The Future of Cryptocurrencies

Taylor Offer

Part 1- Background Information

This paper will discuss pros and cons of cryptocurrencies, and if they can become the dominant currency of the future. The paper will primarily focus on Bitcoin, because it has become the largest and most recognizable cryptocurrency, but first we will start with a brief history on cryptocurrencies.

"The idea of digital money—convenient and untraceable, liberated from the oversight of governments and banks—had been a hot topic since the birth of the Internet (Wallace)". For experts in the field, the rise of cryptocurrencies was a question of "when" and not "if".

Cypherpunks, Ecash, Bit Gold, RPOW and B-money all tried to succeed as cyber currencies but failed. The main reason these currencies failed was because of a lack of trust and security. No one felt comfortable using these new and mysterious currencies. "If a digital dollar is just information, free from the corporeal strictures of paper and metal, what's to prevent people from copying and pasting it as easily as a chunk of text, "spending" it as many times as they want? (Wallace)." Cryptocurrencies could not overcome the "double-spending" problem, the ability of hackers to simply recreate and re-spend the same money. The next big cryptocurrency would be whichever could create a secure way to exchange money, without the threat of "double-spending".

The origin of Bitcoin traces back to November 1st, 2008. This was the first time Satoshi Nakamoto posted “to an obscure cryptography listserv describing his design for a new digital currency that he called Bitcoin (Wallace).” No one had ever heard of Satoshi Nakamoto, and no information on him could be found. He introduced a new system with “block chains” and “miners”. To put it simply, anyone with a powerful enough computer could become a miner. To make each transaction secure, every transaction is visible to the public. Once a transaction is made and Bitcoins are transferred from one account to another, a complex puzzle is created. Any miner can attempt to solve the puzzle. “The difficulty of each puzzle would increase as the number of miners increased, which would keep production to one block of transactions roughly every 10 minutes. In addition, the size of each block bounty would halve every 210,000 blocks—first from 50 bitcoins to 25, then from 25 to 12.5, and so on. Around the year 2140, the currency would reach its preordained limit of 21 million bitcoins. (Wallace)”.

First, a request for Bitcoins to be transferred from one account to another is made. Then a puzzle is created, and whoever “solves” the puzzle is rewarded with Bitcoins. Solving the puzzle requires dedicating a lot of computer power to the server to help support the transaction. Every transaction is visible to the public, but is not connected to the users name. The puzzle system, along with every transaction being public, solves the big “double-spending” problem.

Also, the “reward” for solving the puzzle is halved every 210,000 blocks. This creates a finite number of Bitcoins. Another big failure for past cyber currencies was inflation and volatility. The idea that more units of currency could just be created out of nowhere scared many potential users and investors. If more units are created, given the laws of supply and demand, the value of each unit decreases. Monetary policy, altering the supply of money, is a huge priority for the US Government. Hundreds of brilliant economists are devoted to a team that decides the ideal money supply. For past cryptocurrencies, the money supply was held at the discretion of the creator. The fact that Bitcoin's could not be created randomly and there is a finite amount of them helped entice more people to use them.

The final major factor contributing to Bitcoin's rise to dominance was timing. Bitcoin was started in late 2008, right after the huge market crash. The forecast for the economy was negative and the future of the dollar was uncertain. It was the perfect time for a cryptocurrency to rise to relevance.

The future seemed bright for Bitcoin, but the coins were still not yet valuable. In early 2009, "Gavin Andresen, a coder in New England, bought 10,000 bitcoins for $50 and created a site called the Bitcoin Faucet, where he gave them away for the hell of it. Laszlo Hanyecz, a Florida programmer, conducted what bitcoiners think of as the first real-world bitcoin transaction, paying 10,000 bitcoins to get two pizzas delivered from Papa John's. (He sent the bitcoins to a volunteer in England, who then called in a credit card order transatlantically.) A farmer in Massachusetts named David Forster began accepting bitcoins as payment for alpaca socks. (Wallace)." Until 2011, one Bitcoin was never worth more than a dollar. The future was not looking bright for Bitcoin until Silk Road gained popularity.

Silk Road was founded in February of 2011. Silk Road is a Tor hidden online marketplace. Purchases are anonymous and cannot be traced back to the user. It became a marketplace that sold drugs, illegal paraphernalia, and even hit men. Credit cards were too easy to trace, so almost all transactions were made with Bitcoins. It was not until June of 2011 until the price of Bitcoins started to increase.

In June 2011 Gawker published an article on Silk Road and Bitcoins. Almost over night, the price of 1 Bitcoin went from $9 to $28. This was the first time Bitcoin was exposed to the public. Before, Bitcoin was almost exclusively used for Silk Road. Now, the public wanted in on Bitcoins.

The volatile price of Bitcoin intrigued investors. In 2013, Bitcoins really took off. Instead of mining Bitcoins, many new members wanted to own the currency by buying it. Mt. Gox, Coinbase, and many other marketplaces were used to buy Bitcoins. The demand far outnumbered the supply, and the price shot up. In a few months in 2013, the price of 1 Bitcoin grew exponentially from less than $100 to over $1,000.

