Lecture 1: Introduction to Blockchains

Principles of Blockchains, University of Illinois,
Professor: Pramod Viswanath
Scribe: Suryanarayana Sankagiri

January 26, 2021

What are blockchains?

Blockchains are the technology underlying decentralized trust systems. Let us unpack this sentence, one phrase at a time.

Decentralized system A decentralized system is one where no single entity (person/company) is responsible for the smooth operation of the system. Indeed, blockchains are peer-to-peer systems, where each peer has the same prescribed behavior; no peer is unique. Peers communicate with each other by exchanging messages. Beyond this message exchange, peers function independently of one another.

Trust Trust underpins human society. Trust enables cooperation, which is the hallmark of human activities and organizations (consider this quote from Y. Harari extracted from his book Sapiens: "Humans are the only animals to cooperate flexibly in large numbers"). The underlying mechanism of trust dictates how large groups of humans can cooperate.

Tribal Trust Historically, humans organized themselves around tribal societies, with the trust derived from a shared genetic composition and language and customs.

Institutional Trust In the last 70 years (since the end of WWII), the dominant human organization has been institutional. Examples include "The University of Illinois at Urbana-Champaign" and the "US Supreme Court" and "US Dollar." The underlying mechanism of trust is a set of laws (e.g., the Constitution of the USA) and transparent and rigorous enforcement of the law (e.g., "no one is above the law" mandate). This notion of trust has enabled human societies to cooperate on a global scale. However, the drawback is that the institutions are centralized, and the power to enforce and promulgate the laws is concentrated in the hands of a few individuals. The concentration of power leads to unintended consequences, including corruptibility, autocratic tendencies, and rent-seeking.

Decentralized Trust The siren song of blockchains is that the scaling and flexibility of institutional trust are possible without its negative aspects, i.e., the creation of a decentralized trust system. Blockchains are guaranteed to be secure even if some fraction of peers act maliciously. The only requirement is that sufficiently many peers operate according to the prescribed behavior. This is called the honest majority assumption. Thus, any user of a blockchain does not need to trust all peers in the system or even one particular peer. Instead, it just needs to trust that a majority of peers are honest. This is a key feature of blockchains that are not present in other peer-to-peer systems, or indeed, any other system.

Digital platforms A digital platform is one in which two (or more) parties interact, and some transaction takes place. There are many examples of digital platforms today. For example, Amazon/eBay is a platform for the exchange of goods. It provides a place where sellers can list goods that they are selling, and buyers can choose to buy any listed goods. Among other things, the platform ensures that the transaction takes place securely. It also handles disputes in transactions. Other examples of platforms are Uber/Lyft (for rides), AirBnB (for temporary accommodation), etc. Digital platforms have played a significant role in the global economy in the last decade.

The aforementioned digital platforms are not truly decentralized in the sense, they do not offer distributed trust. By using any platform, we implicitly trust the (single) company behind that platform to handle transactions faithfully. The platform holds a lot of power in arbitrating disputes. It can also arbitrarily decide the fees to charge for the service. (Of course, the reputation/popularity of the platform is at stake, which prevents it from behaving arbitrarily).

Blockchains hold the promise to decentralize the digital platforms we see today. From a user's perspective, the platform's functionality will be identical. However, the platform will no longer be operated by a single company but rather a multitude of small stakeholders, each running the same blockchain code. The 'trust' factor in the system becomes distributed.

A short history of blockchains

The term blockchain was introduced in late 2008 with the advent of Bitcoin. Bitcoin is a cryptocurrency: a decentralized, digital payment platform. As such, cryptocurrencies are one of the simplest applications of blockchains. Today, there is a multitude of blockchain designs for cryptocurrencies and other applications. However, they all retain many of the core design components that were introduced in Bitcoin. Thus, the term 'blockchain' has remained in all of them.

