PANTERA
PRIMER

March 11th, 2014

Ronald A. Glantz
Director of Research

WHAT IS BITCOIN?

Bitcoin is a consensus network that enables a new payment system and completely digital currency. 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 can be considered to be cash for the Internet. Bitcoin can also be seen as the most prominent triple entry bookkeeping system in existence. While there are or have been at least 110 other digital currencies, Bitcoin accounts for 77% of the market value of all digital currencies and an even higher percentage of digital currency users.

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. Behind the scenes, the Bitcoin network shares 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 with 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". An address is like a bank account into which a user can receive, store, and send bitcoins. Instead of being physically secured in a vault, bitcoins are secured with public-key cryptography. Each address consists of a public key, which is published, and a private key, which the owner must keep secret. Anyone can send bitcoins to any public key, but only the person with the private key can spend them. While addresses are public, nobody knows which addresses belong to which people; Bitcoin addresses are pseudonymous. After depositing your bitcoins into a “wallet”, the wallet alerts (“broadcasts”) every other user of bitcoins that it contains bitcoins. This information is incorporated into the block chain. The wallet generates a public key accessible to anyone and a private key (unless your wallet is on an exchange, such as Bitstamp) or address that authorizes sending bitcoins to other public addresses. If you want to, say, purchase a flight on Virgin Galactic, you contact them, make a user account (e.g., your name), and then tell them that payment will come from your public key. You then go to your wallet or exchange and broadcast the amount from your public key to their public key. This is published on a peer-to-peer

network which validates it against the sender's public key, checks that the sending address's balance is sufficient, and propagates it to all of the other nodes on the network. The transaction is eventually received by a miner, who incorporates the transaction into a block. This block is then flooded into the network and is incorporated into the global block chain. The bitcoins now belong to Virgin Galactic's public key.

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.

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 near field communication (NFC) technology.

WHAT ARE THE ADVANTAGES OF BITCOIN?

- Payment freedom – It is possible to send and receive any amount of money instantly anywhere in the world at any time. No bank holidays. No borders. No imposed limits. Bitcoin allows its users to be in full control of their money.
- Very low fees – Bitcoin payments are currently processed with either no fees or extremely small fees. Users may include fees with transactions to receive priority processing, which results in faster confirmation of transactions by the network. In addition, services 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.
- Attractive for microtransactions – Because the fees are so low, bitcoins can be used in transactions that are economically unattractive for most merchants, especially in developing countries.
- 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 payment card industry 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.

CAN BITCOIN LEAD TO NEW BUSINESSES?

One of the most exciting things about Bitcoin is that its block chain ledger system is a potential category killer in recording ownership (real estate titles, stock and bond certificates, etc.). This could lead to new ways of doing business, such as keeping records of wagers and legal documents. The puzzle of attempting to solve the problems of smart property, smart contracts, and decentralized autonomous organizations (DOA) is how interest in next-generation cryptocurrency protocols originally started.

Examples of next-generation block chains include:

- Smart multi-signature escrow services
- Financial derivatives
- Identity and reputation systems
- DOA's
- Savings wallets
- Crop insurance
- Decentralized (yet managed) data feeds
- Peer-to-peer gambling
- On-chain stock market transactions
- On-chain decentralized marketplace
- Decentralized dropboxes
- Sub-currencies

The most ambitious of all cited applications is the concept of DAO's -- autonomous entities that operate on the block chain without any central control, avoiding all dependence on legal contracts

and organizational bylaws in favor of having resources and funds autonomously managed by a self-enforcing smart contract on a cryptographic block chain.

There does not seem to be a need to create a new currency, or even a new protocol, when the problem can be solved entirely by using existing technologies. While a planned update to the Bitcoin protocol (Version 0.9) does allow for limited data use within transactions, the scripting systems intrinsic to Bitcoin are currently far too limited to allow the kind of arbitrarily complex computation that DAO's require.

WHAT ARE THE DISADVANTAGES OF BITCOIN?

- 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. 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 digital currency, so it is difficult to forecast 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 maturing.

WHY DO PEOPLE TRUST BITCOIN?

