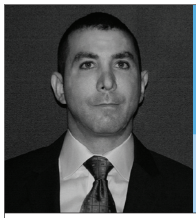
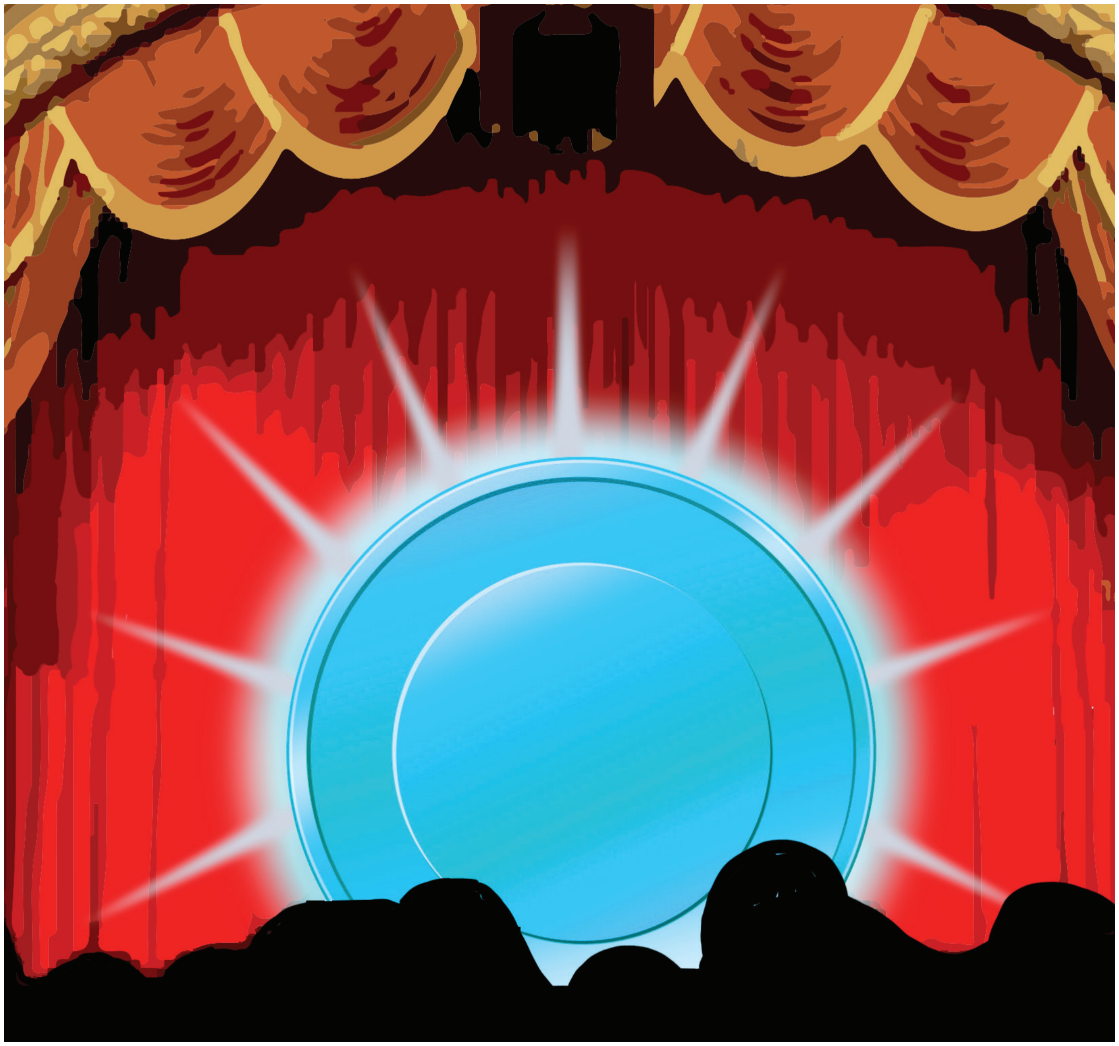


Noah Silverman

The E-Penny Opera

We're witnessing the opening act of what could prove to be a grand event in the annals of commerce – the advent of electronic crypto-currencies



What is a crypto-currency?

