Republic of Namibia

Financial Intelligence Centre

P.O.BOX 2882, WINDHOEK

Tel: + 264 61 2835100, Fax +264 61 2835259

Web address: www.fic.na

E-mail address: helpdesk@fic.na

BITCOIN SCAMS

ISSUED: MAY 2021

1. Introduction

The Financial Intelligence Centre (FIC) has worryingly observed an increasing trend in financial crimes related to virtual currencies, particularly Bitcoin Scams. Bitcoins, often described as cryptocurrencies, virtual currencies or digital currencies are the most commonly used virtual currencies. Fraudsters appear to be taking advantage of the increased usage of these virtual assets or digital currencies to illegally solicit funds from members of the public through deceptive, dishonest and fraudulent means. These scams often result in huge financial losses to members of the public. Proceeds from such are often laundered through the financial system. The FIC is sharing this publication to help enhance public awareness around such activities.

2. Understanding Bitcoin transactions

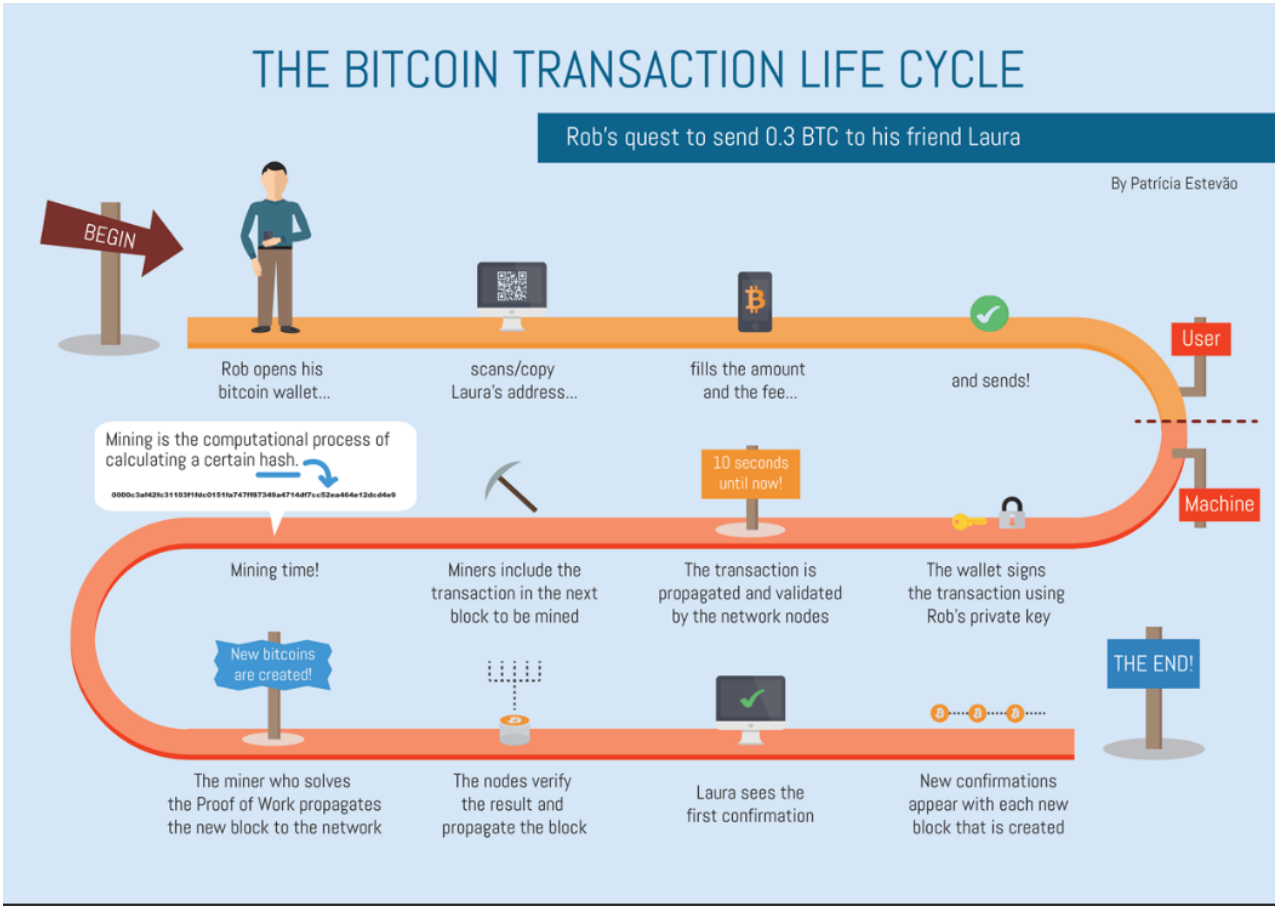


Figure 1: Bitcoin transaction life cycle

Bitcoins are currencies which are completely virtual and are stored in “digital wallets” which exists either in the cloud or on a user’s computer. The wallet functions more like a virtual bank account that allows the user to send or receive Bitcoins, pay for goods or to save their money, see Figure 1[1] above.

Bitcoins move on the blockchain which is a consensus network that enables the movement of values, including digital currency. The blockchain is a decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. Unlike conventional fiat currencies regulated and controlled by central banks, Bitcoin is not controlled by any financial institution or government. Anyone can open or create a wallet from which to receive or send Bitcoins. Owing to complex control measures on the blockchain, it is almost impossible to amend or remove transactions once processed and confirmed.

