BITCOINS AND THE CRYPTO CURRENCIES: MONETARY CHALLENGE FROM THE CYBERSPACE

Thejaka Perera
Assistant Vice President - Litigation, DFCC Bank

The cyberspace has paved way for a variety of community dependent concepts. They include social media, social networking, encyclopedias built and maintained by the society and sometimes social vigilantes.

The traditional institutions created by the society are challenged by the trends and establishments emerging as a result of the cyberspace. The cable TV is being replaced by the YouTube, Everybody uses the Wikipedia and The Encyclopedia Britannica is not being printed any more, Facebook is challenging the basic social interactions.

Will the traditional currency system be challenged by its alternative in the cyberspace? Who would have thought that the cyberspace would create its own variant of money or the currency that is governed by the internet community?

The crypto-currencies are that variant and the Bitcoin is the most famous of them all.

Bitcoin is a new type of money that is completely virtual. Bitcoin utilizes the same methodology adopted by peer to peer file sharing (torrents) to build a digital currency that has no central authority. No entity governs Bitcoin.

Each Bitcoin is basically a computer file which is stored in a 'digital wallet' on a smartphone or computer. Every single transaction is recorded in a public list called the "blockchain". This makes it possible to trace the history of Bitcoins so people can't spend coins they do not own, make copies or undo transactions.

There are three main ways people get Bitcoins.

* You can buy Bitcoins using 'real' money.
* You can sell things and let people pay you with Bitcoins.
* Or they can be created using a computer.

Bitcoins are valuable simply because people believe they are valuable. Bitcoins are valuable as long as people are willing to exchange them for real goods and services, and even cash.

People can also spend their Bitcoins fairly anonymously. Although all transactions are recorded, nobody would know which 'account number' was yours unless you told them.

In spite of the convenience it provides, some states have banned them, some have opted to treat them like a commodity and rest of the governments and authorities are cautiously watching the scenario as it unfolds.

Is it just a toy for financial anarchists or a new innovation that is created by the society, for the society that will pave way for a laissez faire monetary system?

Or is it just another asset bubble?

Currency; Essential features

A currency or money derives its name from Middle English: "curraunt" which means "in circulation" which denotes tokens in many forms circulated as a medium of exchange[1]. The most common form is banknotes, or coins, issued by governments as physical tokens.

What is money? Although this seems a simple question, when posed with a question of this nature the economists identify three elements that are essential to constitute money. Whatever is denoted as money should be;

* A store of value
* Unit of account
* Medium of exchange

At first, metals were used to stand for value stored in the form of metal as a commodity. Thus the metal itself was the store of value, examples being silver, gold, and bronze. These metals were mined, weighed, and embossed in order to ensure that the recipient is getting a correct weight of the metal. Thus the coins were created.

Then the Chinese introduced paper money, as an alternative to the coins that are heavy and cumbersome to handle. Paper money was first brought in as a promissory note issued in respect of a deposit of coins that eliminated the need for transport of coins.

Thus history shows that the form of money evolved as per the convenience of the users.

Also the sovereign state can decide which currency may be used. But paper money has no intrinsic value. And the issuer of paper money could print more notes than the underlying asset value, thus creating new concepts such as inflation and monetary policy controls.

A sovereign state has control of its own currency, that control is usually exercised either by a central bank or by a monetary authority. A monetary authority is created and supported by its sponsoring government; as such the government that creates it has express and implied control over the monetary authority and thereby the currency.

Also currencies are subject to trading between each other in foreign exchange markets.

[1] http://www.thefreedictionary.com/currency

These markets determine the relative values of the different currencies. In every state prices are expressed in units of currency. The value of the currency can be judged only against an external reference. This reference is the exchange rate, which is a fundamental price in any economy. An exchange rate is the price at which two currencies can be exchanged against each other. Determining the relative values of different currencies is the role of the foreign-exchange markets. [2]

Usually currency is money issued by a state and has limitations of recognition. But there are currencies that are accepted beyond the geographical boundaries of the issuing country. British pounds, U.S. dollars, and European Euros are examples. Currencies do not necessarily take the form of physical objects, but can be used as a medium of exchange as long as they are in the form of stores of value and units of account.