Satoshi Nakamoto was the man who created it, but who was he? No one has ever met or seen him. Was he even a real person? Who was behind Mt. Gox, Coinbase and all the Bitcoin exchanges? Can they be trusted? How are they regulated? Consumers trusted these exchanges with their credit card information. They were also purchasing Bitcoins for thousands of dollars. The price of Bitcoin is so risky and volatile, but the potential upside outweighed the risk.

After hitting a record high $1,242 for 1 Bitcoin, almost the price an ounce of gold, Bitcoin has severely dropped. As of now (3/21/13), 1 Bitcoin is worth $428. This is largely due to the collapse of Mt. Gox. 850,000 Bitcoins went “missing” from Mt. Gox after a hacker attack. Those Bitcoins were never returned to their owners, and many consumers lost a lot of money. The risk associated with hackers and the security of their Bitcoins scared many people away. The demand for Bitocoins decreased, and so did the price. Is it possible for a cryptocurrency to have a stable price and be immune to hackers?

Part 2- Pro Cyber-Currency

Paper and coin currencies are very outdated. They have been around for centuries, and although technology has advanced significantly, paper and coins have remained more or less the same. There are many glaring problems with this currency that cryptocurrencies can easily replace.

First, paper currency cannot be traced. While the general public may argue this is a positive thing, it is not. Lost cash cannot be returned to the original owner. Also, once money is stolen there is no way to prove who’s it really is. A cryptocurrency has the ability to trace back money to the original owner in case it is lost or stolen.

Another problem is accessibility. It requires planning and luck to always ensure to have the right amount of cash on hand. Everyone has been in a predicament where they would like to buy or do something but they did not have cash on them. A cryptocurrency could have a personalized secret pin or passcode that could be given to transfer funds. Regardless of where you are or what you have on you, you can always have access to your funds.

Lastly, a cryptocurrency will save everyone money. It will save the government money because they will no longer have to spend so much on creating physical currency. It will save businesses money because they will no longer have to pay 2-3% credit card fees. And lastly, it will save the consumer money because it will insure that they spend all of their money, opposed to having it lost or stolen or not even picked up (That change at the register after a purchase adds up).

Part 3- Against cryptocurrency

A cryptocurrency could never be immune from hackers. Nothing online can ever be secure enough to the extent that it cannot be hacked into. Getting a Facebook or Email account hacked is one thing, but getting your cryptocurrency account and all your money taken is another.

People like hard cash. They don't trust technology, but they trust their money in their wallets or under their mattresses. If the people are not willing to adapt to a cryptocurrency, there will never be a ubiquitous cryptocurrency.

A cryptocurrency can never be stable. Many people in the federal government control the monetary supply very closely. Who will control the money supply for a cryptocurrency? Who determines how much 1 unit is worth? The currency will be too volatile to use as our primary form of money.

Part 4- Conclusion

While valid arguments are made for both sides, I think cryptocurrencuies will take over in the future. “If someone were to perfect a flying car, governments around the world would be faced with a conundrum. Over the centuries humans have developed a transport system complete with quaint country streets, bustling six-lane highways, electronic toll booths and police officers to monitor it all. So should the powers that be try to fit the flying car into the current model or create a whole new scheme that allows the new technology to flourish? (Sharf).” I think it would be hard for any individual to defend not moving forward with a flying car, and I think the same can be said about cyber currencies. Ed Moy, the former director of the U.S. Mint, said it best “Government moves very slow and cautiously. Digital technology moves very quickly, so eventually the conflict is going to be crypto-currencies moving faster than what governments are comfortable with.” Right now the currency is moving too fast for the government to keep up, but eventually it will slow down and the government will be able to regulate and maybe even implement it. I think cryptocurrencies could follow the same trend as paper money. According to Jack Weatherford, author of “The History of Money”, “Like the Bitcoin, it (paper money) was a revolutionary idea that got out of hand and the value of the dollars dropped drastically. After the revolution, the US abandoned paper money and returned to the use of coins. It took another century before the US government was able to create an effective paper money system.” Bitcoin, with its suspicious background and unknown owner, might not be the dominant cryptocurrency of the future, but I believe the world will soon convert to cryptocurrencies.

Bibliography

Bollen, Rhys. "The Legal Status of Online Currencies: Are Bitcoins the Future?" N.p., n.d. Web. 30 Mar. 2014.

Sharf, Samantha. "For Bitcoin Lessons In The History Of Failed Currencies." *Forbes*. Forbes Magazine, 29 Mar. 2014. Web. 30 Mar. 2014.

"Bitcoin Could Disrupt Traditional Banking Globally." - *Worcester Research and Publications*. N.p., n.d. Web. 01 Apr. 2014.

"Bitcoin – On Its Way Out?" *Binary Options Leader RSS*. N.p., 01 Apr. 2014. Web. 01 Apr. 2014.

"Hidden Flipside." *The Economist*. The Economist Newspaper, 15 Mar. 2014. Web. 31 Mar. 2014.

“Virtual Economy Looms as Digital Cash Grows up." *Science Direct*. N.p., n.d. Web. 01 Apr. 2014.”