3. How do these schemes operate?

Bitcoin’s rapid rise in value over the years has attracted a lot of interest, with members of the public finding it as a high return yielding investment. However, such growth rate has equally been exploited to defraud unsuspecting persons. While Bitcoin is used as a currency, many users also regard such as an investment instrument. Those with investment objectives often buy and hold such coins expecting (or hoping) that its value would increase. As the value increases over time, speculators would often sell to recoup investments plus returns while others prefer to hold on to the Bitcoin as an asset of value which increases their financial position (balance sheet). Fraudsters are aware of the exceptional growth of Bitcoin value in recent years and appear to use such to lure unsuspecting members of the public into various scams. Figure 2[2] below shows the growth of Bitcoin in value over the years.

[1]Source: https://www.bing.com/images/search?view=detailV2&ccid=K6iO4o2o&id=AF783E4A3629B9C94727F5209A870908F1462188&thid=OIP.K6iO4o2oxd0IeU0luVze0wHaFP&mediaurl=https%3A%2F%2Fwww.weusecoins.com%2Fimages%2Fbitcoin-transaction-life-cycle-high-resolution.png&exph=877&expw=1240&q=bitcoin+process+map&simid=607996304960675046&ck=BB9648B1B632E537180CB8AA9781349A&selectedindex=11&form=IRPRST&ajaxhist=0&ajaxserp=0&vt=0&sim=11&cdnurl=https%3A%2F%2Fth.bing.com%2Fth%2Fid%2FR2ba88ee28da8c5dd08794d25b95cded3%3Frik%3DiCFG8QgJh5og9Q%26pid%3DImgRaw