Crypto-currencies are a new type of asset that have been rapidly growing in popularity over the past few years. They are, in effect, a form of digital bearer bond with no underlying asset. Some people consider these new currencies an asset for investment and trading, others consider them a viable currency for purchasing goods and services, and a few consider the whole thing a giant Ponzi scheme destined to collapse.

I will be publishing a series of articles in *Wilmott* magazine discussing different aspects of this new asset class. My goal, in this first article, is to provide a comprehensive overview of this new asset class. In future articles, I plan to discuss more details regarding the underlying technology, as well as investigate pricing, risk, and trading strategies.

Currently, Bitcoins (often denoted as BTC) are the most popular asset in this class. So, a majority of this first article will be slanted toward a focus on BTC. They have experienced more liquidity, faster adoption, more media attention, and attracted more venture capital investment than all the other crypto-currencies combined.

Why do we care?

Crypto-currencies offer a number of advantages over cash, gold, credit cards, or other forms of payment. They can be anonymous, provide for 100 percent verifiable transactions that can't be reversed, are generally impossible to counterfeit, and allow instant person-to-person payments globally. Furthermore, and much to the fear of credit card companies, payment can be made faster, more securely, and with zero transaction fees.

Some example scenarios follow, where a crypto-currency makes life easier.

- **Micropayments:** Imagine, if you will, a teenager living in Panama who is a fan of a small garage band in Moscow. He wants to buy their latest song directly from their Web site for 15 cents. Currently, there is no way to efficiently do this. The credit card fees alone would be prohibitive, the band would need to set up a payment processor, the teenager would need a credit card, etc. PayPal may seem like an option, but that would require the kid to have a bank account and meet their verification requirements. Then, the band would have to set up with PayPal as a merchant, meet all their requirements, etc. Finally, PayPal's transaction fees would make a price of 15 cents impossible. With Bitcoin, our music fan can send payment of any amount, directly to the band, with zero fees and zero hassle. His transaction is instantly verifiable.

- **Safe wealth storage:** As a second example, consider a family moving to a new country. If they don't have established banking with easy wire transfer, it may be difficult to carry their wealth with them. (Traditionally, families have transported their wealth in cash, precious stones, gold, or even Persian rugs.) With Bitcoin, they can convert all their assets to digital form. Then they may simply put their digital wallet on a thumb drive, a laptop, print it on paper, or even email their account info. Upon reaching their destination, the account is accessed and the crypto-currency converted to the local currency. No heavy boxes to carry and no risk of robbery during travel.
- **Improved e-commerce:** A merchant selling product online can generate a unique payment address for each client. (These addresses are unique and virtually unlimited. I will discuss the details later in this article.) Each invoice, payment, and shipment can then be absolutely tied to payment. Furthermore, there can never be a chargeback or reversal of payment. The purchase order, bid, product purchased, payment, shipping manifest, receipt of delivery, and all customer communication are tied together by a single, unique digital identifier.
- **Money laundering:** Not all use of crypto-currency is positive. For example, small drug dealers either accept payment in Bitcoin or convert cash payments to Bitcoin. Those digital coins are then sent up the chain of the drug cartel. Instead of having to send truckloads of cash over the border, risking intervention, the criminals just email a tiny digital key to an anonymous digital address owned by the drug overlord. The criminal empire may then hoard the digital currency, pay their employees, or convert it to a local currency anywhere in the world. There is zero cost, zero transportation risk, and full anonymity. Furthermore, it would be almost impossible for law enforcement to trace the money or establish any connection between the drug lord and the street dealers. This is the type of scenario that has law enforcement *very* concerned.
- **Tax evasion:** Your local plumber comes over to fix a leaky faucet. You pay him in Bitcoin from your anonymous account to his. Later, he purchases a few beers after work with Bitcoin. The bar owner then buys some groceries from a local farmers' market using the Bitcoin. Because of the anonymous nature of these transactions, no sales tax, state tax, liquor tax, or federal income tax was collected or paid on any of these transactions. (Of course, this is no different from everyone just using cash.)

