Bitcoins Integrity and reliability.

GMIT

Conor Tighe

Abstract

Bitcoin has become one of the staple technologies of the information age revolutionizing the way people trade goods and services online while inspiring many other cryptocurrency's that have followed since its creation. In last August/early September of 2017 bitcoins value reached an all-time high of 3903.06 euro and validating its credibility to many who doubted it would last as far as 2017. But still many in the technology and economics industries doubt its stability and usability, labelling the currency as a 'bubble' with no real-world use. This could be a result of bitcoins volatility through-out the years. An excellent research paper by Benjamin M.Blau on bitcoins Price dynamics and speculative trading in bitcoin found that "during 2013, speculative trading contributed to the unprecedented rise and subsequent crash in Bitcoin's value nor do we find that speculative trading is directly associated with Bitcoin's unusual level of volatility". I found that the anonymity of its creator also creates unease among some, as they bring in to question the founder of bitcoins motivations and how reliable this unnamed individual is if the block chain faces problems in the future. With bitcoins independency from government regulation and low transaction fees still many retailers and investors are strong believers in the cryptocurrency.

Contents

Chapter 1

Introduction

Bitcoin is a cryptocurrency published on the 31 October 2008 by an unknown programmer or group of programmers under the name of Satoshi Nakamoto. It was the first decentralized digital currency that did not require overhead administration by an organization or individual. Along with the publication of the currency came a research paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" explained how the system operates and protects the coins and users. The paper went on to describe a peer-to-peer system that uses a "network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed", this system would become known as the block-chain or honest-chain. The block-chain is the underlying technology behind bitcoins independence from governments and banks. Users of the cryptocurrency did not have to rely on outside intervention from a 3rd party for their online transactions as this mathematical proof-of-work approach eliminated the need for each person involved to give their identities to the 3rd party. The block-chain has proven itself to be an efficient and fast approach to handling online transactions by the sheer popularity of bitcoin and its daily use across the world. Lucinda Shen from Fortune.com stated in an article when discussing the incorporation of a block chain by banks in 2017 that after surveying 200 global banks its reported that 15% of banks worldwide plan to use the blockchain for their transactions. The invention of the block-chain itself could be considered just as innovative as bitcoins with many other cryptocurrencies like Ethereum using the design pattern for coin circulation. The block-chain that is referred to when talking about bitcoin is known as the honest chain, which is powered by the collective CPU processing power of hardware around the work known as miners. These machines vary from high performance computers to pools of less efficient computers working together but all the systems contributing share the same goal. Roughly every 10 minutes mining computers will collect a group of pending transactions know in the block-chain as a block and use it to create a mathematical puzzle. The first miner to solve the puzzle will announce it to the rest of the network, then other miners will validate the solution while checking if the person sending has enough in their bitcoin wallet balance to complete the transaction. Once enough miners approve the block it is added to the ledger which is updated across the network. The incentive for these miners to contribute to the block chain is for every solution to a block found bitcoins are given as a reward as of now. This reward was 50 bitcoins before it was halved on the 28th of November 2012, it halved again on 7th of October 2016 to become the current reward of 12.5 and will eventually drop to 6.25. This is because the reward schedule set by Satoshi Nakamoto is the only way to create new bitcoin and with a cap of 21 million bitcoins to be allowed to exist the reward for mining bitcoins is set to half ever 4 years. 16,579,938 bitcoins have been mined so far with an average of 1800 being mined each day the next halve should take place on the 15 Jun 2020, this process will continue until the reward payout has halved a total of 32 times and the final bitcoins are released to the world at 0.00000042 bitcoins per block. Since there are no organization overseeing bitcoin once a password to a wallet is forgotten the bitcoins are lost forever, it is estimated that up to 25% have been lost for good. These bitcoins are not destroyed just made inactive, “Lost coins only make everyone else’s coins worth slightly more. Think of it as a donation to everyone.” - Satoshi Nakamoto. Bitcoin has reached milestones that any thought would never come with the blockchain sustaining it for 9 years, but it this enough evidence to consider bitcoin a legitimate currency beyond digital gold? how reliable this proof of work system is and how can we tell if the bitcoins that utilize it have a practical future?