[2] Source: https://www.statista.com/statistics/326707/bitcoin-price-index/

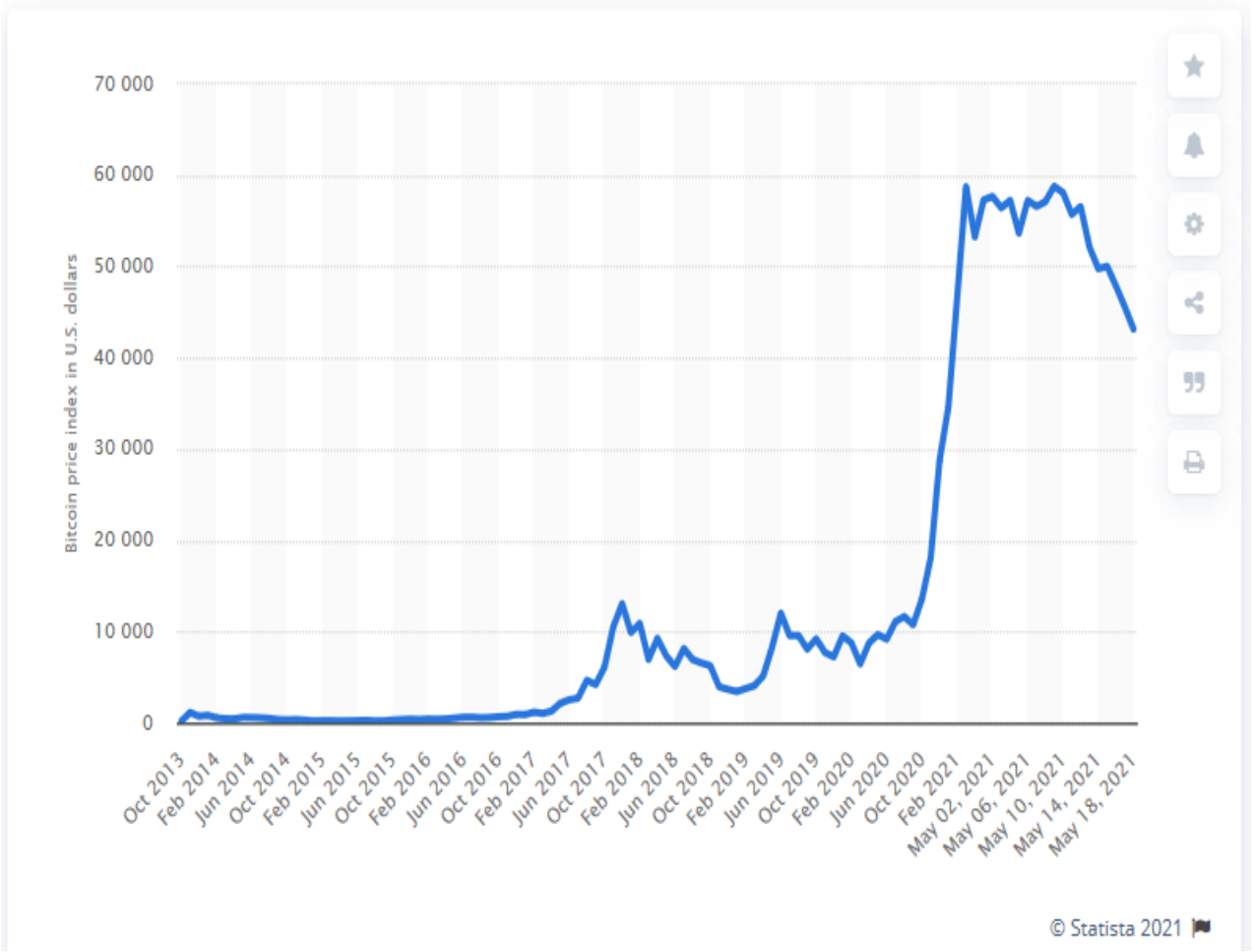


Figure 2: Growth in price of Bitcoin, per unit of Bitcoin in USD

Exchange Houses play a key role in Bitcoin operations. They operate in a manner similar to conventional banks as they facilitate the exchange of fiat currencies to Bitcoin and vice-versa. Members of the public who want to buy or sell Bitcoin often do so through Exchange Houses. Around the world, many reported cases show that Exchange Houses are often targeted by hackers. Hackers have many times managed to penetrate the access control systems of Exchange Houses to steal Bitcoins in the custody of Exchange Houses. Some of the largest Exchange Houses have not recovered from such and have been liquidated. Targeting Exchange Houses often requires a certain degree of knowledge and capacity to penetrate the sophisticated access control systems of these exchanges.

This publication mainly seeks to create awareness around risks to individual members of the public making use of Bitcoins. From local observations, the highest risks or exposure to fraud is usually with speculators who intend to buy and resell Bitcoins for quick financial returns. Criminals target such persons with promises of investing on their behalf to ensure much higher returns. Various schemes are presented to unsuspecting members of the public demonstrating why it is lucrative to invest via agents or brokers than persons investing in their individual capacity without intermediaries. A common scheme is promises or assurances that investing via brokers or agents enables the broker to pool funds from many people and make larger investments which result in much higher returns than what an individual investor can ever generate. This is the common way unsuspecting members of the public have been coerced to invest in Bitcoin via agents or brokers. Many times, these investments would be sourced from large groups but only a few lucky ones could receive returns while most 'investors' would not receive any returns, let alone their initial investments. It has become apparent that pyramid scheme operators often make use of virtual asset investments as one of their investment instruments. The FIC has issued[3] a similar report warning about illicit Pyramid scheme operations. Such is worth looking at in this context.

