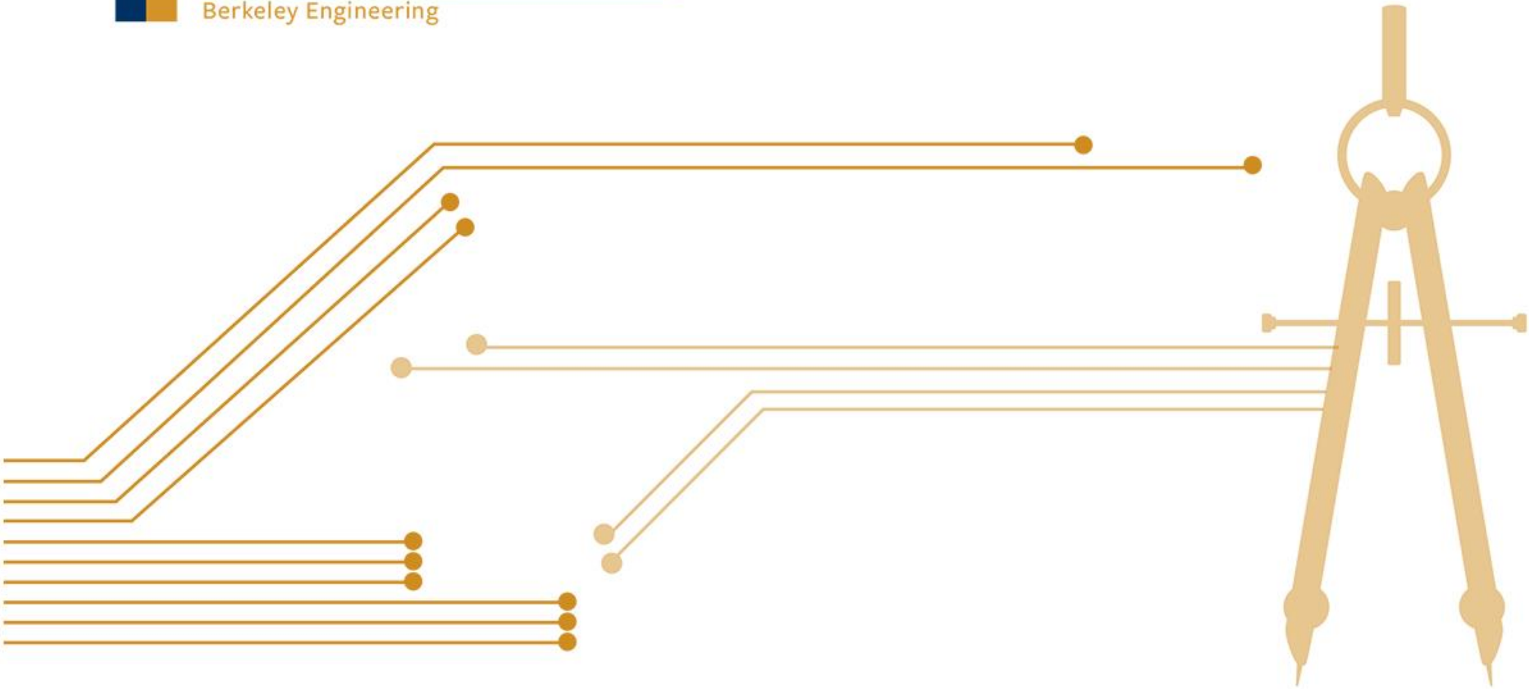
Pantas and Ting
Sutardja Center
for Entrepreneurship & Technology
Berkeley Engineering



Future of Blockchain - A Berkeley Perspective

Ikhlaq Sidhu, Alexander Fred-Ojala
Sutardja Center for Entrepreneurship & Technology, UC Berkeley

Feb 11, 2018

Berkeley
UNIVERSITY OF CALIFORNIA

Future of Blockchain - A Berkeley Perspective

Ikhlaq Sidhu, *Alexander Fred-Ojala*
Sutardja Center for Entrepreneurship & Technology, UC Berkeley
Feb 11, 2018

Current Situation: Blockchain is an Emerging Technology With a Significant Promise

In 2009, a previously unknown cryptographer by the name of Satoshi Nakamoto introduced a mysterious new digital currency to the world. Ignored by the traditional finance industry, Bitcoin gained popularity quietly on the Internet and now is considered the first mainstream cryptocurrency that has been heralded as the biggest innovation in finance since the invention of the double-sided ledger. The comparison is no mistake, cryptocurrencies can be considered the re-invention of the ledger, a public ledger, once the exclusive playground of banks and governments. The power behind cryptocurrencies is Blockchain technology, an equally mysterious concept that can only exist in a world of cheap high speed computing power and ubiquitous Internet.

Since Blockchain's introduction in 2009 as the base technology enabling the Bitcoin network, Blockchain has offered significant promise to revolutionize the IT and financial landscape, disrupting the traditional roles of governments, banks and other institutions. Marc Andreessen, the co-creator of the first commercial Web browser, Netscape, and a big investor in the technology, claims it is one the greatest breakthroughs in Computer Science in the 21st century. At the core of Blockchain is the ability to create a global database (extended from a ledger/list) which is immutable (not changeable by anyone after the fact), transparent, trusted, even when the parties who write to it are not trusted by each other.

