TITLE OF THE ARTICLE: THE MONEY LAUNDERING RISKS AND VULNERABILITIES ASSOCIATED WITH MMM NIGERIA

AUTHOR: EHI ERIC ESOIMEME

CONTRIBUTOR AT KYC360

DEPUTY EDITOR IN CHIEF OF DSC PUBLICATIONS LTD

EMAIL ADDRESS: EHIESOIMEME@YAHOO.COM

CORRESPONDING AUTHOR: EHI ERIC ESOIMEME

AUTHOR OF THE BOOK: THE RISK-BASED APPROACH TO COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

ACKNOWLEDGMENTS

I would like to express my profound and sincere appreciation to Tom Brown CAMS, for impacting on me, the research skills needed to carry out this project.

COMPETING INTERESTS

I declare that I have no competing interests.

ABSTRACT:

PURPOSE – This paper aims to help build awareness with the regulatory, enforcement and customs authorities as well as reporting entities about money laundering risks and vulnerabilities of the MMM Scheme, and how to mitigate them.

DESIGN/METHODOLOGY/APPROACH – This paper relies mainly on primary and secondary data drawn from the public domain. It also relies on documentary research.

FINDINGS – This paper determined that the MMM Scheme could be used by criminals to launder proceeds of crime.

ORIGINALITY/VALUE – While most publications on MMM are focused on fraud, this paper focuses on the money laundering risks and vulnerabilities associated with the MMM scheme.

1. INTRODUCTION

Criminals have shown adaptability and opportunism in finding new channels to launder the proceeds of their illegal activities and to finance terrorism. As the Internet becomes more and more a worldwide phenomenon, Ponzi schemes are potentially subject to a wide range of risks and vulnerabilities that can be exploited by criminal organizations and terrorist groups.[1]

Investments in Ponzi Schemes like Mavrodi Mondial Movement (MMM) can be used to integrate money of illegal origin into the financial system, akin to investment of proceeds of crime in gambling. MMM Nigeria encourages users to provide help to other participants using bitcoin rather than traditional currencies. If you transfer money (provide help) via the Bitcoin (not a bank), you have an opportunity to acquire Mavro-50% in the MMM Scheme.[2] **Virtual currencies such as Bitcoin and other emerging payments technologies, while representing an opportunity for financial innovation, have attracted the attention of various criminal groups, and may be vulnerable to abuse by money launderers.**

Bitcoin is the preferred method of online payment for illicit commodities including firearms and drugs. The majority of dark web websites have payment systems reliant on Bitcoin because of the perceived anonymity of these types of payment product. Current criminal exploitation of Bitcoin can be divided into two distinct areas: internally against the Bitcoin platform and users themselves, for example theft

[1] Financial Action Task Force (2008), 'MONEY LAUNDERING & TERRORIST FINANCING VULNERABILITIES OF COMMERCIAL WEBSITES AND INTERNET PAYMENT SYSTEMS', Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20TF%20Vulnerabilities%20of%20Commercial%20Websites%20and%20Internet%20Payment%20Systems.pdf (accessed 16 January 2017).

[2] MMM Nigeria (2017), 'What is Bitcoin and how to participate in MMM using bitcoins?', Available at: http://nigeria-mmm.net/bitcoin/ (accessed 16 January 2017).

or fraud; and externally by exploiting the system as a means of exchange, for example money laundering, terrorist financing or the purchase of criminal commodities.[3]

Investments in MMM Nigeria are therefore a risk area for money laundering due to a lack of transparency regarding Bitcoins. Indeed, investments may be unclear and obscure, making it difficult to verify the origin of the invested funds. This situation is in fact not different from the acquisition of any private company in the industrial or commercial sector.

This paper aims to help build awareness with the regulatory, enforcement and customs authorities as well as reporting entities about money laundering risks and vulnerabilities of the MMM Scheme, and how to mitigate them.

While most publications on MMM are focused on fraud, this paper focuses on the money laundering risks and vulnerabilities associated with the MMM scheme.

This section is divided into two subsections i) What are Ponzi Schemes and ii) How Does MMM Nigeria Work.

1.1. WHAT ARE PONZI SCHEMES

A Ponzi scheme is an investment fraud that involves the payment of purported returns to existing investors from funds contributed by new investors. Ponzi scheme organizers often solicit new investors by promising to invest funds in opportunities claimed to generate high returns with little or no risk. In many Ponzi schemes, the fraudsters focus on attracting new money to make promised payments to

[3] HM Treasury (2015), 'UK national risk assessment of money laundering and terrorist financing', Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf (accessed 17 October 2015).

earlier-stage investors to create the false appearance that investors are profiting from a legitimate business.[4]

'Ponzi' schemes have existed for many years. They are simple and effective scams in which the promoters attract investors to a scheme by promising a very high return on investment, while guaranteeing the security of the investment.[5]

Part of the money deposited by early investors is used by the scheme's promoter to pay subsequent investors their first dividend cheques or interest. These initial returns help convince victims that the scheme is both lucrative and sound.

In the early stages of a Ponzi scheme, only a few investors are required for the scheme to be successful. The promoter continues paying the investors dividends until the investors are comfortable with their investments and willing to invest more.

The scammers use some of the funds deposited by early investors to pay initial dividend cheques or interest - at this early stage the ponzi scheme only requires a few investors to operate successfully. The promoter continues paying the investors impressive dividends for a couple of months until the investors, encouraged by the early dividends, decide to invest more.[6]

The investors may also encourage their friends and relatives to invest. Soon there is a steady flow of funds into the scheme and an ever-growing number of investors.

---

[4] U.S. Securities and Exchange Commission (2013), 'Ponzi Schemes', Available at: https://www.sec.gov/answers/ponzi.htm (accessed 17 January 2017).

[5] Australian Transaction Reports and Analysis Centre (2015), 'Financial crime and money laundering threats and methodologies', Available at: http://www.austrac.gov.au/typologies-2009-threats-methodologies (accessed 16 January 2017).

[6] Australian Transaction Reports and Analysis Centre (2013), 'AUSTRAC typologies and case studies report', Available at: http://www.austrac.gov.au/sites/default/files/documents/typ13_full.pdf (accessed 17 January 2017).

If the promoter is disciplined and retains sufficient funds in the scheme to continue to pay out 'dividends', a ponzi scheme can continue for many years. Theoretically, if the scheme continues to draw in new investors, it could go on indefinitely. In practice such schemes usually collapse because the promoter starts to spend the money too quickly, or the pool of investors starts to dry up.[7]

The schemes are named after Charles Ponzi, who duped thousands of New England residents into investing in a postage stamp speculation scheme back in the 1920s. At a time when the annual interest rate for bank accounts was five percent, Ponzi promised investors that he could provide a 50% return in just 90 days. Ponzi initially bought a small number of international mail coupons in support of his scheme, but quickly switched to using incoming funds from new investors to pay purported returns to earlier investors.[8]

1.2. HOW DOES MMM NIGERIA WORK?

MMM is a community of people providing each other financial help on the principle of gratuitousness, reciprocity and benevolence.