Quasi currencies and alternative currencies

There are many forms of media of exchange, such as "BarterCard" where the goods and services are bartered through a network, loyalty points issued by credit card issuers and airline networks, Microsoft points or Game-Credits. Another example is highly popular and highly regulated 'asset backed' 'alternative currencies' such as mobile-money schemes like MPESA in Kenya.[3]

The latest trend is the emergence of private, decentralized, trust based and networks supported alternative currencies such as Bitcoin, Litecoin, Peercoin or Dogecoin, as well as branded currencies. These currencies are Internet-based and digitally stored. The Bitcoin is the first of its kind and the most popular and all other subsequent variants can be folded back to Bitcoin.

But is Bitcoin a store of value and a unit of account? Or is it a just simple medium of exchange created out of convenience?

When one looks at the alternative currencies that are distinct from centrally controlled government-issued currencies, one would naturally wonder who control the monetary policy, money supply, exchange rate and exchange rate markets.

However the supply of Bitcoin is limited by its own code. The mining process is designed to become tougher and tougher where at one point in time the cost of mining will exceed the value of the currency thus limiting the money supply.

[2] The Economist - Guide to the Financial Markets (https://docs.google.com/file/d/0B_Qxj5U7eaJTZTJkODYzN2ItZjE3Yy00Y2M0LTk2ZmUtZGU0NzA3NGI4Y2Y5/edit?pli=1&hl=en#)

[3] Everything You Need to Know About Bitcoin: VICE Podcast 027 (https://www.youtube.com/watch?v=SNssKmeXrGs)

Bitcoins - origin

In 2008, just before Bitcoin's official commencement, a nine-page proposal written in a very scientific manner was released onto the internet bearing the name and email address of a man called Satoshi Nakamoto.

The media have homed-in on the individual behind the creation of Bitcoins. His humble manner and shyness for fame have paved the way for many imposters. But the man widely believed to be the author of 2008 research paper and the creator of the computer code of Bitcoin is living in Los Angeles under the name "Dorian Prentice Satoshi Nakamoto,"

Descended from Samurai and the son of a Buddhist priest, Nakamoto was born in July 1949 in the city of Beppu, Japan, where he was brought up in the Buddhist tradition by his mother, Akiko. In 1959 after a divorce and remarriage, she emigrated to California, taking her three sons with her. Nakamoto's skill for math and science was evident from an early age. However, he seems to have an undocumented period in his life where he was involved in military research as an engineer.[4]

This has led some conspiracy theorists to believe that Bitcoins is an underground government project. However Bitcoins have been popularly accepted by the society.

Nakamoto's document proposed an "electronic cash" that "would allow online payments to be sent directly from one party to another without going through a financial institution," with transactions time-stamped and viewable to all. This document can be found online at www.bitcoin.org, and analyzed in the subsequent chapters.

The innovative step in this proposal was replacing the role of banks as the trusted intermediaries with Bitcoin users, who would act as guards for the integrity of the system, verifying transactions using their computing power in exchange for Bitcoin, thus transferring the monetary control and authority to the society.

Bitcoin production is mathematically designed to move at a calibrated pace to boost value and scarcity and thereby to remain inflation proof, halving its amount every four years. This supply is designed to stop when Bitcoins reach a total of 21 million in 2140. Bitcoins can be divided by up to eight decimal places, with the smallest units called "Satoshis."

Bitcoin is a currency that dwell in the computer code and can be sent anywhere in the world without incurring bank or exchange fees, and is then stored on a cellphone or hard drive until used again. Because the currency resides in computer code, it can also be lost when a hard drive crashes, or stolen if someone else accesses the keys to the code.

[4] The Face Behind Bitcoin By Leah McGrath Goodman / March 6, 2014 http://mag.newsweek.com/2014/03/14/bitcoin-satoshi-nakamoto.html

Apparently, the reason for excitement about Bitcoin is that it is the most efficient way to do financial transactions. On the other hand, Bitcoin's ease of use can also lead to easy theft and it is safest when stored on a hard drive that's not connected to the Internet. An international Bitcoin transaction is said to be as easy as sending an email. May be it is the Bitcoin's vulnerability to massive theft, fraud and scandal, which has made the price of Bitcoins fluctuate from more than $1, 200 each last year to as little as $130 in late February 2014.

Features of Bitcoins

The Bitcoin code is based on a network protocol that's been established for decades. As per experts its brilliance is in the design. In order to understand the inner mechanism of the Bitcoins transaction process one may turn to the research proposal published by Satoshi Nakamoto.