Where did it come from (brief history)

The idea of a cryptographically based currency has been discussed amongst computer and software engineers for years. The theory is that most currencies in the world are fiat based or agreement based. (Agreement in the sense that the value is solely derived from agreement amongst the currency users.)

In 2009, a paper describing Bitcoins was announced in an online discussion group (Usenet System) for people interested in cryptography. The author was anonymous and only identified himself by the pseudonym "Satoshi Nakamoto." He simply wrote, "I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party." Many people suspect that the paper was actually published by a group of mathematicians as opposed to one individual. The original paper, for those interested, is still available as a free PDF download at: www.bitcoin.org/bitcoin.pdf.

Many people suspect that the paper was actually published by a group of mathematicians as opposed to one individual

A few people were intrigued by the idea and started developing open-source software to implement the protocol outlined in Nakamoto's paper. Bitcoin Software v0.1 was released on January 11, 2009. On January 12, 2009, the first official BTC transaction was recorded when Nakamoto sent 100 BTC to Hal Finney, a developer for the PGP Corporation. Finney is also credited with creating the first reusable proof-of-work system (a critical component in all crypto-currency systems) in 2004, several years prior to the invention of Bitcoin.

On May 21, 2010, a pizza was bought with Bitcoin, marking the first real-world transaction. US$25 of pizza was bought from a restaurant named Jercos (in Jacksonville, FL) for 10,000 BTC (worth about US$1,000,000 today). Since then, Bitcoin volume has grown massively, and with over 150,000 coins traded on exchanges daily and a price of around US$120 for one Bitcoin, the average daily volume is about US$18,000,000 (June 2, 2013). This figure does not include all uses of Bitcoin as actual currency, changing hands party-to-party, which can be significantly more than what is traded on the exchange. The overall point being that, from its humble beginning of needing a small fortune to buy a pizza, BTC has experienced massive growth and adoption over the past few years.

Decentralization is the key

There have been many attempts in the past to create digital currencies that would reduce transactional friction. Some examples of previous failures are Beenz, Flooz, and E-gold, all of which are now out of business. Another glaring example of bad behavior was the recently shut down Liberty Reserve. Beenz, Flooz, and E-gold all failed simply due to lack of demand. Liberty Reserve was shut down in May 2013 and its founder arrested. The charge was money laundering.

The thing all these failed currencies had in common was that they were centralized and owned by a private entity. Some played by the rules, others didn't. Liberty Reserve was operated offshore and took no measures to verify its users' identity. It quickly became a haven for criminals looking for ways to launder funds and conduct untraceable transfers.

>

Table 1: The major crypto-currencies

Name	USD value	Avg. daily volume	Market cap (US$)	URL
Bitcoin	120.00	150,000	1,320,000,000	www.bitcoin.org
Litecoin	2.710	112,345	70,000,000	www.litecoin.org
Namecoin	0.706			www.namecoin.info
PPcoin	0.131	20	318,400	www.ppcoin.org

The current generation of crypto-currencies are all decentralized. They are owned by no one, controlled by no one, located nowhere, don't have a headquarters, don't have a central server, don't have a data center, and don't reside under any government's jurisdiction. They truly live in the "cloud" of the Internet, with users simultaneously located everywhere around the world. This, not surprisingly, has given the US government reason for concern. How can they enforce banking and tax laws against an intangible target? There is literally nobody to sue, subpoena, or arrest.

In one sense, the printed private key is the ultimate form of a bearer bond

How does it work?

People keep their coins in digital "wallets." Each wallet has a "private" key and a number of public addresses. Payment is received at any of the public addresses. To send money, the transaction must be digitally signed with the wallet's private key. Coins may be sent from person to person by scanning a barcode, entering an address in their computer, or trading them on an exchange. Entrepreneurs have created a variety of software solutions to facilitate the process, but the underlying concepts are the same. We will review the process in detail below.

The major crypto-currencies currently available are shown in Table 1.

Bitcoin – the current leader

As Bitcoins are the dominant crypto-currency by a significant factor, I will focus on them for the majority of this article. However, most of the concepts we will explore are very similar for the other crypto-currencies.

