International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 5 –NOVEMBER 2014.

Bitcoin: A Peer-to-Peer Online Virtual Currency, Better Alternative to Real Money

G.Baleswari

Asst. Professor, Department of CSE, UshaRama College of Engg & Tech, Telaprolu, Vijayawada, A.P., India

Abstract— Money has had a long history – millennia in length. The common theme amongst all of these currencies is that a trust agreement amongst its users, that particular currency held value. Although people use different mediums of digital currency through video games, Moneypak, and mobile web apps, an entirely standalone currency is revolutionizing the way we perceive money. Bitcoin is the first decentralized digital currency and it's pushing the envelope toward a new virtual economy. Bitcoin, a peer-to-peer online virtual currency, is leading the trend of digital currencies around the world. It is decentralized, meaning there is no central bank or hub where Bitcoins are created and it's purely digital, meaning a physical representation of the currency is not needed. In this paper, we addressed many issues related to bitcoin.

Index Terms— Bitcoin, e-cash system, irreversible, peer-to-peer network, Minting.

I. INTRODUCTION

Bitcoin is a decentralized electronic cash system initially designed and developed by Satoshi Nakamoto (whose name is conjectured to be fake by some, and who has not been heard from since April 2011). The design of Bitcoin was first described in a self-published paper by Nakamoto [14] in October 2008, after which an open-source project was registered on source forge. The genesis block was established on January 3rd 2009, and the project was announced on the Cryptography mailing list on January 11th 2009. Since its invention, Bitcoin has gained amazing popularity and much attention from the press. At the time of the writing, approximately 7M Bitcoins are in circulation; approximately USD $2M to $5M worth of transactions take place each day in Bitcoin; and about eighteen Bitcoin exchanges exist offering exchange services with many real world currencies, (e.g., EUR, USD, CAD, GBP, PLN, JPY, HKD, SEK, AUD, CHF, and so on). Bitcoin's exchange rate has varied widely, reaching as high as USD $30 per Bitcoin although at the time of writing is around USD $5 per Bitcoin. Despite some pessimists' critiques and disbelief, Bitcoin has admittedly witnessed enormous success since its invention. To the security and cryptographic community, the idea of digital currency or electronic cash is by no means new. As early as 1982, Chaum has outlined his blueprint of an anonymous e-cash scheme in his pioneering paper [10]. Ever since then, hundreds of academic papers have been published to improve the efficiency and security of e-cash constructions

Creation of Bitcoin is as different from bank funds' creation as cash is from electrons. It is not controlled by a government's central bank, but rather by consensus of its users and nodes. It is not created by a limited mint in a building, but rather by distributed open source software and computing. After an in-depth investigation of Bitcoin, it found that although Bitcoin uses no fancy cryptography, its design actually reflects a surprising amount of ingenuity and sophistication. Most importantly, it addresses the incentive problems most expeditiously. The first BitCoins were in a block of 50 (the "Genesis lock") created by Satoshi Nakomoto in January 2009. It didn't really have any value at first. It was just a cryptographer's plaything based on a paper published two months earlier by Nakomoto.

Once the Genesis Block was created, BitCoins have since been generated by doing the work of keeping track of all transactions for all BitCoins as a kind of public ledger. The nodes / computers doing the calculations on the ledger are rewarded for doing so. For each set of successful calculations, the node is rewarded with a certain amount of BitCoin ("BTC"), which are then newly generated into the BitCoin ecosystem. Hence the term, "BitCoin Miner" – because the process creates new BTC. As the supply of BTC increases, and as the number of transactions increases, the work necessary to update the public ledger gets harder and more complex. As a result, the number of new BTC into the system is designed to be about 50 BTC (one block) every 10 minutes, worldwide. Even though the computing power for mining BitCoin (and for updating the public ledger) is currently increasing exponentially, so is the complexity of the math problem (which, incidentally, also requires a certain amount of guessing), or "proof" needed to mine BitCoin and to settle the transactional books at any given moment. So the system still only generates one 50 BTC block every 10 minutes, or 2106 blocks every 2 weeks. So, in a sense, everyone keeps track of it – that is, all the nodes in the network keep track of the history of every single BitCoin.

.

Fig 1: Bitcoin Inventor : Mr.satoshi nakamoto

There is a maximum number of BitCoin that can ever be generated, and that number is 21 million. According to the Khan Academy, the number is expected to top out around the year 2140.As of, this morning there were 12.1 million BTC in circulation Our own BitCoin are kept in a file (our BitCoin wallet) in our own storage – our computer. The file itself is proof of the number of BTC we have, and it can move with we on a mobile device. If that file with the cryptographic key in our wallet gets lost, so does our supply of BitCoin funds. And we can't get it back.

The value varies based on how much people think it's worth – just like in the exchange of "real money." But because there is no central authority trying to keep the value around a certain level, it can vary more dynamically. The first BTC were basically worth nothing at the time, but those BTC still exist. As of 11AM on December 11, 2013, the public value was $906.00 US per BitCoin. When I finished writing this sentence, it was $900.00. Around the beginning of 2013, the value was around $20.00 US. On November 27, 2013 it was valued at more than $1,000.00 US per BTC. So it's kind of volatile at the moment, but it's expected to settle down.