In MMM you don't have to make contracts or pledge your property. In MMM there are no lenders and no debtors. Everything is very simple: one participant asks for help — another one helps.

The only thing that MMM demands from its participants is to be honest and kind to each other. You ask for financial help when you need it, you give financial help when you are able to do it.

---

[7] Australian Transaction Reports and Analysis Centre (2015), 'Financial crime and money laundering threats and methodologies', Available at: http://www.austrac.gov.au/typologies-2009-threats-methodologies (accessed 16 January 2017).

[8] Frank B. Cross and Roger LeRoy Miller (2011), 'The Legal Environment of Business: Text and Cases: Ethical, Regulatory, Global and Corporate Issues', Cengage Learning; 8th edition p. 76.

There is no central account, where all the System money flows to and where it can be easily stolen from. ***All the money is only on the banking accounts of the participants themselves! Participants transfer to each other directly, without intermediaries.*** **In fact, MMM only regulates the process — nothing more. So the System completely belongs to people.**

How does it work technically? You declare the willingness to give help (click in your Personal Office (hereinafter PO) "Provide Help"), after which your account will be rewarded with mavro (internal "currency"/scores of the System). Mavros will start growing from the moment of offering the contribution at the rate of 30% per month. (Calculation of reward occurs twice a week, on Tuesdays and Thursdays at 00:00 GMT.) This sum in Mavro shows how much you can request for yourself.

Say you have announced willingness to assist with $ 100. You will be rewarded in your PO with 100 mavro. And they will immediately start growing! A month later, these 100 will become 130 mavro. Accordingly, you will be able to request help for $ 130.

However, it is not necessary at all to wait for a month. Help can be requested at any time. But only after confirmation of your mavro. What does "after confirmation" mean? It means only after you actually transfer money, i.e. really give help to another participant. (But not just declare willingness. :-)) Request for providing help comes to you in your personal office. If you do not do it within 48 hours, you will be removed from the system.

Each participant is allowed to have only one account.[9]

[9] MMM Nigeria (2017), 'How does MMM Work', Available at: http://nigeria-mmm.net/what_is_mmm/ (accessed 7 January 2017).

2. FIVE FACTORS CREATING MONEY LAUNDERING VULNERABILITIES

This section of the paper identifies a range of risk factors that help to identify the money laundering risks associated with MMM Nigeria.

2.1. NON-FACE-TO-FACE RELATIONSHIPS AND ANONYMITY

As with many Ponzi schemes, MMM allows for non-face-to-face business relationships and transactions. This allows a criminal to open a MMM account using the identity of a real person. MMM participants often have many accounts in many locations. Customer Due Diligence measures may prove ineffective where the staff performing online due diligence on a potential customer is unable to physically verify the identity of such customer.

The absence of face-to-face contact may indicate a higher money laundering risk situation due to increased impersonation fraud risk and the chance that customers may not be who they say they are. If customer identification and verification measures do not adequately address the risks associated with non-face to face contact, such as impersonation fraud, the money laundering risk increases, as does the difficulty in being able to trace the funds.[10]

High-risk customers like Politically Exposed Persons (PEPs) could exploit the non-face-to-face feature of MMM by using the identity of low-risk customers (e.g. pensioners) to open MMM accounts. Corrupt PEPs could use the MMM Scheme to conceal the origins of criminal funds by investing large sums of

[10] Financial Action Task Force (2010), 'Money Laundering Using New Payment Methods', Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf (accessed 18 January 2017).

money in the scheme; the money comes back as clean money once the corrupt PEP makes a request for help in the MMM portal. The Corrupt PEP gets his investment back with a profit of 30%.

2.2. METHODS OF FUNDING

The methods by which a Ponzi scheme can be funded impacts on the level of money laundering risk posed.

Anonymous funding methods obscure the origin of the funds, creating a higher money laundering risk.[11]

MMM Nigeria accepts many secure payment options for MMM transactions; Bank wire, MasterCard, Visa Debit, Interac and Bitcoin are all accepted.[12]

The Bitcoin funding option may present a higher money laundering risk than Bank wire, MasterCard, Visa Debit and Interac. Most Banks that offer many different kinds of financial services like the ones mentioned above have in place transaction monitoring systems which can detect suspicious activity based on money laundering and terrorism financing typologies and indicators. Such monitoring systems take into consideration customer risks, country or geography risks, and product, service transaction or delivery channel risks. The transaction monitoring system can also be used to identify multiple accounts or products held by an individual or group, such as holding multiple prepaid cards.

Convertible virtual currencies like Bitcoin, on the other hand, permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They

[11] Financial Action Task Force (2008), 'Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems', Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20TF%20Vulnerabilities%20of%20Commercial%20Websites%20and%20Internet%20Payment%20Systems.pdf (accessed 16 January 2017).

[12] MMM Nigeria (2016), 'Mavro-50% Is Available When You Provide Help in Bitcoin', Available at: http://nigeria-mmm.net/news/mavro_50_is_available_when_you_provide_help_in_bitcoin-6219.html (accessed 17 January 2017).

may also permit anonymous transfers, if sender and recipient are not adequately identified. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. There is no central oversight body, and no anti-money laundering (AML) software currently available to monitor and identify suspicious transaction patterns like those of the traditional banking system. Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger may collect). It thus offers a level of potential anonymity impossible with traditional credit and debit cards or older online payment systems, such as PayPal.[13]

Failure of MMM operators to adequately assess the money laundering risks associated with Bitcoin may result in a customer's account being used to facilitate financial crime.

2.3. RECORD KEEPING, TRANSACTION MONITORING AND REPORTING

Transaction and Customer Due Diligence (CDD) records are key to anti-money laundering/countering the financing of terrorism (AML/CFT) efforts and support law enforcement investigations. At a minimum the transaction record of a payment or funds transfer should include information identifying the parties to the transaction, any account(s) involved, the nature and date of the transaction, and the amount transferred. The relative size of a transaction does not necessarily equal the value of the transaction record to law enforcement, so recordkeeping should be kept for all transactions irrespective of the

[13] Financial Action Task Force (2014), 'VIRTUAL CURRENCIES – KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS', Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (accessed 10 January 2017).

value. The records that are retained should be sufficient to allow the tracing of funds through the reconstruction of transactions.[14]

MMM Nigeria encourages users to provide help to other participants using bitcoins rather than traditional currencies.

The electronic nature of Bitcoins provides in principle a good foundation for effective record keeping and the monitoring of transactions. Bitcoin is nothing more than a digital file that lists every transaction that has ever happened in the network in its version of a general ledger called the "block chain."

Anyone can download the free, open-source software from a website to send, receive, and store bitcoins and monitor Bitcoin transactions. Users can also obtain Bitcoin addresses, which function like accounts, at a Bitcoin exchanger or online wallet service. Transactions (fund flows) are publicly available in a shared transaction register and identified by the Bitcoin address, a string of letters and numbers that is not systematically linked to an individual. Therefore, Bitcoin is said to be "pseudoanonymous".[15]

The money laundering risk in MMM Nigeria increases when users decide to transfer funds using Informal Value Transfer Systems like Hawala and not Bitcoin.