Your account in the Bitcoin world is merely a pair of digital "keys." One is a private key that is used to send payments. Attached to that private key is a public key where you receive payments. The two keys are linked through very advanced cryptographic math, in what is referred to as a one-way algorithm. It is trivial to derive a public key from the private, but virtually impossible to derive the private key from the public. The net result is that you may safely publish your public address to the world so that anyone may pay you at any time. Your private key, however, should be carefully guarded.

For example, one of my public keys is: 1Pgo8UzDeixv3kX65cgcWcamtenmCQ7vfZ.

Feel free to look it up, try to hack it, or even make a deposit.

There are currently four types of wallet, each with its own strengths and weaknesses.

- **Desktop wallets:** These programs are installed on your computer and keep your Bitcoin keys (both private and public) on your local hard drive. Your account is as secure as your computer is. There is the "official" Bitcoin wallet software available from www.bitcoin.it. Another option, which I like for advanced users, is Bitcoin Armory, available at www.bitcoinarmory.com.
- **Online wallets:** There are a variety of services that handle wallet management for you, and provide access to your wallet on their Web site. This means that you can access your account from anywhere, not just sitting in front of your computer. The most popular (and the one I use for some smaller security things) is located at www.blockchain.info. Their Web site wallet integrates perfectly with a phone app, both iPhone and Android, making mobile e-commerce extremely easy. You do, however, run the risk of someone hacking the Web site and stealing your keys (along with everyone else's). Consider these services a trade-off between convenience and security.
- **Mobile wallets:** There are a few mobile wallet solutions for both the iPhone and Android platforms. Some keep your digital keys directly on the phone, while others access your account stored in an online wallet. These are extremely convenient and something that I regularly use. This is truly the future of digital commerce. You and I can literally meet for a coffee and exchange payment between phones in seconds. Or, you can pay a retail outlet from your phone wallet instantly. These apps all use a special kind of square barcode called a "QR code" that is drawn on the phone screen and then scanned by any camera. However, just like cash in my physical wallet, I don't keep much in my mobile Bitcoin wallet. Perhaps $100 or so, but certainly not my life savings.
- **Cold storage:** Another interesting concept is that of "cold storage." Since your Bitcoin account is simply a private key and derived public key (really, just two long strings of characters), there is no need for it to actually exist on your computer. With cold storage, your private key is copied to a thumb drive, or even printed out on a piece of paper, and then deleted from your computer. In one sense, the printed private key is the ultimate form of a bearer bond. Nobody knows you have it, nobody can hack your computer and steal it, and you can instantly realize the value at any time from anywhere in the world. James Bond would love this.

How to participate (how can a person start buying and selling these assets?)

Once you've decided to start using Bitcoins, you need to acquire some. There are three main ways to get Bitcoins into your wallet:

- **Peer-to-peer:** Perhaps the easiest way to get a Bitcoin is to simply buy it from someone. I bought my first Bitcoin from someone I met online at a Bitcoin trading site. You type in your postal code and the Web site matches buyer with seller in the local area. We literally met in a public park with our cellphones handy. I gave him cash and he used the blockchain.info cellphone app to transfer a Bitcoin to my account.

- **Cash-exchange services:** There are existing services that allow people to pay bills (cellphone, utility, etc.) by bringing cash to a local convenience store. Often used by people without checking accounts, some of these services now allow you to make a Bitcoin purchase instead of paying your utility bill. One well-known example is www.bitinstant.com. However, the service fees can be very high, and there may also be limits on transaction size ($500 in the USA).
- **Full trading exchange:** There are now a few major exchanges that act much like retail stock trading Web sites. You open an account, wire some funds, and can then buy and sell just like with any currency or equity exchange. Many even offer direct API access for development of automated algorithmic trading strategies. Another nice feature is that the exchanges all allow you to see the full order book in real time. Some people use them as investment vehicles, others day trade looking for a fast profit.

