

# Currency 3.0: Examining Crypto Currency

Jesse Grushack

Advisors: Prof. Chris Fernandes & Prof. Brad Lewis



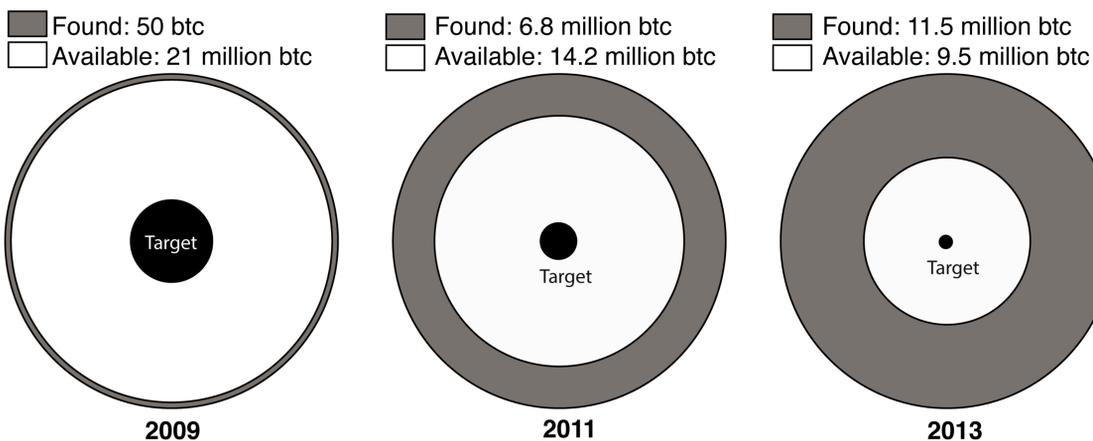
## Abstract

Money was originally backed by gold, a commodity, but is currently backed by the government. But what if money could be backed by mathematics? The purpose of this project is to explore what may be considered the future of money, a virtual payment protocol known as cryptocurrencies. Bitcoin was the first crypto-coin system and currency which has increased in value by over 500% in the past year. But why should people trust a system when everything else on the internet has the ability to be manipulated? This project explores the security of this network and what makes it unbreakable. The project also examines the economic possibilities of having a global distributed trust network. These new technologies will not only play a major part in shaping our future but have potential to change society as we currently know it.

## Bitcoins

- Defined by Google, a bitcoin is “a digital currency in which transactions can be performed without the need for a central bank.”
- Bitcoins operate on a p2p decentralized network controlled by a distributed global ledger system called the block chain.
- Bitcoins can be easily transferred anywhere in the world almost instantly, with very low fees.
- As supply decreases, so does the ability to find bitcoin, like aiming for a shrinking bullseye on a shrinking board.

Bitcoin Supply vs Time



## The Block Chain

- The block chain records all transactions within the Bitcoin network
- The system is maintained by a network of ‘miners’ who are rewarded with bitcoins for keeping the network active and the block chain secure
- Transactions are protected by hashing a message using the SHA-256 algorithm and confirming ‘proof of work’ then combined to form binary trees, built from the bottom up, with any unauthorized change affecting the entire chain

## A ‘Web of Trust’

- Switching to a block chain based web of trust system could save millions of dollars when implemented into an established system such as Ticketmaster saving millions in fees, cutting back on fraud/scalpers, and improving customer experience
- Corporations like Western Union would have to lower fees to compete in money sending
- As long as there remains incentive for users to maintain the network, a third party or central authority is not needed