Hawala is an alternative or parallel remittance system. It exists and operates outside of, or parallel to "traditional" Banking or financial channels. It was developed in India, before the introduction of Western banking practices, and is currently a major remittance system used around the world.[16]

---

[14] Financial Action Task Force (2013), 'GUIDANCE FOR A RISK BASED-APPROACH: PREPAID CARDS, MOBILE PAYMENTS AND INTERNET-BASED PAYMENT SERVICES', Available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf (accessed 12 January 2017).
[15] Bitcoin Project (2017), 'Frequently Asked Questions about Bitcoin', Available at: https://bitcoin.org/en/faq (accessed 15 January 2017).
[16] Financial Crimes Enforcement Network, 'The Hawala Alternative Remittance System and its Role in Money Laundering', p. 5.

The system offers two great advantages for laundering money; the first being that they eliminate the physical movement of money; and the second is that they annihilate or obscure the paper trail. Thus, these systems when used in conjunction with conventional money laundering; make the task of tracking down the laundered money or even the launderer virtually impossible.[17]

Hawala has proven to be very difficult to regulate. For instance, Victor Comras states "most hawala operations are unregulated. Few records are kept and transfers are handled informally and, in most cases, with no real oversight. This offers criminals, an ideal channel for handling its money transfer requirements." To further emphasize the problem of regulation, Comras states "many hawaladars are also well connected with banks in Asia and the Middle East. Their transfer accounts raise few questions and are employed for settlement between hawaladars, hiding completely the transactions originator and ultimate receiver".[18]

[17] Trehan, J., (2002), 'Underground and Parallel Banking Systems', JFC 10(1), pp. 76–84
[18] David C. Faith, (2011), 'The Hawala System' Global Security Studies, Winter', Volume 2, Issue 1, 23 at 28

3. PROTECTING AGAINST THE VULNERABILITIES OF MONEY LAUNDERING

The overall degree of risk of MMM Nigeria is, in a given context, the cumulative effect of combining each of the risk factors described above. In addition, procedures to mitigate risk should be proportionate to the level of risk posed by the product or service. Adopting proportionality criteria allows the risks posed by MMM to be addressed, while maintaining the functionality which is aimed at customer convenience and ease of use.[19]

3.1 EFFECTIVE ACCOUNT OPENING PROCEDURES

Effective account opening policies and procedures are fundamental risk controls for MMM relationships. Effective procedures include the proper identification of the owners of the account, including the beneficial owners, the sources of their wealth and their normal and expected transactions.

The MMM management team should have specific policies for employees who approve, accept and document new MMM accounts. To verify the financial status of an individual, MMM's account opening process should require responsible MMM personnel to identify the principal owners and should include a review of relevant documentation, such as financial statements, credit reports and referrals.

In short, the MMM team should exercise the degree of due diligence necessary to determine what types of risks are included in opening a particular account and then ensure that adequate procedures are in place to identify and control those risks.

[19] Financial Action Task Force (2013), 'GUIDANCE FOR A RISK BASED-APPROACH: PREPAID CARDS, MOBILE PAYMENTS AND INTERNET-BASED PAYMENT SERVICES', Available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf (accessed 12 January 2017).

3.2 MONITORING FOR HIGH RISK ACTIVITY

MMM should monitor high-risk customer activity in order to detect and report suspicious activity in a timely manner. MMM should evaluate accounts on a risk-grade basis, whether by type of business, geographical location, or MMM product or service that may be more vulnerable to money laundering.

While not all MMM accounts or relationships will fall into a higher risk category under this approach, those that do should be managed accordingly. For example, MMM accounts of politically exposed persons like James Ibori should be effectively monitored and properly scrutinized. **Accounts of Politicians ought to be subject to MMM's highest levels of scrutiny, including requirements for senior management approval, prior to opening an account, heightened monitoring, and annual reviews of account developments by the unit head.**

3.3 COMPENSATION AND OVERSIGHT

MMM should design compensation programs that balance quantitative and qualitative factors and that provide measurement tools to assess employee performance in both areas. They should also ensure that account relationship managers are subject to the same or a higher degree of oversight and control as managers of other areas of operation that may expose MMM to risk. Internal controls, audit and compliance processes should ensure that account managers operate with appropriate oversight and are subjected to periodic audit checks.

3.4 TRAINING FOR ANTI-MONEY LAUNDERING COMPLIANCE

MMM are recommended to train all appropriate personnel with respect to their responsibilities to comply with the requirements of the Relevant Anti-Money Laundering Laws/Regulations in Nigeria.[20] MMM training programs should provide relevant examples of money laundering in the MMM Scheme and should discuss MMM policies and procedures, liability issues and regulatory requirements. In addition, the training program should provide for regular updates to ensure employees are kept current in Anti-Money Laundering policies and regulatory changes.

3.5 AUDIT FOR COMPLIANCE WITH ANTI-MONEY LAUNDERING MEASURES

MMM must have an independent testing or audit function for Anti-Money Laundering compliance, including Suspicious Activity Reporting. Audit programs should focus on high-risk accounts and should include comprehensive transaction testing.

[20] The laws enacted to combat money laundering in Nigeria include: the **Money Laundering Prohibition Act 2011 (as amended), Central Bank of Nigeria (CBN) (Anti-Money Laundering and Combating the Financing of Terrorism in Banks and other Financial Institutions in Nigeria) Regulations 2013** and the **Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) Reporting Guidelines 2012**.

4. CONCLUSION

In view of the Money Laundering Risks associated with Bitcoin, MMM Nigeria are recommended to adopt Goldmoney as its preferred method of online payment for MMM transactions.

Goldmoney is a consumer-focused internet platform offering free global payments combined with unprecedented access to secure, redeemable gold for savings.[21]

Goldmoney maintains bank-grade Know Your Customer ("KYC") policies. Every account holder is required to upload their government-issued ID and go through an on-boarding process that includes a background check and mobile phone verification. Ongoing compliance and surveillance of suspicious activity is reported to relevant regulatory agencies.[22]

Goldmoney usually perform background checks prior to approving an individual's application to open a Goldmoney Account or at any other time during the course of the relationship at Goldmoney's discretion. Goldmoney may contact credit bureaus to obtain information about a potential customer for purposes of confirming the applicant's identity under applicable "know-your-client" rules.[23]

If you open a Business Account, you are providing Goldmoney, at its discretion, authorization to obtain your personal and/or business credit report from a credit reporting agency. You are also authorizing Goldmoney to obtain your personal and/or business credit report (a) when you apply for a Business Account; (b) when you request a product for which Goldmoney requires, in its discretion, a review of

---

[21] Goldmoney (2014), 'BitGold Inc. Raises $3.5 Million In Advance of Early 2015 Platform Launch', Available at: https://content.goldmoney.com/news/2014/12/23/bitgold-inc-raises-3-5-million-in-advance-of-early-2015-platform-launch/ (accessed 18 January 2017).