Bitcoin is one among many attempts in history to create a decentralized, digital payment platform (the term 'currency' is to be thought of as a 'token' that is used on this payment platform). Unlike all previous attempts, Bitcoin has stood the test of time. Its popularity, which can be measured by its price in dollars, has grown many-fold over the twelve years since its introduction. In the last six-seven years, Bitcoin has also been studied theoretically, giving us a better understanding of its design and its limitations. This has also given rise to ideas on how to improve its design.

A major reason behind the popularity of Bitcoin is its strong security property, coupled with its truly decentralized nature. It is now well understood that as long as 51% of the peers in Bitcoin are honest, the system is secure (the exact conditions are slightly different, but this suffices for the moment). This has been shown theoretically and has also been borne out in practice. Moreover, anyone can freely join and leave the Bitcoin system at any time; the system is 'permissionless.'

Despite its benefits, there are major drawbacks of Bitcoin, which impact its viability. Some issues can be categorized as scaling issues. For example, the system can only process about seven transactions per second. In contrast, Visa (a centralized digital payment mechanism) processes 50,000 transactions per second. If all people in the world are to switch from Visa to Bitcoin, the system must 'scale' its transaction throughput. Other issues are a lack of desirable properties. For example, if the network is disrupted, transactions that are once 'confirmed' can be reverted. (We say that Bitcoin does not offer 'finality' in confirming transactions).

Some issues of Bitcoin have been addressed in existing systems. For example, Ethereum is a system that allows much more flexibility in terms of the platforms/services that can be created in a blockchain. Many other issues are topics of active research. Currently, there is no one perfect blockchain system. Research in Bitcoin spans designing new systems, analyzing the design theoretically, building them in practice, and testing out the implementation. Thus, it involves all facets of engineering.

What this course is about

This course covers the **fundamental design principles of blockchains**. We study how different blockchain designs impact its security, scalability, and other desirable features. The lectures are divided into three modules.

Understanding Bitcoin The first six lectures cover the complete design of Bitcoin. At the end of this module, you will be able to understand the system as a whole and how it functions as a secure, decentralized payment platform. We will introduce various terms pertaining to Bitcoin and cryptocurrencies (e.g., UTXOs, hash pointers, longest chain rule) and cryptography on a "need to know basis." We will study some attacks on Bitcoin and under what conditions Bitcoin is secure under those attacks.

Scaling Bitcoin The second module aims to improve the throughput, latency, and resource usage (energy, compute, storage, and communication needs) of Bitcoin while maintaining the same security levels. The goal is to work within the overall architecture of Bitcoin itself and systematically improve various design elements.

Beyond Bitcoin The third module covers alternate blockchain protocols that offer properties that are simply not present in Bitcoin. These include accountability, resistance to 51% adversarial attacks, transaction finality, and privacy (the exact meaning of these terms will be made clear later on). We also see how these properties can be combined with Bitcoin-like blockchains via the notion of a 'finality gadget.' This gives us a blockchain with many desirable properties.

Teaching Philosophy This course emphasizes the implementation of blockchains (in software). Thus, the bulk of the evaluation will be based on two projects. The first project involves implementing a Bitcoin client. This will make use of all the concepts learned in the first module of the course. The second project will involve implementing a finality gadget of your choice on top of Bitcoin (from the third module). Rust will be the programming language that is used.

Reference material

This course covers a wide terrain of blockchain designs, from the now-classical to the very recent research literature. We recommend two basic blockchain materials to supplement the fast pace of this course:

- Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, A. Narayanan et. al., Princeton University Press.
- Introduction to Cryptocurrencies, an online course by H. Qureshi.

Two advanced courses cover blockchains from a conceptual and mathematical viewpoint. They provide complementary resources to the material covered here.

- EE 374 at Stanford by Prof. David Tse.
- ECE 595 at the University of Washington by Prof. Sreeram Kannan

The following two sources are good references for consensus algorithms that are the underpinnings of blockchains.

- CS 598LR at UIUC by Prof. Ling Ren.
- Foundations of Distributed Consensus and Blockchains by Prof. Elaine Shi