Fig 2: Official Logo of Bitcoin

II. HOW DOES BITCOIN WORK?

The crux of Bitcoin is based on its block chain, or a large set of data that represents every Bitcoin transaction. All purchases are recorded in the block chain, confirming an owner's possession of Bitcoins. When we download a Bitcoin wallet, we are downloading the block chain, so every user has a copy of the entire network. Once we've downloaded a Bitcoin wallet, the program generates an address by which we will receive Bitcoins. We're then officially ready to begin scouring the web for Bitcoins and products that can be purchased with them. It sounds more technical in theory, but the process is easy. We simply download the wallet program and use it to purchase or receive Bitcoins.

III. HOW SUCCESSFUL IS BITCOIN?

The value of this digital currency depends solely on its perceived success with its users, and so far Bitcoin's solid user base believes it holds the potential to be the universal digital currency standard. MtGox.com, the longest running Bitcoin exchange website, estimates that one Bitcoin is worth nearly $150USD as of April 2013. In December 2012, French bank Aqoba began accepting Bitcoin accounts, backing the digital currency. In February 2013, MegaUpload founder Kim Dotcom publically announced his affinity for Bitcoin and provided Bitcoin payment methods for his new MegaUpload site. The digital entrepreneur also expressed interest in creating a Bitcoin credit card. Bitcoin has surged since then, jumping to more than 200 USD in April. Many other websites are opening up to Bitcoin, either by soliciting donations or allowing purchased through the currency. The website Bitspend.net, for example, allows any user to purchase items using Bitcoins from more popular sites like eBay or amazon.com, something the two websites do not permit. Bitcoin has become so successful, the Financial Crime Enforcement Network (FinCEN) has issued new guidelines for Bitcoin's legal status in the U.S.

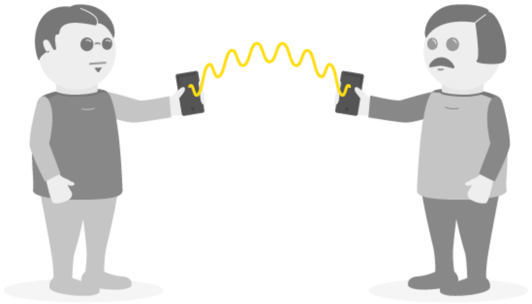

Fig 3: People can send bitcoins to each other using mobile apps or their computers

Bitcoin uses no fancy cryptography; its design actually reflects a surprising amount of ingenuity and sophistication. Most importantly, it addresses the incentive problems most expeditiously.

No central point of trust: Bitcoin has a completely distributed architecture, without any single trusted entity. Bitcoin assumes that the majority of nodes in its network are honest, and resorts to a majority vote mechanism for double spending avoidance, and dispute resolution. In contrast, most e-cash schemes require a centralized bank that is trusted for purposes of e-cash issuance, and double-spending detection. This greatly appeals to individuals who wish for a freely-traded currency not in control by any governments, banks, or authorities.

Incentives and economic system: Bitcoin's eco-system is ingeniously designed, and ensures that users have economic incentives to participate. First, the generation of new bitcoins happens in a distributed fashion at a predictable rate: "bitcoin miners" solve computational puzzles to generate new bitcoins, and this process is closely coupled with the verification of previous transactions.

Predictable money supply. Bitcoin makes sure that new coins will be minted at a fixed rate, that is, the larger the Bitcoin community and the total computational resource devoted to coin generation, the more difficult the computational puzzle becomes. This provides strong incentives for early adopters — the earlier in the game, the cheaper the coins minted.

Divisibility and fungibility. One practical appeal of Bitcoin is the ease with which coins can be both divided and recombined to create essentially any denomination possible.This is an Achilles' heel of (strongly anonymous) e-cash systems, because denominations had to be standardized to be unlinkable, which incidentally makes the computational cost of e-cash transactions linear in the amount. In Bitcoin, linkage is inherent, as it is what prevents double spending; but it is the identities that are "anonymous".

Versatility, openness, and vibrancy. Bitcoin is remarkably flexible partly due to its completely distributed design. The open-source nature of the project entices the creation of new applications and spurs new businesses. Because of its flexibility and openness, a rich extended ecosystem surrounding Bitcoin is flourishing. For example, mixer services have spawned to cater to users who need better anonymity guarantees. There are payment processor services that offer gadgets venders can embed in their webpages to receive Bitcoin payments alongside regular currency.

Transaction irreversibility. Bitcoin transactions quickly become irreversible. This attracts a niche market where vendors are concerned about credit-card fraud and chargebacks. Through personal communication with a vendor selling specialty magazines, he mentioned that before, he could not conduct business with customers in certain countries where credit-card fraud prevails. With Bitcoin, he is able to extend his business to these countries due to the protection he obtains from the irreversibility of transactions. Low fees and friction. The Bitcoin verifiers' market currently bears very low transaction fees (which are optional and chosen by the payer); this can be attractive in micropayments where fees can dominate. Bitcoin is also appealing for its lack of additional costs traditionally tacked upon international money transfers, due to disintermediation. Readily available implementations. Last but not the least, in comparison with other ecash schemes, Bitcoin has provided readily available implementations, not only for the desktop computer, but also for mobile phones. The open-source project is maintained by a vibrant community, and has had healthy developments.