[22] Goldmoney (2016), 'Ownership, Safety, and Security of Your Gold, Available at: https://support.goldmoney.com/customer/en/portal/articles/1946269-ownership-safety-and-security-of-your-gold (Accessed 8th May 2015).

[23] Goldmoney (2016), 'Terms of Service', Available at: https://www.goldmoney.com/terms-of-service (accessed 19 January 2017).

your credit report; or (c) any time Goldmoney reasonably believes there may be an increased level of risk associated with your Business Account.[24]

The Goldmoney platform provides innovative solutions to the challenge of transacting with fully allocated and securely vaulted physical gold. Goldmoney accounts are free and convenient to open by anyone, anywhere in just minutes. Goldmoney provides users with a secure vault account to purchase gold using a variety of electronic payment methods, or with currency through an Automated Teller Machine (ATM) network. The platform also provides transaction capability including: instant cross-border gold payments, merchant invoicing and processing for gold, debit card spending of gold at traditional points of sale, conversions to a customer's external digital-wallet or bank, and physical gold redemptions.[25]

[24] Goldmoney (2016), 'Terms of Service', Available at: https://www.goldmoney.com/terms-of-service (accessed 19 January 2017).
[25] Goldmoney (2015), 'BitGold announces acquistion of GoldMoney', Available at: https://wealth.goldmoney.com/who-we-are/news/bitgold (accessed 19 January, 2015).

APPENDIX 1

FREQUENTLY ASKED QUESTIONS ABOUT BITCOIN

Question 1: What is Bitcoin?

Bitcoin is a consensus network that enables a new payment system and a completely digital money. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. From a user perspective, Bitcoin is pretty much like cash for the Internet. Bitcoin can also be seen as the most prominent triple entry bookkeeping system in existence.

Question 2: Who created Bitcoin?

Bitcoin is the first implementation of a concept called "cryptocurrency", which was first described in 1998 by Wei Dai on the cypherpunks mailing list, suggesting the idea of a new form of money that uses cryptography to control its creation and transactions, rather than a central authority. The first Bitcoin specification and proof of concept was published in 2009 in a cryptography mailing list by Satoshi Nakamoto. Satoshi left the project in late 2010 without revealing much about himself. The community has since grown exponentially with many developers working on Bitcoin.

Satoshi's anonymity often raised unjustified concerns, many of which are linked to misunderstanding of the open-source nature of Bitcoin. The Bitcoin protocol and software are published openly and any developer around the world can review the code or make their own modified version of the Bitcoin software. Just like current developers, Satoshi's influence was limited to the changes he made being adopted by others and therefore he did not control Bitcoin. As such, the identity of Bitcoin's inventor is probably as relevant today as the identity of the person who invented paper.

Question 3: Who controls the Bitcoin network?

Nobody owns the Bitcoin network much like no one owns the technology behind email. Bitcoin is controlled by all Bitcoin users around the world. While developers are improving the software, they can't force a change in the Bitcoin protocol because all users are free to choose what software and version they use. In order to stay compatible with each other, all users need to use software complying with the same rules. Bitcoin can only work correctly with a complete consensus among all users. Therefore, all users and developers have a strong incentive to protect this consensus.

Question 4: How does Bitcoin work?

From a user perspective, Bitcoin is nothing more than a mobile app or computer program that provides a personal Bitcoin wallet and allows a user to send and receive bitcoins with them. This is how Bitcoin works for most users.

Behind the scenes, the Bitcoin network is sharing a public ledger called the "block chain". This ledger contains every transaction ever processed, allowing a user's computer to verify the validity of each transaction. The authenticity of each transaction is protected by digital signatures corresponding to the sending addresses, allowing all users to have full control over sending bitcoins from their own Bitcoin addresses. In addition, anyone can process transactions using the computing power of specialized hardware and earn a reward in bitcoins for this service. This is often called "mining". To learn more about Bitcoin, you can consult the dedicated page and the original paper.

Question 5: Is Bitcoin really used by people?

Yes. There is a growing number of businesses and individuals using Bitcoin. This includes brick and mortar businesses like restaurants, apartments, law firms, and popular online services such as Namecheap, WordPress, and Reddit. While Bitcoin remains a relatively new phenomenon, it is growing

fast. At the end of August 2013, the value of all bitcoins in circulation exceeded US$ 1.5 billion with millions of dollars worth of bitcoins exchanged daily.

Question 6: How does one acquire bitcoins?

- As payment for goods or services.
- Purchase bitcoins at a Bitcoin exchange.
- Exchange bitcoins with someone near you.
- Earn bitcoins through competitive mining.

While it may be possible to find individuals who wish to sell bitcoins in exchange for a credit card or PayPal payment, most exchanges do not allow funding via these payment methods. This is due to cases where someone buys bitcoins with PayPal, and then reverses their half of the transaction. This is commonly referred to as a chargeback.

Question 7: How difficult is it to make a Bitcoin payment?

Bitcoin payments are easier to make than debit or credit card purchases, and can be received without a merchant account. Payments are made from a wallet application, either on your computer or smartphone, by entering the recipient's address, the payment amount, and pressing send. To make it easier to enter a recipient's address, many wallets can obtain the address by scanning a QR code or touching two phones together with NFC technology.

Question 8: What are the advantages of Bitcoin?

- **Payment freedom -** It is possible to send and receive bitcoins anywhere in the world at any time. No bank holidays. No borders. No bureaucracy. Bitcoin allows its users to be in full control of their money.

- **Choose your own fees** - There is no fee to receive bitcoins, and many wallets let you control how large a fee to pay when spending. Higher fees can encourage faster confirmation of your transactions. Fees are unrelated to the amount transferred, so it's possible to send 100,000 bitcoins for the same fee it costs to send 1 bitcoin. Additionally, merchant processors exist to assist merchants in processing transactions, converting bitcoins to fiat currency and depositing funds directly into merchants' bank accounts daily. As these services are based on Bitcoin, they can be offered for much lower fees than with PayPal or credit card networks.
- **Fewer risks for merchants** - Bitcoin transactions are secure, irreversible, and do not contain customers' sensitive or personal information. This protects merchants from losses caused by fraud or fraudulent chargebacks, and there is no need for PCI compliance. Merchants can easily expand to new markets where either credit cards are not available or fraud rates are unacceptably high. The net results are lower fees, larger markets, and fewer administrative costs.
- **Security and control** - Bitcoin users are in full control of their transactions; it is impossible for merchants to force unwanted or unnoticed charges as can happen with other payment methods. Bitcoin payments can be made without personal information tied to the transaction. This offers strong protection against identity theft. Bitcoin users can also protect their money with backup and encryption.
- **Transparent and neutral** - All information concerning the Bitcoin money supply itself is readily available on the block chain for anybody to verify and use in real-time. No individual or organization can control or manipulate the Bitcoin protocol because it is cryptographically secure. This allows the core of Bitcoin to be trusted for being completely neutral, transparent and predictable.