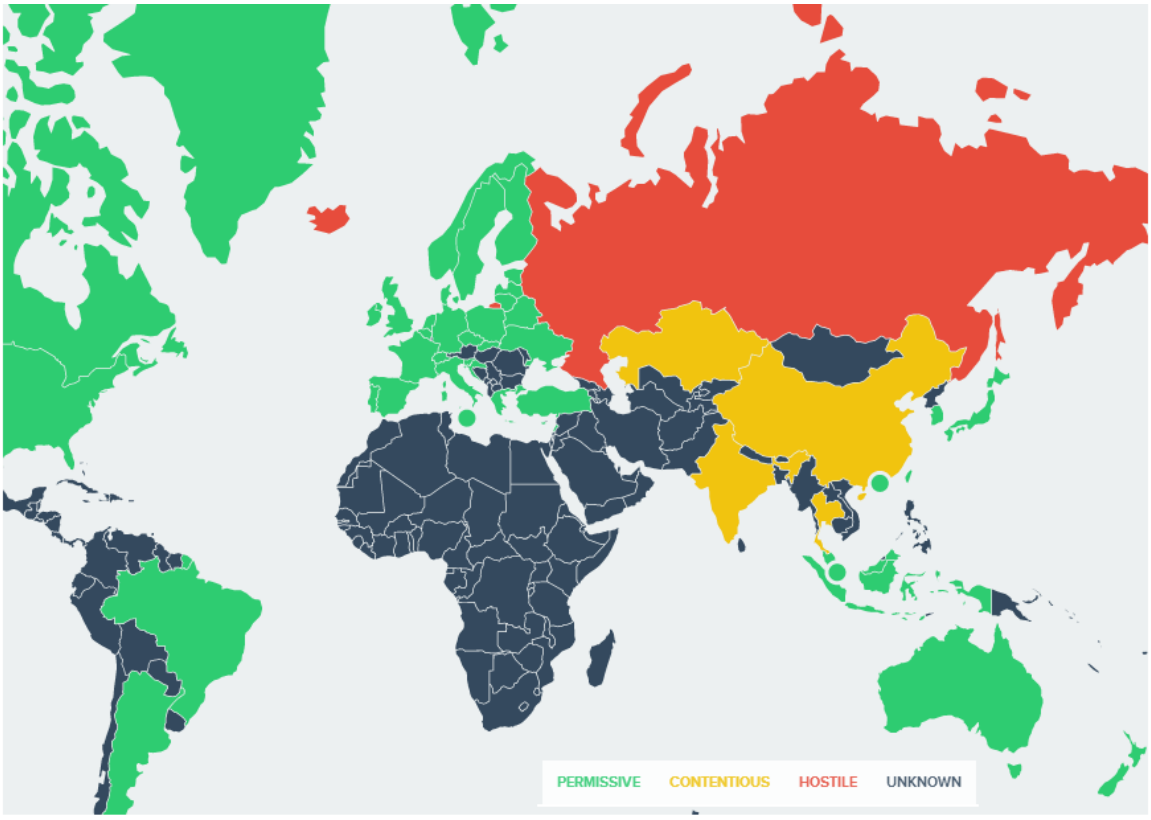
Much of the trust in Bitcoin comes from the fact that it requires no trust at all. Bitcoin is fully open-source and decentralized. This means that anyone has access to the entire source code at any time. Any developer in the world can verify exactly how Bitcoin works. All transactions and bitcoins issued 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.

IS BITCOIN FULLY VIRTUAL AND IMMATERIAL?

Bitcoin is as virtual as the credit card and online banking networks people use every day. 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.

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. In addition, Bitcoin is designed to prevent a large range of financial crimes.
As of February 17, 2014, 42 countries are considered “permissive”, five are “contentious”, and only Russia and Iceland are hostile.



WHAT HAPPENS WHEN BITCOINS ARE LOST?

When a user loses his Bitcoin wallet, it is the same as losing a conventional wallet. 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.

CAN BITCOIN SCALE TO BECOME A MAJOR PAYMENT NETWORK?

The Bitcoin network can 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.

IS BITCOIN LEGAL?

