SWCP Portal

June 2017

The revolution is in the way it works

Bitcoin Changes the Game

Exciting new technologies like the advance of **robotics** and **artificial intelligence** are busy transforming the world with new hardware and lots of computing power. But along with them comes another **emergent technology** that is quite revolutionary but has not gotten quite so much buzz, possibly because it is so complex that few truly understand how it all works.

This new system of doing things was first proposed by an unknown designer less than a decade ago in a **paper** so visionary it could be from another planet. Moreoever, these ideas led to open-source collaboration with others around the globe which soon spawned the world's first totally online digital currency, **Bitcoin**.

Bitcoin and other **internet-based currencies** are already changing the world of ecommerce, for both good and ill. Unlike other forms of money, Bitcoin is not backed by governments or central banks but by self-interest and voluntary cooperation, yet is as portable as "real" cash is.

There are no middlemen, fees, or currency conversion worries, and transactions are basically anonymous. The whole system is a worldwide, uncentralized, peer-to-peer network running the Bitcoin software, which is all **open-source.**

No actual paper or metal tokens are involved; it's all digital. People who buy Bitcoins store their access information in an **electronic wallet** associated with their address, from which they can spend coins or acquire more using encryption.

Bitcoin is an incredibly clever system, but the real genius lays in the **blockchain** bookkeeping technology that is its foundation. **Blockchains** are being proposed as a solution to everything from ending hunger to copy protection to online voting – and it may not be all **hype**, either.

Digital double-dealing

The main difference between things in physical space and those in cyberspace is **mass**. Physical objects possess weight and volume because they are made out of smaller physical objects. Digital objects, on the other hand, do not have such characteristics. They are made out of **data**, information which is utterly weightless.

Therefore, manipulating, and in particular, duplicating physical objects is hard. Not so with data. Information *loves* to be duplicated – in fact, that's the only way it moves about online, by being copied from one location to the next. When Alice sends Bob an email, for example, the original never leaves her computer, but is copied from one server to the next and finally replicated onto Bob's device when he downloads it.

Yet Alice could *also* send the same email to Charlie or Denise or anyone else and Bob would be none the wiser. Not so with physical objects. If Alice gives Bob an apple, she cannot give the same apple to anyone else. This situation creates headaches for information management, but an almost unsolvable quandary for spending cash.

This is the infamous **double-spending** problem. To prevent any funny business, online economic transactions must be rigorously tracked, which is what banks and credit card companies do. They spend a lot of resources to prevent that data from being altered or stolen by outside parties.

But such security comes with a price, and not just in added fees. Such providers know where the money comes from and where it goes, raising privacy concerns for ordinary folks, activists, and entrepreneurs as well as criminals.

Hence Bitcoin's big innovation: the **blockchain**, a massive and ever-growing system of distributed online ledgers. Sections of it, or *blocks*, are stored on all Bitcoin users' computers rather than in one central repository and are all linked in succession, or *chained* together, hence the name. They work together in concert, recording all Bitcoin transactions with **timestamps** so one person cannot spend the same coin twice, nor can the data in one part of the ledger be easily altered as that block would not match others.

That's the part that's easy to understand. How Bitcoin actually works involves **public key encryption** for privacy, very high-powered **math wizardry** to generate new Bitcoins, and ingenious social engineering, too, to motivate people to maintain and extend the blockchain.

Mining by the numbers

Since the blockchain **database** records all transactions made since it began in 2009, it's constantly getting bigger. Now it's around 100 GB. However, the longer it gets, the more trustworthy the chain becomes, as it becomes harder to surreptitiously alter data across the expanse.

The reason for this is that database is managed autonomously, kept secure with complicated number-crunching operations which produce **hashes** – numerical summations of the contents that show any changes as they are then used in the next block. To get people to devote computing power to the effort, called "**mining**", they are rewarded with the creation of new Bitcoins.

This is carefully calculated to be barely profitable, and there is an **upper limit** to the number of Bitcoins of 21 million that will be reached around 2140. Payouts are skewed so that early miners got rewarded more than later ones will.

What this does is create a kind of **artificial scarcity** to maintain value. It seems to work – starting at $.05/coin back in 2010, prices have soared recently to around $2400. There have been many **fluctuations,** a few from **software bugs**, but most due to good old supply and demand.

From out of nowhere

There are **scams**, of course, as hucksters attempt to deceive newcomers, but suspicions on whether or not the entire system is bogus rest to a large degree on its mysterious origin. The design of Bitcoin was first put forth in a **paper** authored by "**Satoshi Nakamoto"** in 2008.

Just exactly who this person (or persons) was remains a mystery, though there have been **many individuals** fingered as possible suspects. Whoever he, she, or they, are or were, the scheme produced is one of undeniable genius. One that paid off very well, too. As one of the first, though not the only miner, Satoshi created about a million Bitcoins for himself. This would result in a value today of about $2 billion.

So what is Bitcoin really, a **cryptocurrency**? Some kind of security? Is it taxable? How should or can it be regulated? Or is it all a scam, like an incredibly elaborate **Ponzi scheme**? These questions are still unresolved, as are concerns about its basic **legality**. The **FBI** in particular is worried about its wide adoption by online criminals.

Bitcoin is not the only **virtual currency** out there now, either, as more competitors emerge along with similar systems being developed by states and financial institutions, too. Regardless of its eventual fate, it is the blockchain itself that may be the most important thing to come out of it.

As a public digital ledger, blockchains can preserve, distribute, and validate other information than monetary values. **Blockchain applications** for online voting, supply chain management, medical records, property and copyright registry, and new insurance options are in the works. This may even lead to so-called "**smart contracts**" which would be automatically self-fulfilling.

One bold effort, **Ethereum**, seeks to decentralize the internet, changing it into a "world computer" where people own the information they create. With blockchains, the sky may be the limit.

Archived at: http://www.swcp.com/newsletters/.
Click on blue terms in PDF file to open links.