Question 9: What are the disadvantages of Bitcoin?

- **Degree of acceptance -** Many people are still unaware of Bitcoin. Every day, more businesses accept bitcoins because they want the advantages of doing so, but the list remains small and still needs to grow in order to benefit from network effects.
- **Volatility** - The total value of bitcoins in circulation and the number of businesses using Bitcoin are still very small compared to what they could be. Therefore, relatively small events, trades, or business activities can significantly affect the price. In theory, this volatility will decrease as Bitcoin markets and the technology matures. Never before has the world seen a start-up currency, so it is truly difficult (and exciting) to imagine how it will play out.
- **Ongoing development** - Bitcoin software is still in beta with many incomplete features in active development. New tools, features, and services are being developed to make Bitcoin more secure and accessible to the masses. Some of these are still not ready for everyone. Most Bitcoin businesses are new and still offer no insurance. In general, Bitcoin is still in the process of maturing.

Question 10: Why do people trust Bitcoin?

Much of the trust in Bitcoin comes from the fact that it requires no trust at all. Bitcoin is fully open-source and decentralized. This means that anyone has access to the entire source code at any time. Any developer in the world can therefore verify exactly how Bitcoin works. All transactions and bitcoins issued into existence can be transparently consulted in real-time by anyone. All payments can be made without reliance on a third party and the whole system is protected by heavily peer-reviewed cryptographic algorithms like those used for online banking. No organization or individual can control Bitcoin, and the network remains secure even if not all of its users can be trusted.

Question 11: Can I make money with Bitcoin?

You should never expect to get rich with Bitcoin or any emerging technology. It is always important to be wary of anything that sounds too good to be true or disobeys basic economic rules.

Bitcoin is a growing space of innovation and there are business opportunities that also include risks. There is no guarantee that Bitcoin will continue to grow even though it has developed at a very fast rate so far. Investing time and resources on anything related to Bitcoin requires entrepreneurship. There are various ways to make money with Bitcoin such as mining, speculation or running new businesses. All of these methods are competitive and there is no guarantee of profit. It is up to each individual to make a proper evaluation of the costs and the risks involved in any such project.

Question 12: Is Bitcoin fully virtual and immaterial?

Bitcoin is as virtual as the credit cards and online banking networks people use everyday. Bitcoin can be used to pay online and in physical stores just like any other form of money. Bitcoins can also be exchanged in physical form such as the Casascius coins, but paying with a mobile phone usually remains more convenient. Bitcoin balances are stored in a large distributed network, and they cannot be fraudulently altered by anybody. In other words, Bitcoin users have exclusive control over their funds and bitcoins cannot vanish just because they are virtual.

Question 13: Is Bitcoin anonymous?

Bitcoin is designed to allow its users to send and receive payments with an acceptable level of privacy as well as any other form of money. However, Bitcoin is not anonymous and cannot offer the same level of privacy as cash. The use of Bitcoin leaves extensive public records. Various mechanisms exist to protect users' privacy, and more are in development. However, there is still work to be done before these features are used correctly by most Bitcoin users.

Some concerns have been raised that private transactions could be used for illegal purposes with Bitcoin. However, it is worth noting that Bitcoin will undoubtedly be subjected to similar regulations that are already in place inside existing financial systems. Bitcoin cannot be more anonymous than cash and it is not likely to prevent criminal investigations from being conducted. Additionally, Bitcoin is also designed to prevent a large range of financial crimes.

Question 14: What happens when bitcoins are lost?

When a user loses his wallet, it has the effect of removing money out of circulation. Lost bitcoins still remain in the block chain just like any other bitcoins. However, lost bitcoins remain dormant forever because there is no way for anybody to find the private key(s) that would allow them to be spent again. Because of the law of supply and demand, when fewer bitcoins are available, the ones that are left will be in higher demand and increase in value to compensate.

Question 15: Can Bitcoin scale to become a major payment network?

The Bitcoin network can already process a much higher number of transactions per second than it does today. It is, however, not entirely ready to scale to the level of major credit card networks. Work is underway to lift current limitations, and future requirements are well known. Since inception, every aspect of the Bitcoin network has been in a continuous process of maturation, optimization, and specialization, and it should be expected to remain that way for some years to come. As traffic grows, more Bitcoin users may use lightweight clients, and full network nodes may become a more specialized service. For more details, see the Scalability page on the Wiki.

Question 16: Is Bitcoin legal?

To the best of our knowledge, Bitcoin has not been made illegal by legislation in most jurisdictions. However, some jurisdictions (such as Argentina and Russia) severely restrict or ban foreign currencies. Other jurisdictions (such as Thailand) may limit the licensing of certain entities such as Bitcoin exchanges.

Regulators from various jurisdictions are taking steps to provide individuals and businesses with rules on how to integrate this new technology with the formal, regulated financial system. For example, the Financial Crimes Enforcement Network (FinCEN), a bureau in the United States Treasury Department, issued non-binding guidance on how it characterizes certain activities involving virtual currencies.

Question 17: Is Bitcoin useful for illegal activities?

Bitcoin is money, and money has always been used both for legal and illegal purposes. Cash, credit cards and current banking systems widely surpass Bitcoin in terms of their use to finance crime. Bitcoin can bring significant innovation in payment systems and the benefits of such innovation are often considered to be far beyond their potential drawbacks.

Bitcoin is designed to be a huge step forward in making money more secure and could also act as a significant protection against many forms of financial crime. For instance, bitcoins are completely impossible to counterfeit. Users are in full control of their payments and cannot receive unapproved charges such as with credit card fraud. Bitcoin transactions are irreversible and immune to fraudulent chargebacks. Bitcoin allows money to be secured against theft and loss using very strong and useful mechanisms such as backups, encryption, and multiple signatures.

Some concerns have been raised that Bitcoin could be more attractive to criminals because it can be used to make private and irreversible payments. However, these features already exist with cash and

wire transfer, which are widely used and well-established. The use of Bitcoin will undoubtedly be subjected to similar regulations that are already in place inside existing financial systems, and Bitcoin is not likely to prevent criminal investigations from being conducted. In general, it is common for important breakthroughs to be perceived as being controversial before their benefits are well understood. The Internet is a good example among many others to illustrate this.

Question 18: Can Bitcoin be regulated?

The Bitcoin protocol itself cannot be modified without the cooperation of nearly all its users, who choose what software they use. Attempting to assign special rights to a local authority in the rules of the global Bitcoin network is not a practical possibility. Any rich organization could choose to invest in mining hardware to control half of the computing power of the network and become able to block or reverse recent transactions. However, there is no guarantee that they could retain this power since this requires to invest as much than all other miners in the world.