Bitcoin mining is quite costly, especially on an individual level, but can be lucrative if the right technical capacity created and properly managed. Scammers have created fake web pages that offer mining power *(hashing)* with supposed guaranteed profits on investment over a short period of time. Usually, this is used to merely solicit investments or funds from unsuspecting members of the public in the disguise of such being invested in Bitcoin mining or hashing capacity. Investors are assured that the lucrative returns from such mining activities will be shared with them. What has come to the fore in many reports is that such investment schemes, along with their fake web pages, would in time disappear with funds collected from the public.

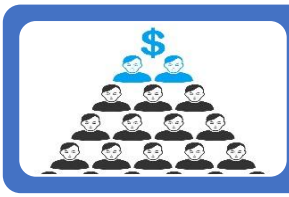
Below are some common techniques used by fraudsters in this regard:

[3] Source: FIC Website: https://www.fic.na/uploads/Public_Awareness/Forewarning_Reports/Pyramid%20Schemes.pdf

Fraudulent Bitcoin Exchanges: Fraudsters set up illicit bitcoin exchanges. These exchanges may trick users by offering extremely competitive investment returns.

Bitcoin Mining Schemes: Because Bitcoin mining on an individual level is quite costly in terms of power consumptionon, scammers have come up with fake web pages that offer mining power (*hashing*) with guaranteed profits on investment over a short period of time. Later when they have collected enough money they close these pages and disappear with investors' money.

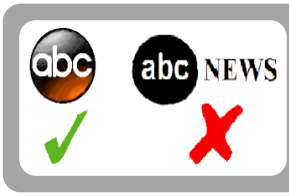
Malware: When the Bitcoin wallet is connected to the internet, fraudsters can use malware to get access to such funds. One can download malware by clicking links in your email, also from some websites and social media platforms. Some malware programs, once installed, will change bitcoin addresses so the bitcoin gets sent to the hacker's address.



Pyramid Schemes: These are fraudulent schemes where participants are paid to recruit others to participate. They promise consumers or investors large profits based primarily on introducing new members into the scheme, not based on profits from Bitcoin investments. However, when the schemes get too large and cannot raise enough revenues from new investors to pay earlier investors or when the pool of recruits is depleted, the scheme eventually collapses.

Ponzi Schemes: This is a "get rich quick scheme" where scammers promise investors significant amounts of money on their investments in Bitcoins within extremely short periods of time. However, there is no real investment being made, the scammers only pay existing investors with funds collected from new investors. The scheme eventually collapses when there is a short supply of new investments.

Phishing scams: Scammers impersonate a service, company or individual by way of email or other text-based communication, or by hosting an illegitimate website. The goal is to trick a victim into revealing his or her private keys or to send bitcoins unknowingly to the scammer's address.



Fraudulent Websites: Criminals use professional-looking websites and the names of well-known brands or individuals to lure their victims.

Fraudulent Mobile Applications: Another common way scammers trick bitcoin investors is through illegitimate applications available for download through Google Play and the Apple App Store etc. These are malicious apps are designed to steal users bitcoin keys and passwords.

4. How do I protect myself from these Scams?

Always protect bitcoin private keys. Never share private keys with anyone;

Use strong passowrds and update same regularly (passwords with combination of letters, numbers, other characters etc.);

Do not open suspicious texts, pop-up windows or click on links or attachments in emails;

Be careful when shopping online and always make use of reputable and trustworthy online shopping services.

Do not be rushed or pressured into making a decision regarding transactions on the blockchain or investments;

Properly identify the entities or persons to invest with. Find out if they or their entiy is registered with any regulatory body, amonst others;

Before downloading any bitcoin wallet on the Google Play or Apple App Store etc., read reviews around such and also do research on any allegations, reports around such platform;

Make use of reputable exchanges (verify their existance/legitimacy) before sending any money or any bitcoins;

Be very cautious about the type of applications that have administrator access to devices;

Beware of any investment scheme that allows more levels of distributors to collect commissions on a single sale.

REMEMBER

Scammers raise funds by applying pressure tactics that force unsuspecting persons into making hasty decisions influenced by great promises. Always research the legitimacy and history of such entities prior to investing with them. In the same vein, members of the public are urged to be vigilant and do proper due diligence before investing in cryptocurrencies in general. If you become a victim of a Bitcoin scam, immediately file a report with the FIC at the Bank of Namibia or contact the nearest police station to initiate a criminal investigation.