Hackers and thieves

Despite the best attempts by armies of hackers over the past several years, nobody has been able to counterfeit a Bitcoin. The system was designed to make this virtually impossible. Teams of very smart computer programmers and mathematicians have worked hard on designing a system resistant to every imagined weakness. But, there are other ways for criminals to steal your digital funds. Just like the US dollar, which is extremely hard to counterfeit, it is much more efficient for a mugger to simply take your wallet. There have been many cases of Bitcoin theft, both from personal computers and from large companies storing thousands. If a hacker breaks into your computer and steals your private key, that is all they need to steal all of your digital funds. Furthermore, the anonymity of Bitcoin makes it almost impossible to catch the thieves or trace the stolen funds. There are currently a few hardware and software solutions to help protect against this kind of theft. I recommend that you employ something other than a password consisting of your cat's name or kid's birthday. This is another reason why cold storage is strongly suggested for large sums.

Technical details

Role of cryptography

Crypto-currency is based on cryptography. More specifically, the Elliptical Curve Digital Signature Algorithm (ECDSA). As I mentioned briefly above, your Bitcoin account is actually just a pair of digital "keys." These keys are two very long numbers computed from the ECDSA. One is known as your "public key" and the other your "private key." Your public key is the one you publish to the whole world, and your private key is the one you guard with utmost secrecy.

These keys are mathematically related. I like to imagine a scene from some old Cold War spy movie. You're given half of a torn dollar bill and told your contact in East Berlin will present the other half to prove who they are. Modern, public key cryptography isn't that different, except for a clever and critical improvement. With public key cryptography, you never have to show your half; it is kept secret forever.

I recommend that you employ something other than a password consisting of your cat's name or kid's birthday

Here is the clever bit. ECDSA is known as a one-way algorithm. It is trivial to compute the public key if you know the private key, but impossible to compute the private key given the public key. This enables a critical function of all crypto-currency, known as "signing." In simple terms, I sign a string of text (or full document) by combining it with my key and pushing it through the algorithm. An entirely new random number is produced and broadcast to the world. There are two things anyone can do with this new number. They can verify that it was indeed signed by me, and they can verify that the text has not changed. Changing even one letter of the text would change the output and be detected immediately.

Bitcoins, for example, rely on a publically visible transaction ledger. This lists every exchange of every Bitcoin since the very beginning. Each transaction is signed by the payer, verifying that he is the owner of the amount transferred and has approved the transfer. A transaction, in very simplified terms, would look something like this:

- Date: January 1, 2013
- From Account 12345
- To Account 6789
- Amount: 3.5 Bitcoins
- Signature: 3451234AF23423

Anyone who wishes to can verify that this transaction was signed by the owner of account 12345 and that the details listed are correct, all by simply using the listed signature. The entire ledger of these signed transactions is known as the "Block Chain" and accessible to anyone.

Peer-to-peer communication system

Crypto-currency runs by consensus. There is a peer-to-peer protocol where all the computers in the world running the software communicate with each other instantly. Various computers may join or leave the network at any second, but there are always a large number of them connected at any time. When I send a Bitcoin to my friend, the signed transaction is broadcast over the entire network. In this sense, Bitcoin transactions are fully transparent and instantly verifiable.

The same peer-to-peer nature is what makes Bitcoin so threatening to existing infrastructure. There is no central entity to sue, arrest, embargo, or otherwise attack. No central bank can print more of them. No politician can influence the supply. (Although I'm sure they're trying to figure out a way.) The entire system simply lives in the cloud of the Internet. This also makes the system extremely resistant to fraud or manipulation. With nobody in charge, there is nobody with authority to do anything fraudulent. As Bitcoins become more popular, there are more peers in the node, spread all over the world. Growth in popularity is truly growth in security.

Guarantee against "double spend"

One big concern with any crypto-currency is the issue of double spending. Transaction signing, as explained above, allows for absolute verification of authenticity, but it doesn't prevent me from sending the same payment to multiple people. Someone dishonest could simply keep spending the same Bitcoin over and over again. Fortunately, this has been anticipated and accounted for. Double spend is prevented in two distinct ways. Initially, a transaction is broadcast to the entire peer-to-peer network. If the same Bitcoin is broadcast, but with a different recipient, multiple peers on the network will immediately reject it in error. The second protection against double spend happens during the mining stage, which is explained in the next section.

