# The Magic of Blockchain

*Ayan Bhattacharya*
Baruch College, The City University of New York
New York, USA.

In October 2008, almost out of nowhere, a mysterious figure named Satoshi Nakamoto posted a short paper on cryptographic mailing lists describing an architecture that could – the paper claimed – replace existing centrally controlled currencies. Dismissed initially by the mainstream as a nerdish fantasy, interest in crypto currencies exploded abruptly last year. All of a sudden, it seemed that the financial press and investing public could not get enough of bitcoins and its cousins, and the daily gyrations of crypto markets quickly became the subject of animated discussions on coffee tables all around the world!

Many opine that the current crypto currency craze is a bubble, and that it may very well be. However, there is a growing realization – among researchers and practitioners alike – that the fundamental scaffolding on which bitcoins operate is indeed radical. This scaffolding is the Blockchain.

## 1. The Idea of Blockchain

Try teaching your grandma about the internet, and after the first few sessions there is the inevitable question – is WhatsApp the Internet – or, is Facebook the Internet – or otherwise, is Gmail the Internet? As you may have patiently explained, indeed WhatsApp, Facebook and Gmail are the Internet, but the Internet is much, much more. The relation between crypto currencies and the blockchain is similar. Bitcoins are an application built on top of blockchain. As interesting as bitcoins potentially are, the truly fundamental innovation is at the level of the blockchain.

At the most basic level, blockchains provide practical solutions to two inter-related problems in game theory and cryptography – creating common-knowledge and obtaining consensus – in a large population of independent entities. These were open questions in the fields for a long time. Complete technical details of the blockchain solution to these problems would require a lot of computer science jargon; however, the essence of the innovation can be captured through simplified analogies.

## 2. Blockchain and Consensus

To understand how a blockchain obtains consensus, let us turn to an analogy with the most popular consensus creating mechanism we humans have created – voting.

Suppose we have an honest distributed system. Distributed: means that each node is a stand-alone entity. Honest: means that at least a majority of the nodes in the system are non-corrupt ("nodes in a system" is really an abstract representation; a concrete realization could be anything, for instance a scattered population of voters). How can one poll such a distributed system so that one gets the honest majority's opinion? One way could be to undertake “conventional” voting -- one node, one vote. But simple voting is "cheap" and easy to rig in a distributed system. Suppose corrupt nodes send two votes instead of one, it would be very hard to detect, and the outcome is compromised. The first essential innovation of blockchain is to propose a robust alternative voting mechanism building on a technique called “proof-of-work”. What does that mean? Suppose there are multiple candidates in an election. Instead of simply asking the nodes to choose between candidates, a blockchain requires each node to solve a special kind of puzzle, and then attach their solution to the puzzle along with the vote. The class of puzzles that is used is another novelty and they involve specialized cryptographic techniques, but the idea can be explained through another analogy.

Suppose every node of the population is equipped with an infinite number of sealed boxes – each such box containing the 52 playing cards, with the Queen of Hearts on top. These boxes are special: they are very heavy; to shake a box (in other words, to shuffle one pack of cards), it takes a single node 20 seconds. At the end of 20 seconds, each node makes a mark indicating its vote on the box – that’s the vote – and submits as many boxes as it wants to. So technically, each node can submit more than one vote. Once all the boxes have been submitted, they are opened, and the number on the card at the top of the deck in each box is noted, along with the vote mark on the box. Now comes the catch – not all votes are taken as valid. Only if the card on top of a box is a King of Hearts, the vote is recorded; otherwise the vote is discarded. Importantly, no node knows which card has to be on top for the vote to be recorded – that's a secret – and it is different from the card that is initially on the top of each deck (for example, we had a Queen of Heart on top of each deck initially).