It is however possible to regulate the use of Bitcoin in a similar way to any other instrument. Just like the dollar, Bitcoin can be used for a wide variety of purposes, some of which can be considered legitimate or not as per each jurisdiction's laws. In this regard, Bitcoin is no different than any other tool or resource and can be subjected to different regulations in each country. Bitcoin use could also be made difficult by restrictive regulations, in which case it is hard to determine what percentage of users would keep using the technology. A government that chooses to ban Bitcoin would prevent domestic businesses and markets from developing, shifting innovation to other countries. The challenge for regulators, as always, is to develop efficient solutions while not impairing the growth of new emerging markets and businesses.

Question 19: What about Bitcoin and taxes?

Bitcoin is not a fiat currency with legal tender status in any jurisdiction, but often tax liability accrues regardless of the medium used. There is a wide variety of legislation in many different jurisdictions which could cause income, sales, payroll, capital gains, or some other form of tax liability to arise with Bitcoin.

Question 20: What about Bitcoin and consumer protection?

Bitcoin is freeing people to transact on their own terms. Each user can send and receive payments in a similar way to cash but they can also take part in more complex contracts. Multiple signatures allow a transaction to be accepted by the network only if a certain number of a defined group of persons agree to sign the transaction. This allows innovative dispute mediation services to be developed in the future. Such services could allow a third party to approve or reject a transaction in case of disagreement between the other parties without having control on their money. As opposed to cash and other payment methods, Bitcoin always leaves a public proof that a transaction did take place, which can potentially be used in a recourse against businesses with fraudulent practices.

It is also worth noting that while merchants usually depend on their public reputation to remain in business and pay their employees, they don't have access to the same level of information when dealing with new consumers. The way Bitcoin works allows both individuals and businesses to be protected against fraudulent chargebacks while giving the choice to the consumer to ask for more protection when they are not willing to trust a particular merchant.

Question 21: How are bitcoins created?

New bitcoins are generated by a competitive and decentralized process called "mining". This process involves that individuals are rewarded by the network for their services. Bitcoin miners are processing transactions and securing the network using specialized hardware and are collecting new bitcoins in exchange.

The Bitcoin protocol is designed in such a way that new bitcoins are created at a fixed rate. This makes Bitcoin mining a very competitive business. When more miners join the network, it becomes increasingly difficult to make a profit and miners must seek efficiency to cut their operating costs. No central authority or developer has any power to control or manipulate the system to increase their profits. Every Bitcoin node in the world will reject anything that does not comply with the rules it expects the system to follow.

Bitcoins are created at a decreasing and predictable rate. The number of new bitcoins created each year is automatically halved over time until bitcoin issuance halts completely with a total of 21 million bitcoins in existence. At this point, Bitcoin miners will probably be supported exclusively by numerous small transaction fees.

Question 22: Why do bitcoins have value?

Bitcoins have value because they are useful as a form of money. Bitcoin has the characteristics of money (durability, portability, fungibility, scarcity, divisibility, and recognizability) based on the properties of mathematics rather than relying on physical properties (like gold and silver) or trust in central authorities (like fiat currencies). In short, Bitcoin is backed by mathematics. With these attributes, all that is required for a form of money to hold value is trust and adoption. In the case of Bitcoin, this can

be measured by its growing base of users, merchants, and startups. As with all currency, bitcoin's value comes only and directly from people willing to accept them as payment.

Question 23: What determines bitcoin's price?

The price of a bitcoin is determined by supply and demand. When demand for bitcoins increases, the price increases, and when demand falls, the price falls. There is only a limited number of bitcoins in circulation and new bitcoins are created at a predictable and decreasing rate, which means that demand must follow this level of inflation to keep the price stable. Because Bitcoin is still a relatively small market compared to what it could be, it doesn't take significant amounts of money to move the market price up or down, and thus the price of a bitcoin is still very volatile.

Question 24: Can bitcoins become worthless?

Yes. History is littered with currencies that failed and are no longer used, such as the German Mark during the Weimar Republic and, more recently, the Zimbabwean dollar. Although previous currency failures were typically due to hyperinflation of a kind that Bitcoin makes impossible, there is always potential for technical failures, competing currencies, political issues and so on. As a basic rule of thumb, no currency should be considered absolutely safe from failures or hard times. Bitcoin has proven reliable for years since its inception and there is a lot of potential for Bitcoin to continue to grow. However, no one is in a position to predict what the future will be for Bitcoin.

Question 25: Is Bitcoin a bubble?

A fast rise in price does not constitute a bubble. An artificial over-valuation that will lead to a sudden downward correction constitutes a bubble. Choices based on individual human action by hundreds of thousands of market participants is the cause for bitcoin's price to fluctuate as the market seeks price discovery. Reasons for changes in sentiment may include a loss of confidence in Bitcoin, a large

difference between value and price not based on the fundamentals of the Bitcoin economy, increased press coverage stimulating speculative demand, fear of uncertainty, and old-fashioned irrational exuberance and greed.

Question 26: Is Bitcoin a Ponzi scheme?

A Ponzi scheme is a fraudulent investment operation that pays returns to its investors from their own money, or the money paid by subsequent investors, instead of from profit earned by the individuals running the business. Ponzi schemes are designed to collapse at the expense of the last investors when there is not enough new participants.

Bitcoin is a free software project with no central authority. Consequently, no one is in a position to make fraudulent representations about investment returns. Like other major currencies such as gold, United States dollar, euro, yen, etc. there is no guaranteed purchasing power and the exchange rate floats freely. This leads to volatility where owners of bitcoins can unpredictably make or lose money. Beyond speculation, Bitcoin is also a payment system with useful and competitive attributes that are being used by thousands of users and businesses.

Question 27: Doesn't Bitcoin unfairly benefit early adopters?

Some early adopters have large numbers of bitcoins because they took risks and invested time and resources in an unproven technology that was hardly used by anyone and that was much harder to secure properly. Many early adopters spent large numbers of bitcoins quite a few times before they became valuable or bought only small amounts and didn't make huge gains. There is no guarantee that the price of a bitcoin will increase or drop. This is very similar to investing in an early startup that can either gain value through its usefulness and popularity, or just never break through. Bitcoin is still in its

infancy, and it has been designed with a very long-term view; it is hard to imagine how it could be less biased towards early adopters, and today's users may or may not be the early adopters of tomorrow.

Question 28: Won't the finite amount of bitcoins be a limitation?

Bitcoin is unique in that only 21 million bitcoins will ever be created. However, this will never be a limitation because transactions can be denominated in smaller sub-units of a bitcoin, such as bits - there are 1,000,000 bits in 1 bitcoin. Bitcoins can be divided up to 8 decimal places (0.000 000 01) and potentially even smaller units if that is ever required in the future as the average transaction size decreases.

Question 29: Won't Bitcoin fall in a deflationary spiral?

The deflationary spiral theory says that if prices are expected to fall, people will move purchases into the future in order to benefit from the lower prices. That fall in demand will in turn cause merchants to lower their prices to try and stimulate demand, making the problem worse and leading to an economic depression.