To the best of our knowledge, Bitcoin has not been made illegal by legislation in any jurisdiction. However, some jurisdictions (such as Argentina) severely restrict or ban all foreign currency. 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.

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 appear to be 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.

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 investing more than all of the 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.

WHAT ABOUT 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 that could cause income, sales, payroll, capital gains, or some other form of tax liability to arise with Bitcoin. There is currently no U.S. legislation and several countries (e.g., Germany and Slovenia) have exempted bitcoins from taxation.

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 leave a public proof that a transaction did take place, which can potentially be used in 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.

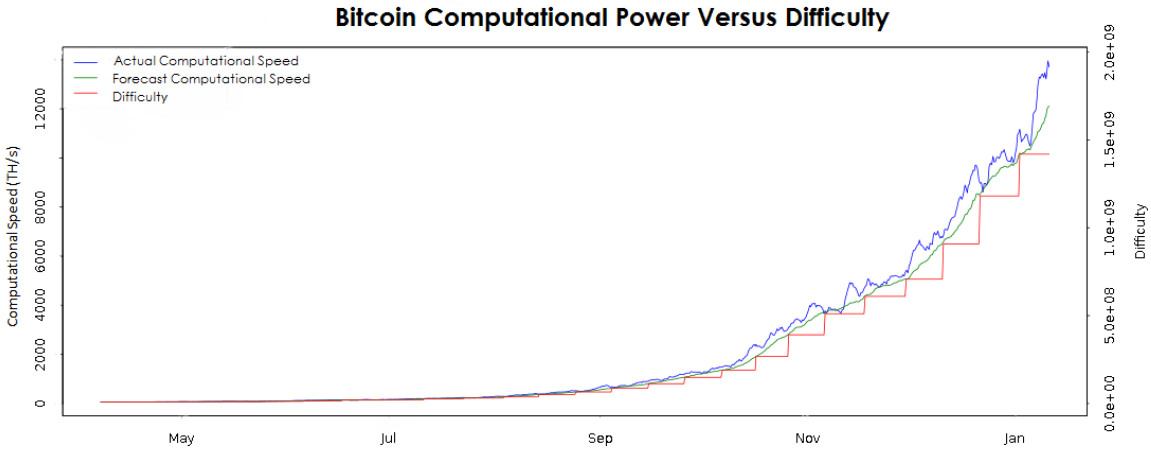
HOW ARE BITCOINS CREATED?

New bitcoins are generated by a competitive and decentralized process called "mining". This process involves individuals being 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 every 10 minutes at a decreasing and predictable rate. The number of new bitcoins created is automatically halved over time until issuance halts when there are 21 million bitcoins in existence. From January 2009 to November 2012, the reward was 50 bitcoins, resulting in 10,500,000 being created (210,000 blocks). The current reward is 25 bitcoins, so that 5,250,000 will be created in years 5-8. That quantity will halve to 12.5, so that it will be 2,625,000 in years 9-12, and so on. At this point, Bitcoin miners will probably be supported exclusively by numerous small transaction fees.

The developers of Bitcoin wrote a computer code designed to release new coins every 10 minutes. This was done by automatically adjusting a "proof of work" problem after every 2,016 blocks, based on the time it took to solve the previous set. In theory, the rate is adjusted every two weeks (20,160 minutes), although this happens faster if processing power is added to the network during the period. Miners originally used the CPU's in normal PC's, but it wasn't long before an arms race began. CPU's were supplanted by faster Graphics Processing Units, which in turn transitioned to Field Programmable Gate Arrays configured to run the algorithm and, more recently, to Application Specific Integrated Circuits hardwired in the foundry to carry out the algorithm. The brilliance of the original concept is demonstrated by the following chart, showing that the time to mine is staying steady despite an acceleration in computational speed since September 2013.



As additional computational power is brought on, the likelihood of any particular miner or group of miners controlling a significant share of the processing power decreases. This, in turn, increases the overall strength of Bitcoin's decentralized nature.

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, store of value, 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 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.

WHAT DETERMINES BITCOIN'S PRICE?

Like other currencies, 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 are 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.

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.

