Bitcoin Protocol: Model of 'Cryptographic Proof' Based Global Crypto-Currency & Electronic Payments System
Download the PDF research reports titled:

Future of Bitcoin & Statistical Probabilistic Quantitative Methods:
Global Financial Regulation (Interview: Hong Kong Institute of CPAs)

Bitcoin Protocol: Model of 'Cryptographic Proof' Based
Global Crypto-Currency & Electronic Payments System

Bitcoin Protocol: Model of 'Cryptographic Proof' Based Global Crypto-Currency & Electronic Payments System

Yogesh Malhotra, PhD
www.yogeshmalhotra.com

Griffiss Cyberspace, Global Risk Management Network, LLC
306 Market St., Griffiss Air Force Base, Rome, NY 13441, U.S.A.
www.FinRM.org

"The much-vaunted security of [Bitcoin's] underlying protocol has also been questioned. "Several risks, threats, and vulnerabilities are inherent in the design of the bitcoin protocol which is susceptible to cryptographic vulnerabilities," says Yogesh Malhotra, Chief Research Scientist at Global Risk Management Network..." - ***Hong Kong Institute of Certified Public Accountants Magazine*, A+, 10(2), February 2014.**

"Tokyo-based bitcoin exchange Mt. Gox filed for bankruptcy last week, saying hackers had stolen the equivalent of $460 million from its online coffers. The news rocked the bitcoin world, and it could even bring down the much-hyped digital currency."
- The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster, *Wired*, March 03, 2014.

"Bitcoin price volatility implies huge market risk." - Economist Nouriel Roubini
- Roubini launches stinging attack on bitcoin, *CNBC*, March 10, 2014.

December 04, 2013

This research report represents the first known attempt with specific technical focus on cryptographic 'proof of work' in the context of virtual crypto-currencies such as Bitcoin. The cryptography, encryption and cryptanalysis technical focus of the report is intentional and related to Bitcoin's innovative capabilities, vulnerabilities and threats. Situated somewhere along the trajectory between real money and quantum money, virtual crypto-currencies based upon 'cryptographic proof' represent a natural stage in the evolution of global finance. The feasibility and large-scale global implementation of Bitcoin as a crypto-currency has earned it admiration as a remarkable conceptual and technical achievement and an elegant solution. Its cryptographic solution enables creation and regulation of issue of crypto-currency, preventing its counterfeiting and double-spending, and securing its global transmission at minimal transaction cost while using little time. Central to all those interesting innovations is the cryptographic 'proof of work' supplanting trust in a third-party that is the central focus of the current study.

"The bitcoin protocol provides an elegant solution to the problem of creating a digital currency—i.e., how to regulate its issue, defeat counterfeiting and double-spending, and ensure that it can be conveyed safely—without relying on a single authority... It represents a remarkable conceptual and technical achievement, which may well be used by existing financial institutions (which could issue their own bitcoins) or even by governments themselves."
-- **The Federal Reserve Bank of Chicago**, *Chicago Fed Letter*, December 2013, No. 317

Bitcoin Protocol: Model of 'Cryptographic Proof' Based Global Crypto-Currency & Electronic Payments System

Abstract

"For the importance of money essentially flows from its being a link between the present and the future."
-- *The General Theory of Employment, Interest, and Money*, John Maynard Keynes, 1935

"You can know the name of a bird in all the languages of the world, but when you're finished, you'll know absolutely nothing whatever about the bird... So let's look at the bird and see what it's doing -- that's what counts."
-- "What is Science?" *The Physics Teacher*, 1969, Richard P. Feynman

Money is an interesting construct that continues to occupy the fancy of many ranging from economists to quantum physicists. Virtual crypto-currencies enabled by global interconnectivity and 'cryptographic proof of work' represent a natural stage in the evolution of virtual global financial transactions and exchange. Bitcoin is one such crypto-currency that seems to be a 'remarkable conceptual and technical achievement' and 'an elegant solution' to creating a digital currency, regulating its issue, countering counterfeiting and double-spending, and ensuring secure transmission without relying on a single authority. Central to the interesting innovation is the cryptographic 'proof of work' that supplants trust in any third-party in enabling exchange of value. This research report is the first known attempt to specifically focus on cryptographic 'proof of work' in the context of Bitcoin and how it really works in enabling Bitcoin's innovative capabilities. It also analyzes the mystery shrouding Bitcoin's origin trying to examine if it is a cryptographic protocol, virtual currency, financial instrument, or *something else*. Central focus is on Bitcoin's cryptographic proof based P2P electronic payment system with focus on Bitcoin addresses and public key cryptography, transactions and ECDSA-based digital signatures, time-stamping and organizations of transactions into blocks, and mining of cryptographic proof to create the transaction block chain and enable trust. Some perspective of the multi-billion dollar 'Bitcoin economy' is also provided in the context of analysis of Bitcoin mining and cryptographic proof computing power requirements. Potential weaknesses in Bitcoin's security and encryption protocols and recently highlighted key security vulnerabilities and attacks including lack of perceived user identification anonymity are discussed.

Introduction: *Virtual* Currency: Beginning of the End of *Real* Money?

The *IEEE Spectrum* special report Future of Money heralding 'The Beginning of The End of Cash' chronicles growing trend of virtual currency transactions. It outlines growing use of centralized and decentralized digital cash such as Bitcoin. Beyond virtual currencies, it discusses how quantum computing developments will enable quantum money, i.e., real