The abstract of the 2008 research proposal by Satoshi Nakamoto is reproduced below: (Although it sounds extremely technical the creator's idea could be absorbed by a lay person).

"Abstract:

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone".[5]

An attempt is taken to explain Nakamoto's words to non-technical audience in the foregoing text.

In the introduction he addresses the issue of a necessity of a trusted third party or an intermediary in financial transactions, and the cost of financial intermediation. And at the beginning he finds no other alternative to make non-reversible payments for nonreversible services without an intermediary in payment methods other than by using physical cash.

Then he proposes an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. He proposes a method that is computationally impractical to reverse by using a peer-to-peer (where two or more computers get together to share resources and computational

[5] Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto (www.bitcoin.org)

power without any hierarchy)[6] distributed timestamp server (a publically accessible server that keeps time of an event in the network) to generate computational proof of the chronological order of transactions.

Nakamoto's system is secure as long as there are honest record keepers distributed in the cyberspace collectively control this system than any cooperating group of attackers or counterfeiters. Given the large network in the internet and given the postulation that a group of fraudsters never will be able to control the internet with a collective motive without each one getting greedy over the others, the authenticity of the system should prevail. Thus the Bitcoin economy relies on the scale of the internet.

Bitcoin transactions

The paper defines an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a function called a hash (A function that reduces a file of data to a computer code) of the previous transaction and the public key (something similar to the username) of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

Although this explanation sounds like a technical draft for a computer engineer one may find a similarity of this system and the system of a bill of exchange, promissory note or a cheque where the owner endorses and delivers the instrument in exchange for value.

But the Bitcoin is a computer file that can be duplicated. How does one ensure that a previous owner did not spend the coin more than once?

Nakamoto proposed that the only way to confirm the absence of an earlier transaction (with the same coin) is to be aware of all transactions. To achieve this without a trusted intermediary, all the transactions must be publicly announced, and the participants need to agree on a single history of the order in which the transactions occurred. The payee only needs proof from the majority of the computers (in the internet) that at the time of each transaction there is in fact a fresh Bitcoin being spent.

To solve this problem the concept of a "time-stamp server" is introduced. A timestamp server works by marking the time and widely publishing to the internet the time at which an event occurs with respect to a Bitcoin. Each timestamp includes the previous timestamp in a sequence forming a chain of events. In order to avoid infinite number of timestamps as the coin gets spent, Nakamoto has suggested a methodology (of which the details as per his research proposal is highly technical), which essentially means bundling the previous usage details. But this bundle cannot be created or counterfeited without undoing all the previous transactions.[7]

[6] *www.computerworld.com › Networking*

[7] Section 4 Proof of work - Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto

Again, for the time stamping as well, the internet will stand as evidence. The assumption, that one may not amass a rough network with an intention to counterfeit beating the majority of the honest users (or computers), is adopted.

Mining Bitcoins

There is no central authority to issue Bitcoins. The computer code of the Bitcoin is open source and available to public. But the computers have to work and cipher them. The steady addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation. Thus the act of creating Bitcoins is called mining and the people that engage in this activity are called miners.

In this case, computer time and electricity are the resources that are spent. If the cost of the input resources is less than the value of a coin, there will be an incentive for the miners to mine coins. Since the supply of Bitcoins is mathematically limited by its own creation code, once the determined number of coins has entered circulation, the currency will be completely inflation free.

But like in gold rush the miners have to compete for the mining, and the process of mining is designed to be more complex towards the end. Thus the miners and the machines engage in pure "capitalistic competition". Yet their presence in the network is critical. It distributes new Bitcoins in a relatively fair way, as only those people who dedicate some effort to making Bitcoin work get to enjoy the coins as they are created. But because mining is a competitive enterprise, miners have started collective mines by pooling resources.

Privacy in Bitcoins

The traditional banks impose a level of privacy by statute. But there is no trusted third party in this instance. The necessity to announce all transactions publicly prevent the privacy. But Nakamoto maintains that privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous (Bitcoin needs a public key and a private key to effect transactions). The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges to the public, but without telling who the parties were.[8]

However the risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

Digital wallet and secure storage of Bitcoins

Bitcoins are stored in public addresses that are somewhat similar to the concept of a username, but complicated like the following example.

[8] Section 10 Proof of work - Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto

"1FDoodNaSmZ4vnePePDEnJtAiQNrpcGwjC."