Bitcoin, for example, is designed so that there will eventually only be 21 million units in existence

"Mining" new currency

Crypto-currency has to come from somewhere. If a few billion dollars' worth simply appeared overnight, they would have no value (no quantitative easing here!). Furthermore, if anyone could simply invent a digital number, calling it currency, then the asset would have no value. There needs to be a way to introduce the concept of "work" into creating units of the asset. The term "mining" is used, as people like to compare the work of creating crypto-currency to the mining of gold. Both reward you, hopefully, with some units of the asset in return for your hard work.

Mining is performed by solving a massively difficult mathematical problem. There is no closed-form solution, so millions of iterations of random numbers must be attempted in order to find the solution. Depending on the speed of your hardware, and various other factors, it could take months to solve the problem. Each time a problem is solved, the winner is awarded some units of the asset by the system. (For example, the current Bitcoin reward is 25 Bitcoins.) However, the reward is not guaranteed to every participant. It is a race to the finish, with the first person finding the solution collecting the prize. I've met several people who generate anywhere from US$100 to US$1000 per day mining, although those amounts are getting harder and harder to produce.

The profitability of mining has given rise to an entirely new industry that produces specialized hardware just for this purpose. Technology started with desktop computers a few years ago, moved to GPU chips, then on to FPGA, and finally to custom-built ASIC chips. You can easily spend US$5000 or more on a mining system.

It would seem like mining is an easy way to generate a steady revenue stream. Even if you had doubts as to the long-term value of the asset, mining profits could be converted to your favorite currency immediately. However, the system has a built-in safety valve that makes things difficult. Bitcoin, for example, is designed so that there will eventually only be 21 million units in existence. The growth is strictly regulated to ensure that this total will not be reached until around 2140. This controlled supply policy was designed to taper off slowly and approximately match the mining rate of gold. (You can read the exact details at: https://en.bitcoin.it/wiki/Controlled_supply.)

Privacy and anonymity (not the same thing)

People are often confused by the supposed anonymity of crypto-currency. While individual addresses may be anonymous, the actual transactions are not. The strength of the entire system relies on the peer-to-peer transaction log discussed above. This means that every transaction to and from every address is visible. I've literally downloaded every transaction in Bitcoin history to my laptop. It's all there for anyone to see. You could even find the first Bitcoin ever generated and trace its entire history. The issue is that every address is just a string of characters. So, if you don't know who is attached to that address, you don't know who conducted the transaction. So, while the transactions are public, the people behind them are not. As an example, you can see the full transaction history of any address by visiting www.blockchain.info.

If a merchant only has a single address for receiving payment, someone could look at the transaction log and know their exact revenue at any time. This is one of the reasons for a suggested protocol to use different public addresses for every transaction, or at least every person you deal with. This way, no person can see the transaction beyond the address they used. Bitcoin allows for an almost unlimited number of receiving addresses.

To summarize, the level of privacy or anonymity depends directly on how you choose to interact with the system.

The future

There has been a lot of debate about just what the future holds for crypto-currencies. Some traditional finance people see it as a "flash-in-the-pan" destined for an early death. They remind me of someone I met years ago who referred to the Internet as "Just another kind of CB radio," which had no future and would also die out quickly. Some people just fail to see the potential of new paradigms.

From what I've seen, heard, and read, there is a massive groundswell of entrepreneurs, investors, venture capitalists, and innovators all working around the clock to leverage this exciting new space. Undoubtedly, many will fail. But, some will succeed and the currency will continue to grow.

I'll end with a quote. When asked about challenging the Fed, Yifu Guo, founder of Avalon Miner, simply said, "It's not about trying to beat the system, we're just going to ignore it."

About the Author

Noah Silverman is a data scientist, quant, machine learning expert, and entrepreneur. He has a consulting business, Smart Media Incorporated, at: www.smartmediacorp.com. Noah is also a doctoral candidate in statistics at UCLA and expects to complete his PhD by December 2013.