The above mechanism guarantees that the "probability of recording an honest vote" is greater than "probability of recording a corrupt vote", as long as the majority is honest. The guarantee comes from the randomization of the shuffle, and because the boxes are "heavy", and the card needed on top for the vote to be recorded is secret – and different from the card on top of the decks initially. Corrupt nodes can submit multiple boxes with corrupt votes, but unless the boxes have been shuffled, it is no good. And since it takes 20 seconds to shuffle, a corrupt node will have shuffled only one box when the boxes are collected. As one has multiple independent rounds of voting, since probabilities multiply, the difference in probabilities keep piling up. After sufficient number of rounds, we are almost guaranteed to record the honest opinion. That is the beauty of the blockchain: it is a computational solution to the problem of corrupt nodes. But that’s not all!

### 3. Blockchain and Common Knowledge

The examples above assumed that we have an honest aggregator of the votes. However, there is no reason to believe that election commissions will always stay impartial and honest! What if the arbiter of votes is itself corrupted? The blockhain handles this problem by doing away with the centralized vote aggregator completely, relying instead on a “public ledger”. A public ledger, in its most simple form, is like a giant scoreboard of live updating vote-counts that all entities can observe. The technical problem that a giant scoreboard addresses is one of common knowledge.

The apocryphal tale of the unfaithful wives is a good fable to explain the purpose of a public ledger (it might very well have been the tale of unfaithful husbands, just interchange the wife and husband in the story). The story goes something like this. In a quaint old village live a 100 married couples. Every evening the men of the village meet around a fire and praise the virtue of their faithful wives. However, if a husband suspects that his wife has been unfaithful, he invokes a curse at the fire that immediately turns his wife into a stone statue. If a wife is ever unfaithful, through some magical telepathic device, everyone in the village gets to know about the affair, except for the husband. Now suppose all women in the village are unfaithful. What happens? Nothing – because the husbands have no way of knowing. Due to the magical device, each husband thinks that the other wives are unfaithful, but he never gets to know about his own wife. For many years this village is thus a picture of tranquility with the husbands praising their wives every evening, till one day, a holy man comes and publicly declares that "a wife in this village has been unfaithful". For 99 days thereafter, all stays the same, with the husbands praising their virtuous wives, but on the 100th day, all the 100 ladies in the village become stone statues!

It is easy to see the reason for this calamity. From the magic device each husband knows that 99 other wives are unfaithful, so for 99 days a husband can hold on to the belief that his own wife is above suspicion. But if every husband in the village holds on to this belief for the 99 days, there are no curses invoked at the fire for 99 evenings, and thus everyone knows that everyone holds this beliefs. On the 100th day, this belief system has to unravel because at least one wife has been unfaithful. Thus you have the 100 stone statues on day 100. Game theorists use this fable to illustrate various finer points about knowledge, reasoning and belief. In reference to the blockchain, the main message is that without common knowledge the truth of a situation can stay distorted for indefinite amounts of time. Till the holy man's arrival, the husbands praise the wives at the fire even though the wives have been unfaithful. The holy man's declaration is like an announcement on a public billboard that everyone can see. The public ledger in the blockchain plays a similar role.

### 4. The Opportunity

The land of the blockchain today is like the terrain of the internet in the early 1990s. A bitcoin is like the Alta vista search engine or AOL chat tool: interesting early applications of the internet, but hardly ones that scratched the full potential of the World Wide Web. The disruptive potential of the blockchain mechanism is still unfolding and early entrepreneurs with the vision have the chance to make a real difference.

This opportunity is especially important for India. Indian businesses have not had a major hit since the IT outsourcing revolution, which has largely run its course. Further, the new waves of startup fueled tech-based businesses in India are largely knockoffs of Western or Chinese ideas, adapted to local Indian conditions. This is unlikely to lead to revolutionary global innovative companies that can disrupt businesses the way the Googles or Amazons have done. The blockchain revolution provides India another chance to take a place at the high-table of global innovation. If India can create an ecosystem that is at the forefront of research and innovation in the blockchain, the next Google can very well come from the country.