Bitcoin for E-Commerce:
Principles and Applications

E

Xunhua Wang
James Madison University, USA

Brett Tjaden
James Madison University, USA

M. Hossain Heydari
James Madison University, USA

INTRODUCTION

Amateurs study cryptography; professionals study economics – Allan Schiffman, 2 July 2004

Few people took note on January 8th, 2009, when an email (see Figure 1) was sent to the cryptography mailing list to announce the first release of a new electronic cash system, called *Bitcoin* (Nakamoto, 2008). About four and half years later, when Ross William Ulbricht was arrested in October, 2013 for allegedly running the online black market Silk Road where Bitcoin was adopted as the payment system (Grossman & Newton-Small, 2013), Bitcoin was already well known, if not widely used. Today Bitcoin is traded on exchange markets for several hundred dollars per coin unit, and merchants such as Amazon, eBay, and Target now accept bitcoin payments.

Figure 1. The 2009 email announcing Bitcoin v0.1

Bitcoin v0.1 released
owner-cryptography@metzdowd.com [owner-cryptography@metzdowd.com] on behalf of Satoshi Nakamoto [satoshi@vistomail.com]

Sent: Thursday, January 08, 2009 2:27 PM
To: cryptography@metzdowd.com

Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

See bitcoin.org for screenshots.

Download link:
http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

Windows only for now. Open source C++ code is included.

- Unpack the files into a directory
- Run BITCOIN.EXE
- It automatically connects to other nodes

DOI: 10.4018/978-1-4666-9787-4.ch072

So, what is Bitcoin? How does it work? Why do people accept it? What is its future? How will it affect electronic commerce? Despite significant media coverage on Bitcoin (Goodman, 2014; Andreessen, 2014; Grossman & Newton-Small, 2013) and quick adoption of Bitcoin by an increasing number of merchants, the complex technical details of Bitcoin remain elusive to both the general public and many professionals. This chapter aims to answer all these questions in a straightforward manner.

Commodity Cash and Fiat Cash: Double Spending and Anonymity

The history of cash can be dated back to 7th Century BC, if not earlier, when Lydia used the first standardized metal coins (Surowiecki, 2012; Davies, 2002). Before that, two persons conducted trades through bartering, when each side had what the other wanted and the values of the goods were considered equivalent (Acton & O'Grady, 2007). Cash was invented to make trading easier by allowing merchants to defer consumption (i.e., one's selling and buying do not have to happen simultaneously) and measure the values of different goods (Surowiecki, 2012). Essentially, cash serves a medium of exchange.

In addition to coins, other scarce items such as silver jewelry were also used as cash. These kinds of physical goods-based cash are *commodity money*.

Later, *paper bills* were introduced by Venetian merchants around the 12th century in the west and by Kublai Khan throughout China in around the 13th century (Surowiecki, 2012). Unlike commodity money based on scarce goods, paper bills can be created cheaply and in abundance, but this runs the risk of overprinting, which causes inflation and devalues the currency. As a result, to get widely accepted, paper bills are often supported by governments. At one time, paper bills were backed by gold held by central banks, and could be exchanged for a specific amount of gold. This is no longer the case with most national currencies, which are called *fiat money* since they have value only because a certain government decrees that they do.

Two points deserve more attention. First, commodity money is inherently hard to forge, due to the inherent value of the goods used for money (such as silver) and easy-to-forge goods do not make for good commodity money. As a result, commodity money is naturally immune to double spending: after Alice has spent her commodity money, she does not have it anymore and cannot double spend it. In contrast, paper bills do not have this inherent characteristic and could be forged if not property designed. To make it hard to clone/forge paper bills, many security features have been used in their printing, such as special paper, an enlarged off-center portrait, watermark, fine-line printing patterns, color-shifting ink, security thread, and micro-printing. These security features can be easily verified, either with naked eyes, a magnifier, or a special pen. It is worth noting that these existing security features on paper bills are not foolproof and government mints keep introducing new designs and features (such as those in the new $20 bill) against more advanced counterfeiting technologies.

An even less noticeable property of commodity money and fiat money is that they are hard to trace. Commodity money is naturally hard to trace because there is no trusted third party for tracking. Fiat cash does have a trusted third party, namely the issuer, but since cash does not directly flow back to the bank after it is spent, tracking is hard too. For example, Alice may withdraw a dollar bill, with a unique serial number on it, from her bank account and then give it to Bob for a can of soda. Later, Bob may spend this bill at another vendor. As long as the bill does not go back to the bank immediately, it will be hard for the bank to trace how Alice has spent the money and trace where Alice has been. In other words, paper bills have the property of anonymity, which is an essential building block for privacy and democracy. (Admittedly, anonymity has a dark side, as it makes money-laundering possible for criminals.)