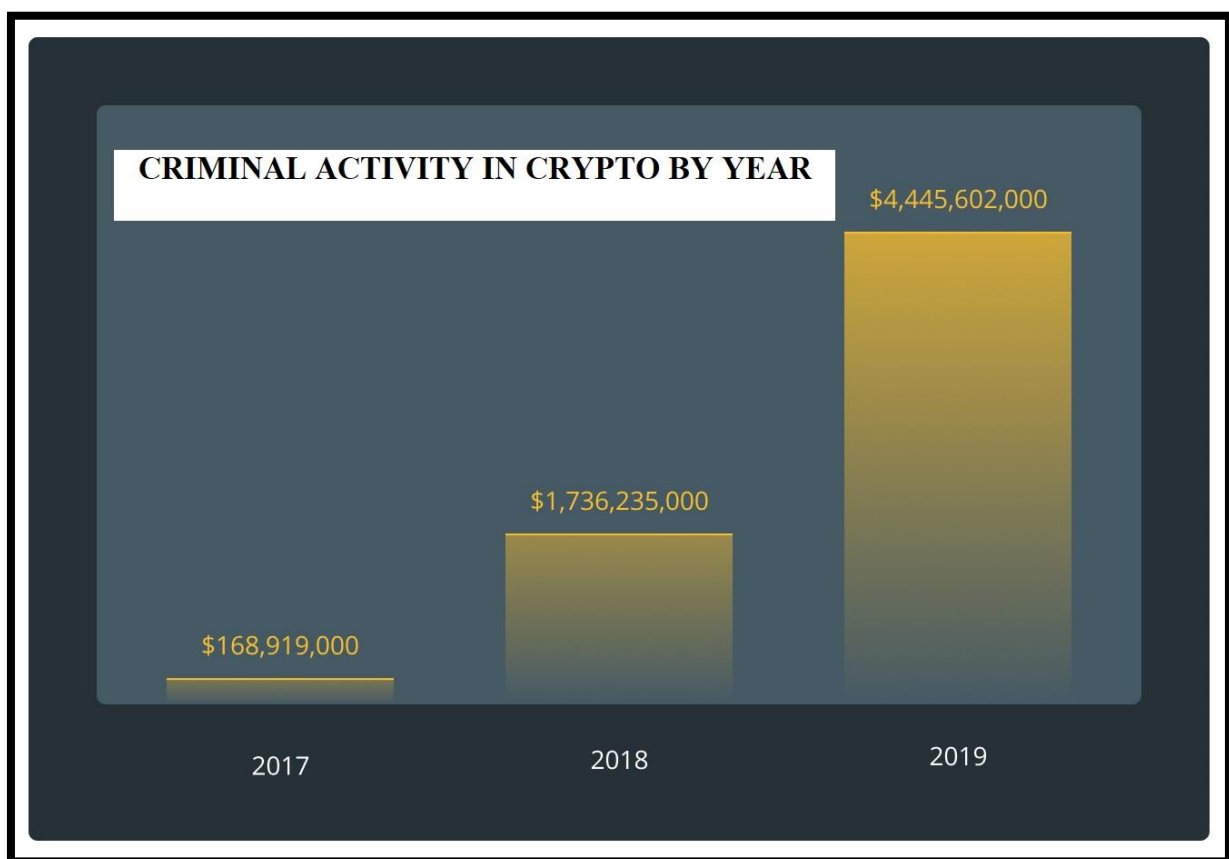
Digital currencies such as Bitcoin have gained traction. Bitcoin seems to offer an innovative option to citizens disenchanted with the existing monetary system. Bitcoin is not a currency for a government, it is a global currency for the people. Bitcoin is a technological masterpiece, a digital version of gold, eGold. However, in its early days, Bitcoin acquired an unsavoury reputation for facilitating illicit commerce. It has been used recently by hackers who demanded ransomware payments in bitcoins. Cryptocurrency ransom payments are often asked when criminals hold corporate data hostage. Following an attack on its computer systems, Brazilian meat processing company JBS, which delivers a fifth of all the beef consumed in the United States, paid an \$11 million ransom in Bitcoin. US authorities said the group responsible was hacking collective "REvil," which allegedly has ties to Russia. Known as a ransomware attack, this type of extortion sees corporate data stolen or computer systems locked. The availability of cryptocurrencies has accelerated large-scale ransomware attacks by making it easy to move large sums of ransom money across borders in seconds in a way that is untraceable and definitely uncontrollable.

GRAPHS

Source: H. Partz. Coinbase added 8 million new users in the past year, 2019, page 1



Source: W. Heasman. The fact, the fiction and the context, 2019, page 8



---000---