Although this theory is a popular way to justify inflation amongst central bankers, it does not appear to always hold true and is considered controversial amongst economists. Consumer electronics is one example of a market where prices constantly fall but which is not in depression. Similarly, the value of bitcoins has risen over time and yet the size of the Bitcoin economy has also grown dramatically along with it. Because both the value of the currency and the size of its economy started at zero in 2009, Bitcoin is a counterexample to the theory showing that it must sometimes be wrong.

Notwithstanding this, Bitcoin is not designed to be a deflationary currency. It is more accurate to say Bitcoin is intended to inflate in its early years, and become stable in its later years. The only time the quantity of bitcoins in circulation will drop is if people carelessly lose their wallets by failing to make backups. With a stable monetary base and a stable economy, the value of the currency should remain the same.

Question 30: Isn't speculation and volatility a problem for Bitcoin?

This is a chicken and egg situation. For bitcoin's price to stabilize, a large scale economy needs to develop with more businesses and users. For a large scale economy to develop, businesses and users will seek for price stability.

Fortunately, volatility does not affect the main benefits of Bitcoin as a payment system to transfer money from point A to point B. It is possible for businesses to convert bitcoin payments to their local currency instantly, allowing them to profit from the advantages of Bitcoin without being subjected to price fluctuations. Since Bitcoin offers many useful and unique features and properties, many users choose to use Bitcoin. With such solutions and incentives, it is possible that Bitcoin will mature and develop to a degree where price volatility will become limited.

Question 31: What if someone bought up all the existing bitcoins?

Only a fraction of bitcoins issued to date are found on the exchange markets for sale. Bitcoin markets are competitive, meaning the price of a bitcoin will rise or fall depending on supply and demand. Additionally, new bitcoins will continue to be issued for decades to come. Therefore even the most determined buyer could not buy all the bitcoins in existence. This situation isn't to suggest, however, that the markets aren't vulnerable to price manipulation; it still doesn't take significant amounts of money to move the market price up or down, and thus Bitcoin remains a volatile asset thus far.

Question 32: What if someone creates a better digital currency?

That can happen. For now, Bitcoin remains by far the most popular decentralized virtual currency, but there can be no guarantee that it will retain that position. There is already a set of alternative currencies inspired by Bitcoin. It is however probably correct to assume that significant improvements would be required for a new currency to overtake Bitcoin in terms of established market, even though this remains unpredictable. Bitcoin could also conceivably adopt improvements of a competing currency so long as it doesn't change fundamental parts of the protocol.

Question 33: Why do I have to wait for confirmation?

Receiving notification of a payment is almost instant with Bitcoin. However, there is a delay before the network begins to confirm your transaction by including it in a block. A confirmation means that there is a consensus on the network that the bitcoins you received haven't been sent to anyone else and are considered your property. Once your transaction has been included in one block, it will continue to be buried under every block after it, which will exponentially consolidate this consensus and decrease the risk of a reversed transaction. Each confirmation takes between a few seconds and 90 minutes, with 10 minutes being the average. If the transaction pays too low a fee or is otherwise atypical, getting the first confirmation can take much longer. Every user is free to determine at what point they consider a transaction sufficiently confirmed, but 6 confirmations is often considered to be as safe as waiting 6 months on a credit card transaction.

Question 34: How much will the transaction fee be?

Transactions can be processed without fees, but trying to send free transactions can require waiting days or weeks. Although fees may increase over time, normal fees currently only cost a tiny amount. By default, all Bitcoin wallets listed on Bitcoin.org add what they think is an appropriate fee to your

transactions; most of those wallets will also give you chance to review the fee before sending the transaction.

Transaction fees are used as a protection against users sending transactions to overload the network and as a way to pay miners for their work helping to secure the network. The precise manner in which fees work is still being developed and will change over time. Because the fee is not related to the amount of bitcoins being sent, it may seem extremely low or unfairly high. Instead, the fee is relative to the number of bytes in the transaction, so using multisig or spending multiple previously-received amounts may cost more than simpler transactions. If your activity follows the pattern of conventional transactions, you won't have to pay unusually high fees.

Question 35: What if I receive a bitcoin when my computer is powered off?

This works fine. The bitcoins will appear next time you start your wallet application. Bitcoins are not actually received by the software on your computer, they are appended to a public ledger that is shared between all the devices on the network. If you are sent bitcoins when your wallet client program is not running and you later launch it, it will download blocks and catch up with any transactions it did not already know about, and the bitcoins will eventually appear as if they were just received in real time. Your wallet is only needed when you wish to spend bitcoins.

Question 36: What does "synchronizing" mean and why does it take so long?

Long synchronization time is only required with full node clients like Bitcoin Core. Technically speaking, synchronizing is the process of downloading and verifying all previous Bitcoin transactions on the network. For some Bitcoin clients to calculate the spendable balance of your Bitcoin wallet and make new transactions, it needs to be aware of all previous transactions. This step can be resource intensive and requires sufficient bandwidth and storage to accommodate the full size of the block chain. For

Bitcoin to remain secure, enough people should keep using full node clients because they perform the task of validating and relaying transactions.

Question 37: What is Bitcoin mining?

Mining is the process of spending computing power to process transactions, secure the network, and keep everyone in the system synchronized together. It can be perceived like the Bitcoin data center except that it has been designed to be fully decentralized with miners operating in all countries and no individual having control over the network. This process is referred to as "mining" as an analogy to gold mining because it is also a temporary mechanism used to issue new bitcoins. Unlike gold mining, however, Bitcoin mining provides a reward in exchange for useful services required to operate a secure payment network. Mining will still be required after the last bitcoin is issued.

Question 38: How does Bitcoin mining work?

Anybody can become a Bitcoin miner by running software with specialized hardware. Mining software listens for transactions broadcast through the peer-to-peer network and performs appropriate tasks to process and confirm these transactions. Bitcoin miners perform this work because they can earn transaction fees paid by users for faster transaction processing, and newly created bitcoins issued into existence according to a fixed formula.

For new transactions to be confirmed, they need to be included in a block along with a mathematical proof of work. Such proofs are very hard to generate because there is no way to create them other than by trying billions of calculations per second. This requires miners to perform these calculations before their blocks are accepted by the network and before they are rewarded. As more people start to mine, the difficulty of finding valid blocks is automatically increased by the network to ensure that the average

time to find a block remains equal to 10 minutes. As a result, mining is a very competitive business where no individual miner can control what is included in the block chain.

The proof of work is also designed to depend on the previous block to force a chronological order in the block chain. This makes it exponentially difficult to reverse previous transactions because this requires the recalculation of the proofs of work of all the subsequent blocks. When two blocks are found at the same time, miners work on the first block they receive and switch to the longest chain of blocks as soon as the next block is found. This allows mining to secure and maintain a global consensus based on processing power.

Bitcoin miners are neither able to cheat by increasing their own reward nor process fraudulent transactions that could corrupt the Bitcoin network because all Bitcoin nodes would reject any block that contains invalid data as per the rules of the Bitcoin protocol. Consequently, the network remains secure even if not all Bitcoin miners can be trusted.

Question 39: Isn't Bitcoin mining a waste of energy?