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. One final point – bubbles always involve leveraged purchases. Unlike real estate or securities, all bitcoin purchases are fully funded.

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 are 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, the 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.

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.

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 bitcoins can be divided up to eight decimal places (0.00000001 BTC, called

Satoshi, in honor of Satoshi Nakamoto, the pseudonym of the inventor of Bitcoin), and potentially even smaller units if more than 21 trillion are ever required. As the average transaction size decreases, transactions can be denominated in sub-units of a bitcoin, such as millibitcoins (1 mBTC or 0.001 BTC).

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 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 among central bankers, it does not appear to always hold true and is considered controversial among 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.

ISN'T SPECULATION AND VOLATILITY A PROBLEM?

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 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. When that happens, bitcoins will be valued more for transactions than as a store of value.

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. In additional, 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 volatile; it still doesn't take significant amounts of money to move the market price up or down.

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 as long as it doesn't change fundamental parts of the protocol.

WHY DO I HAVE TO WAIT 10 MINUTES FOR A TRANSACTION?

Receiving a payment is almost instantaneous with Bitcoin. However, there is a 10 minute delay on average before the network begins to confirm your transaction by including it in a block and before you can spend the bitcoins you receive. 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. Every user is free to determine at what point they consider a transaction confirmed, but six confirmations are safer than waiting three months on a credit card transaction.

HOW MUCH WILL THE TRANSACTION FEE BE?

Most transactions can be processed without fees, but users are encouraged to pay a small voluntary fee for faster confirmation of their transactions and to remunerate miners. When fees are required, they generally don't exceed a few pennies in value. Your Bitcoin client will usually try to estimate an appropriate fee, when required.

Transaction fees are used as a protection against users sending transactions to overload 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 (0.0005 BTC for a 1,000 BTC transfer) or unfairly high (0.004 BTC for a 0.02 BTC payment). The fee is defined by attributes such as data in transaction and transaction recurrence. For example, if you are receiving a large number of tiny amounts, then fees for sending will be higher. Such payments are comparable to paying a restaurant bill using only pennies. Spending small fractions of your bitcoins rapidly may also require a fee. If your activity follows the pattern of conventional transactions, the fees should remain very low.

WHAT IF I RECEIVE A BITCOIN WHEN MY COMPUTER IS POWERED OFF?

Bitcoins will appear the 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.

WHAT DOES "SYNCHRONIZING" MEAN AND WHY DOES IT TAKE SO LONG?

Long synchronization time is only required with full node clients like Bitcoin-Qt. 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 must keep using full node clients because they perform the task of validating and relaying transactions.

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.

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 as well as 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.

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. Also, Bitcoin doesn't require an expensive Federal Reserve System ($5.1 billion), Secret Service ($1.4 billion), or Bureau of Engraving and Printing ($0.8 billion).

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.

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 spending, 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.

WHAT DO I NEED TO START MINING?

In the early days of Bitcoin, anyone could find a new block using their computer's central processing unit (CPU). Next, miners used video game graphic cards and then to pin grid array (PGA) boards.

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. Adoption of application-specific integrated circuits (ASIC) customized for bitcoin mining has recently had a noticeable increase in the speed of bitcoin issuance.

IS BITCOIN SECURE?

The Bitcoin protocol uses the strongest algorithms used by the NSA for encrypting Secret-level documents. Anyone can generate as many addresses as they want for free. There are approximately as many possible Bitcoin addresses are there are atoms in the Earth, so generating duplicate addresses (and thus having access to someone else's funds) is practically impossible. Most Bitcoin users maintain a number of addresses, stored in a digital wallet.

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 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.

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.

On the whole, the cryptographic and game-theoretical foundations behind the Bitcoin system have proven to be rock solid, and the fact that no one has yet claimed the $140 million reward for breaking these foundations is a testament to this. To the average user, there are only two ways to lose one's bitcoins to malicious activity: entrust the bitcoins to a third party service that turns out to itself be insecure or fraudulent, or have your own computer get hacked by a computer virus – both of which are problems in the traditional financial system as well, costing the U.S. economy $50 billion per year.

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, a majority of 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.

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.