If a payer want to send a payee Bitcoins, the payee can give the payer his public addresses. Each public address has a private key; similar to a password. Only someone who knows the private key can spend the Bitcoins stored there.

To make dealing with Bitcoins easier, one can use a Bitcoin wallet. A wallet can be either a program downloaded on to a computer or a website where one would simply log in. But the wallet helps to manage all the address and keys easily. One such example is "Coinbase". In here, one can purchase and sell Bitcoins for dollars, but also one can send and receive Bitcoins to and from any address. There are other websites (online wallets) that provide advanced security and backup features.

If one is still worried about a wallet being hacked and emptied, he can also store Bitcoins on paper, which one can keep in a secure location similar to a safe deposit box. Creating a paper Bitcoin wallet is really nothing more than printing out a public address and the matching private key.[9]

Thus Nakamoto has proposed a system for electronic transactions without relying on trust. The proposal is robust and simple. The proposal started the framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, he proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change.

All the rules and incentives are enforced with a consensus mechanism. The rules of the system are enforced on everyone by each other. Not even the software developers can tamper with it against the wishes of the users.

Usage of Bitcoins

Although there are still a limited number of dealings done through Bitcoins, you can use it to buy beer in Berlin, order pizza in Amsterdam, and hire a taxi in Edinburgh. The acceptance of Bitcoin has spread to businesses as diverse as Tesla (a highly successful electric car manufacturer), OkCupid (online matchmaker), and Virgin Galactic, (Richard Branson's space aviation company).[10]

The popularity of the Bitcoin has soared and several reasons have been given for the surge: .[11]

[9] Moneytalksnews.com Bitcoin for dummies (http://www.moneytalksnews.com/2014/04/25/bitcoin-for-dummies/#P6EqkHQo7KHs0Dyx.99)

[10] Bitcoin: Experts clash over the crypto-currency http://www.bbc.co.uk/news/technology -25130261

[11] Bitcoin: Experts clash over the crypto-currency http://www.bbc.co.uk/news/technology -25130261

* Speculators piling in after a US Senate hearing into the innovation of Bitcoins
* Chinese citizens turning to it as a way to shift their wealth out of the country
* Members of the public buying at least a fraction of a Bitcoin (the smallest unit is 0.00000001)
* Bitcoin enables micropayments - instead of ads, tiny fractions of a penny could flow from your browser directly to sites you visit, with no middleman fees
* Crowd-funding (A community based venture capitalism)
* Anyone with a smart phone can accept Bitcoin: No complicated merchant bank accounts are needed
* Bitcoin is barely five years old.

Taxation

Countries and their tax authorities have been struggling with how to regulate it, with some seeing it as a route for tax evasion or money laundering.

Russia has declared transactions illegal, China has banned its banks from handling Bitcoin trades, and there have been calls for the US to do the same. Singapore has imposed a tax on Bitcoin trading and using it to pay for services, after classifying it as goods, rather than a currency.

The UK's tax authority has scrapped plans to charge value added tax (VAT) on Bitcoin trading. HM Revenue & Customs also said it would not levy the 20% tax on the creation, or so-called 'mining', of the virtual currency. It said Bitcoin trading and other activities, like charges for verifying transactions, "are exempt because they fall within the definition of 'transactions, including negotiation, concerning deposit and current accounts, payments, transfers, debts, cheques and other negotiable instruments'". And the profits or losses of companies using Bitcoins, and on exchange movements between currencies, will be subject to corporation tax, the government agency added.[12]

The dark side of Bitcoin

The Bitcoin with no regulation or financial intermediation has facilitated illegal trades on underground ecommerce sites such as the Silk Road (a website that trades in contraband). Federal Bureau of Investigation, in October 2013 shut the online black market Silk Road and seized its $3.5 million cache of Bitcoin. The FBI is now one of the largest holders of Bitcoin in the world.

In recent past, a revived version of Silk Road as well as one of Bitcoin's biggest exchanges, Tokyo-based Mt. Gox, shut down and filed for bankruptcy after attacks by hackers drained each of millions of dollars. This was before the rise of today's multibillion-dollar Bitcoin economy, boosted last year by the endorsement of outgoing Federal Reserve chair Ben Bernanke, who said crypto currencies "may hold long-term promise."