Spending energy to secure and operate a payment system is hardly a waste. Like any other payment service, the use of Bitcoin entails processing costs. Services necessary for the operation of currently widespread monetary systems, such as banks, credit cards, and armored vehicles, also use a lot of energy. Although unlike Bitcoin, their total energy consumption is not transparent and cannot be as easily measured.

Bitcoin mining has been designed to become more optimized over time with specialized hardware consuming less energy, and the operating costs of mining should continue to be proportional to demand. When Bitcoin mining becomes too competitive and less profitable, some miners choose to stop their activities. Furthermore, all energy expended mining is eventually transformed into heat, and the

most profitable miners will be those who have put this heat to good use. An optimally efficient mining network is one that isn't actually consuming any extra energy. While this is an ideal, the economics of mining are such that miners individually strive toward it.

Question 40: How does mining help secure Bitcoin?

Mining creates the equivalent of a competitive lottery that makes it very difficult for anyone to consecutively add new blocks of transactions into the block chain. This protects the neutrality of the network by preventing any individual from gaining the power to block certain transactions. This also prevents any individual from replacing parts of the block chain to roll back their own spends, which could be used to defraud other users. Mining makes it exponentially more difficult to reverse a past transaction by requiring the rewriting of all blocks following this transaction.

Question 41: What do I need to start mining?

In the early days of Bitcoin, anyone could find a new block using their computer's CPU. As more and more people started mining, the difficulty of finding new blocks increased greatly to the point where the only cost-effective method of mining today is using specialized hardware. You can visit BitcoinMining.com for more information.

Question 42: Is Bitcoin secure?

The Bitcoin technology - the protocol and the cryptography - has a strong security track record, and the Bitcoin network is probably the biggest distributed computing project in the world. Bitcoin's most common vulnerability is in user error. Bitcoin wallet files that store the necessary private keys can be accidentally deleted, lost or stolen. This is pretty similar to physical cash stored in a digital form. Fortunately, users can employ sound security practices to protect their money or use service providers that offer good levels of security and insurance against theft or loss.

Question 43: Hasn't Bitcoin been hacked in the past?

The rules of the protocol and the cryptography used for Bitcoin are still working years after its inception, which is a good indication that the concept is well designed. However, security flaws have been found and fixed over time in various software implementations. Like any other form of software, the security of Bitcoin software depends on the speed with which problems are found and fixed. The more such issues are discovered, the more Bitcoin is gaining maturity.

There are often misconceptions about thefts and security breaches that happened on diverse exchanges and businesses. Although these events are unfortunate, none of them involve Bitcoin itself being hacked, nor imply inherent flaws in Bitcoin; just like a bank robbery doesn't mean that the dollar is compromised. However, it is accurate to say that a complete set of good practices and intuitive security solutions is needed to give users better protection of their money, and to reduce the general risk of theft and loss. Over the course of the last few years, such security features have quickly developed, such as wallet encryption, offline wallets, hardware wallets, and multi-signature transactions.

Question 44: Could users collude against Bitcoin?

It is not possible to change the Bitcoin protocol that easily. Any Bitcoin client that doesn't comply with the same rules cannot enforce their own rules on other users. As per the current specification, double spending is not possible on the same block chain, and neither is spending bitcoins without a valid signature. Therefore, It is not possible to generate uncontrolled amounts of bitcoins out of thin air, spend other users' funds, corrupt the network, or anything similar.

However, powerful miners could arbitrarily choose to block or reverse recent transactions. A majority of users can also put pressure for some changes to be adopted. Because Bitcoin only works correctly with a complete consensus between all users, changing the protocol can be very difficult and requires an

overwhelming majority of users to adopt the changes in such a way that remaining users have nearly no choice but to follow. As a general rule, it is hard to imagine why any Bitcoin user would choose to adopt any change that could compromise their own money.

Question 45: Is Bitcoin vulnerable to quantum computing?

Yes, most systems relying on cryptography in general are, including traditional banking systems. However, quantum computers don't yet exist and probably won't for a while. In the event that quantum computing could be an imminent threat to Bitcoin, the protocol could be upgraded to use post-quantum algorithms. Given the importance that this update would have, it can be safely expected that it would be highly reviewed by developers and adopted by all Bitcoin users.

SOURCE: Bitcoin Project (2017), 'Frequently Asked Questions about Bitcoin', Available at: https://bitcoin.org/en/faq (accessed 15 January 2017).

APPENDIX 2

ABOUT THE AUTHOR

Ehi is a Senior Associate within Deji Sasegbon (SAN) and Co. He also heads the publishing team. His areas of expertise includes amongst others: comparative law, money laundering law, international banking law, energy law, intellectual property law and criminal law.

Ehi has authored more than 10 publications, including three books on Money Laundering Law/Banking Law. Ehi's second book titled 'The Risk-Based Approach to Combating Money Laundering and Terrorist Financing' has been cited by other publications. Notable amongst them is Exposing Fraud: Skills, Process and Practicalities (Wiley Corporate F&A) Dec 2, 2015 by Ian Ross.

Ehi was recently listed among the contributors for the new KYC360 website (the world's leading platform for anti-money laundering professionals). Ehi Contributes articles, webinars and podcasts to the website. Ehi's most recent article titled 'Balancing Anti-Money Laundering/Counter-Terrorist Financing Requirements and Financial Inclusion for Migrants: A Case Study of Germany' has been endorsed by professionals in the Anti-Money Laundering Industry.

Ehi completed his undergraduate studies at the University of Lagos, postgraduate studies at Cardiff University and his professional course on Money Laundering Law at the University of Manchester.

Ehi intends to further his education with a PhD Degree in Law. His proposal has already been approved by the University of Exeter.

Ehi is a member of the Industry's Largest International Network of Financial Crime Detection and Prevention Professionals (ACAMS). His Membership number is 1000157079. The Membership provides

Ehi access to exclusive anti money laundering publications, continuing education and training, networking and professional growth.

Ehi received an award from the Top Executives in the Law, Legal & Information Services Industry for his publications in the legal world.

Ehi has upcoming publications with the Journal of Money Laundering Control: Emerald Insight.

Ehi has been invited by numerous scholarly journals to peer review research articles.

Ehi has been involved in many extra-curricular activities. In December 2012, Ehi worked with Cardiff Digs/Environmental Champions as a Student Volunteer on a variety of projects. The projects focused on waste and recycling, housing and energy efficiency, sustainable travel, fair-trade, environmental tasks including river clean ups, green police and much more. In August 2013, Ehi registered as a Millennium Volunteer (MV) in the Placement Program organised by Cardiff Digs/Environmental Champions and received a 50 hours certificate by the Welsh Government to that effect.

For more information on Ehi visit: http://www.amazon.com/Ehi-Eric-Esoimeme-Esq/e/B00OESQ4VS

Follow Ehi on LinkedIn: https://ng.linkedin.com/pub/ehi-esoimeme/70/912/b3b

Download Ehi's Articles here: http://ssrn.com/author=2237772