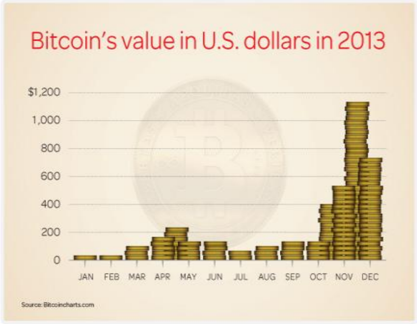

Fig 4: Bitcoin Value in USD

IV. MALWARE ATTACKS

Reported malware attacks on Bitcoin are on the rise, resulting in the theft of private keys. The online wallet service mybitcoin.com recently lost $1:3 million worth of users' coins due to malware [1]. Several solutions can be envisaged; we mention: Threshold cryptography. A natural countermeasure to malware is to split private keys into random shares, using standard threshold cryptography techniques, and distribute them onto multiple locations, e.g., a user's desktop computer, her smart phone, and an online service provider. In this way, only when a threshold number of these devices collaborate, can a user spend her coins. Of course, doing so can harm the usability of the system, since coins can no longer be spent without operating multiple devices (even though not all the devices but only a chosen number of them are needed at once). Super-wallets. To address the usability concern, we propose the simple idea of superwallet, i.e., a user's "personal bank" where most of her coins are stored. The superwallet is split across multiple computing devices, using threshold techniques as above. In addition, the user carries a small sub-wallet with her on her smartphone. Pre-approved transactions are setup so that the user can withdraw money from her super-wallet onto her sub-wallet, periodically in small amounts (similar to how real banks let people withdraw cash from ATMs today). The user now only needs her smartphone to spend money in her wallet, and in case her smartphone is captured by an adversary, the user only loses the small amount of money that she has in her wallet, but not that in her personal bank. Large amounts can always be spent from the super-wallet using a threshold of devices. Both approaches can be implemented as backward-compatible and incrementally deployable wrappers, requiring changes in the signature generation but not verification.

V. Conclusion

We have provided a preliminary but broad study of the crypto-monetary phenomenon Bitcoin, whose popularity has far overtaken the e-cash systems based on decades of research. Bitcoin's appeal lies in its simplicity, flexibility, and decentralization, making it easy to grasp but hard to subvert. We studied this curious contraption with a critical eye, trying to gauge its strengths and expose its flaws, suggesting solutions and research directions. The global peer-to-peer networking protocol that's behind Bitcoin and others like it is intrinsically decentralized, with no central issuer or network operation. That makes it difficult—if not impossible—for an entity such as the Federal Reserve Board to intervene. The Federal Reserve simply doesn't have the authority to supervise or regulate Bitcoin in any way. Our conclusion is, while the instantiation is impaired by its poor parameters, the core design could support a robust decentralized currency if done right.

VI. REFERENCES

[1] Bitcoin ewallet vanishes from internet. www.tribbleagency.com/?p=8133.
[2] Bitcoin wiki: Contracts. en.bitcoin.it/wiki/Contracts.
[3] Bitomat loses data and mybitcoin shuts down. www.launch.is/blog.
[4] Deflationary spiral. en.bitcoin.it/wiki/Deflationary spiral.
[5] M. Abdalla, X. Boyen, C. Chevalier, and D. Pointcheval. Distributed public-key cryptography from weak secrets. Proc. PKC, 2009.
[6] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar. On bitcoin and red balloons.research.microsoft.com/pubs/156072/bitcoin.pdf, 2011.
[7] X. Boyen. Halting password puzzles. Proc. Usenix Security, 2007.
[8] J. Camenisch, S. Hohenberger, and A. Lysyanskaya. Compact e-cash. Proc. Eurocrypt, 2005.
[9] S. Canard and A. Gouget. Divisible e-cash systems can be truly anonymous. Eurocrypt '07.
[10] D. Chaum. Blind signatures for untraceable payments. Proc. Crypto, 1982.
[11] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Secure distributed key generation for discrete-log based cryptosystems. J. Cryptology, 2007.
[12] B. Laurie. Decentralised currencies are probably impossible but let's at least make them efficient. www.links.org/files/decentralised-currencies.pdf.
[13] P. MacKenzie and M. Reiter. Two-party generation of DSA signatures. Proc. Crypto, 2001.
[14] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. www.bitcoin.org.
[15] T. Okamoto. An efficient divisible electronic cash scheme. Proc. Crypto, 1995.
[16] K. Poulsen. New malware steals your bitcoin. wired.com/threatlevel/2011/06.
[17] F. Reid and M. Harrigan. An analysis of anonymity in the bitcoin system. Arxiv:1107.4524.