[12] HMRC scraps VAT on virtual currency Bitcoin (http://www.bbc.co.uk/news/buness -26426550)

Former Federal Reserve Chairman Alan Greenspan has commented that Bitcoin prices are unsustainably high after surging 89-fold in a year and that the crypto currency isn't actually currency. He has speculated another bubble and further added that "It has to have intrinsic value. You have to really stretch your imagination to infer what the intrinsic value of Bitcoin is. I haven't been able to do it. Maybe somebody else can".[13]

But the critics of the Greenspan's statement say at the beginning of the internet the same skepticism existed for internet banking, mobile money transfers. With the passage of time Bitcoin exchanges and wallets would bring in more security and less theft. There is optimism that Bitcoin will hold for long term as the Bitcoin is more efficient than any currencies and has much lower transaction costs.[14]

The currency has also attracted the attention of the U.S. Senate, the Department of Homeland Security, the Federal Reserve, the US Internal Revenue Service, the Treasury Department's Financial Crimes Enforcement Network, and the Securities and Exchange Commission.

But it should be noted that a currency created by the society cannot be repressed or shut down. If a global superpower shuts down Bitcoins the society will create "Bitcoins 2.0 (version two)" and so on.

Global trade and e-Commerce

Trade is increasingly 'unbundled', with countries no longer trading in goods other than design or assembly. Goods are 'made in the world'. Thus, the flow of trade has increased. Services cannot always easily be measured at the border and some estimates put them at 40% of total trade now.[15]

Current global e-commerce volumes are estimated to be in the range of USD 963 billion to USD 1.3 trillion as of 2013 as estimated by different entities such as Goldman Sachs to eMarketer[16]. These volumes are growing. The predictions before the dot.com bubble burst (in 2000) were in the range of USD 4.5 trillion by 2005, as predicted by Goldman Sachs. [17]

According to eMarketer prediction, the global e-commerce market was expected to grow 17% in 2013. With total sales of $420 billion, North America is the largest e-commerce

[13] Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value (http://www.bloomberg.com/news/2013-12-04/greenspan-says-bitcoin-a-bubble-without-intrinsic-currency-value.html)

[14] Bitcoin Battle – Forbes (http://www.forbes.com/sites/kashmirhill/2014/03/26/warren-buffett-says-bitcoin-is-a-mirage-why-marc-andreessen-thinks-hes-wrong/)

[15] Global trade unbundled - Special Report by Standard Chartered Bank Research Wing

[16] *"eMarketer"* is an independent market research company that provides insights and trends related to digital marketing, media and commerce.

[17] E-commerce and Development *Key Trends and Issues*
http://www.wto.org/english/tratop_e/devel_e/wkshop_apr13_e/fredriksson_ecommerce_e.pdf

market for the moment, but is expected to be overtaken by the Asia-Pacific region in 2014. The emerging nations in the Asia-Pacific region will be the largest contributor to global e-commerce growth in the next few years, as per the eMarketer. Online sales in the region are expected to grow 23% this year, with China and Indonesia seeing particularly strong growth (65% and 71%, respectively).[18]

In terms of buyer penetration, mature markets such as North America and Western Europe are still far ahead of emerging markets. 72 percent of internet users in Western Europe and North America were expected to buy goods or services online in 2013, whereas penetration in Asia is still below 50 percent.[19]

Bitcoin is made for e-commerce, although it can be used for over the counter trades as well. And currently the value of the Bitcoins in circulation is estimated to be in the range of USD 1 billion. It only takes simple arithmetic and simple economics to understand that the value of the Bitcoin will only further appreciate.

But experts agree that Bitcoin poses the biggest threat to the payment systems and not to the currencies. As the popularity grows Cash/Credit based card systems, remittance systems and other e-exchanges like "paypal" should go out of business before the fiat currency disappears from the system. Merchant fees and transaction fees is a reason for Bitcoin to become popular among small businesses.[20]

Legal aspects of alternative currency

Bitcoin may be the media of exchange in disputed transactions. Also it is prone to theft and one needs a protective measures or reactive measures in order to address any losses that may arise.

The classic legal texts of the Bills of Exchange Ordinance & Evidence Ordinance have been adaptable for the ever-changing commerce for more than a century. These time tested legal provisions have not been able to adapt to the changes that took place within the last decade.

However some attempts have been made to bring the current legal framework up-to-date with the commercial innovations. The recognition of the digital signatures and recognition of electronic evidence are examples. But final test of the effectiveness of these legal innovations lie in a proper judicial review in a practical scenario.

It is implicit that new legal regimes will evolve to facilitate the revolutionary commercial practices developed by the information technology.

[18] http://www.statista.com/chart/1223/global-e-commerce-sales-2013/

[19] .do

[20] Everything You Need to Know About Bitcoin: VICE Podcast 027 (https://www.youtube.com/watch?v=SNssKmeXrGs)

Conclusion: Community acceptance and future of Bitcoin

Dr Stephen Kinsella makes the following commentary on the Bitcoins : [21]

“The Bitcoin phenomenon is the purest manifestation of what Charles McKay described in his 1841 book Extraordinary Popular Delusions and the Madness of Crowds. At the psychological level of the investor, there’s no difference between Bitcoins, tulips, railways, or the stock market bubbles of the 1920s, 1990s, or the mid 2000s.

In this case a lot of people are deciding a string of electrons are worth something, as opposed to nothing, and they want to sell it to the next guy as soon as possible.

As long as you pass your Bitcoins on to the next guy while extracting a profit, you’ll be happy. There is always a greater fool. Right up until the moment there isn’t one.”

It might seem that Bitcoin is just like fiat currency issued by governments. But its worth is based solely on the willingness of holders and merchants to accept it in trade. The “fiat” (meaning “let there be”) in “fiat money” reflects the power of governments to command and tax. Because of their power to tax, governments can make money by fiat, simply by declaring their willingness to accept that money in repayment of tax debts. Historically, money arose from, and in conjunction with, this power. But one may argue that the society commands more power than the governments.

Or may be Bitcoin is money that arose to simplify what would otherwise be complex and cumbersome barter transactions in the virtual world. But in the case of Bitcoin, there is no source of value. The computing power used to mine the Bitcoin is gone and cannot be reused for a more productive purpose. If Bitcoins cease to be accepted in payment for goods and services, their value will be precisely zero.

In particular, Bitcoin represents what ought to be the refutation of the Efficient-Markets Hypothesis, (EMH) which still guides most regulation of financial markets. [22]

[21] Dr Stephen Kinsella: Senior lecturer in economics at the University Of Limerick’s Kemmy Business School Also writes a weekly column for the Irish Independent newspaper (Bitcoin: Experts clash over the crypto-currency http://www.bbc.co.uk/news/technology-25130261)

[22] The Bitcoin Bubble and a Bad Hypothesis by John Quiggin (Professor of economics at the University of Queensland, Australia and adjunct professor at the University of Maryland, College Park) http://nationalinterest.org/print/commentary/the-bitcoin-bubble-bad-hypothesis-8353

The efficient-markets hypothesis

An investment theory that states it is impossible to "beat the market" because market efficiency causes existing prices to always incorporate and reflect all relevant information. According to the EMH, stocks always trade at their fair value on stock exchanges, making it impossible for investors to either purchase undervalued stocks or sell stocks for inflated prices. As such, it should be impossible to outperform the overall market through expert stock selection or market timing, and that the only way an investor can possibly obtain higher returns is by purchasing riskier investments.[23]

The EMH states that the market value of an asset is equal to the best available estimate of the value of the services or income flows it will generate. In the case of a company stock, this is the discounted value of future earnings.

Since Bitcoins do not generate any actual earnings, they must appreciate in value to ensure that people are willing to hold them. But an endless appreciation, with no flow of earnings or liquidation value, is precisely the kind of bubble the EMH says can't happen. [24]

J M Keynes is supposed to have said, "The market can stay irrational longer than you can stay solvent."

But on the other hand, Bitcoin is a tool of the internet. There are many entities and tools within the internet that have created value out of nothing. Entities like Google, Facebook, Youtube have a combined market capitalization exceeding the combined GDP of several small nations. But without the internet they are nothing. If Bitcoin dominates the internet one day, the intrinsic value of the Bitcoin will be the value of the internet.

However one statement will truly stand:

The big advantage of Bitcoin as "stateless money" is that when it collapses, the government won't have to bail it out.[25]

[23] http://www.investopedia.com/terms/e/efficientmarkethypothesis.asp

[24] The Bitcoin Bubble and a Bad Hypothesis by John Quiggin (Professor of economics at the University of Queensland, Australia and adjunct professor at the University of Maryland, College Park) http://nationalinterest.org/print/commentary/the-bitcoin-bubble-bad-hypothesis-8353

[25] The Bitcoin Bubble and a Bad Hypothesis by *John Quiggin*