The result and promise of Blockchain technology and its related view of the world includes:

- Global electronic transaction commerce including secure financial payment/transfers with reasonably short settlement times
- Increased financial transparency leading to lower corruption, less illicit activity, and/or fewer black market options
- The possibility of a true, user controlled, and tamper-resistant digital identity and digital records
- Distributed networks of smart contracts that automatically execute transactions-based policy and on real life events.

- A decentralized internet where information and data are owned by the user, rather than the service provider
- Automatic grid infrastructure with minimal maintenance, e.g. electric grid where producers and consumers could connect without going through a central instance.

In its current state, many leading companies and governments explore demonstrations of the Blockchain integrated into finance, supply chain, identity management, credential validation, property exchange recording, and other verticals. In most of these cases, the proof of concept demonstrations are indicative of the possibility and promise, but have yet to be deployed in meaningful or scalable manner.

One of the main reasons why true adoptability of Blockchain technology has been slow is because of the uncertainty in policy. Firms and organizations are waiting for political decision makers to clearly state how rules and laws related to tax and financial exchange will affect the technology. So far, we have witnessed the earliest forms of actual Blockchain implementations in applications that involve compliance. In these cases, the value of immutability, decentralization, and transparency are the most significant. We expect security applications to be the next area where significant adoption will take place. There is also a general trend in all industries and governments, where slow but steady acceptance of Blockchain technology is taking place.

We expect the gradual development of a globally transparent ledger which will become the backbone of many new applications. Blockchain technology today is in its infancy, but for institutions, states, and companies alike to ignore this technological revolution would be equivalent to ignoring Internet technology when it emerged 25 years ago. We expect many researchers and firms to compete and work on algorithms, technological improvements and infrastructure that can offer the Blockchain promise in a scalable, yet secure manner. We believe that it is crucial for institutions, organizations, and governments to be part of this groundbreaking development and research.

What are the Next Technological Breakthroughs in Blockchain

For Blockchain technology to transform industries and everyday lives of people there is a lot of technological development still to be made. We would like to compare this to the development of the original Internet that allowed a certain number of applications (i.e. web browsing, email, information sharing, etc.). This first iteration of the Internet (Web 1.0) was made possible by open protocols developed by researchers. The true Internet economy that we are witnessing today emerged from the second layer of the Internet, namely interactive and social applications (Web 2.0). This second wave of Internet companies included Facebook, LinkedIn, Instagram, etc. that thrive on human exchange and interaction.

In a similar way, we expect a wave of Blockchain solutions that will solve a new set of social issues to disrupt the current world order. Thus, it may not be enough for people to simply have direct access to the primitives of a global Blockchain ledger. We believe that as the current set of issues with Blockchain protocols, scalability technologies, and standards are resolved, Blockchain will deliver impact on societies and people all over the world, creating new winners and losers. This is the horizon we would like to explore and that is what we consider as the next stage of Blockchain.

There exists a number of challenges and new values that could be created via Blockchain if these problems were pursued:

1. Consensus mechanisms need to be developed and game theoretical models for decision making need to be thoroughly studied, especially to keep the systems decentralized and prevent / lower the incentive of a majority take over.

2. Given the number of transactions that will be possible on Blockchain, a person will require their own Personal policy / User Interface to manage a personal control layer for their transaction flow.

3. There will be so many transactions, that sophisticated AI technologies will be required to detect anomalies the get recorded.

4. A policy language to control your acceptances of transactions will likely be needed. Today, this layer does not exist.

5. Keeping the infrastructure alive and optimally distribute workload will be a major issue:

    a. First the scalability issues will be significant as the number of transactions per user grow on an exponential scale with time. And then the number of nodes that keep copies grow on an exponential scale. The product of the two defines the complexity of the emerging system.

    b. Security standards and hacking prevention measures becomes a significantly larger issue particularly since humans will trust the systems instead of centralized authorities.

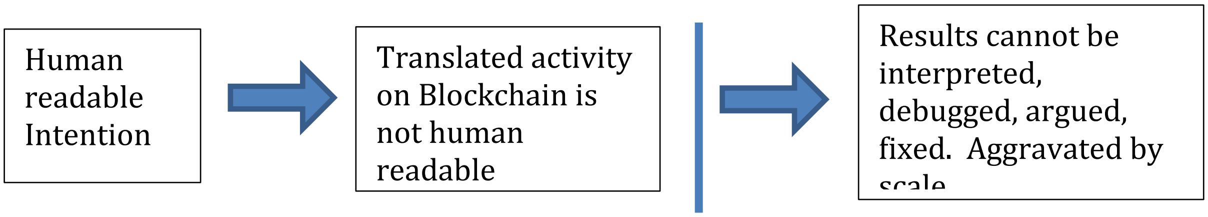
c. We must consider how the emerging Blockchain infrastructure will map to and/or interface with emerging new failure points.

6. Perhaps the largest barrier for the Blockchain today and the most evident point of failure for smart contracts will be how this technology interacts with the real-world. These are called edge cases or edge devices, points in the network that have to register something that has happened in the real-world and then utilize that information in the smart contract system. The problem is evident as any smart contract is only as reliable as the information that it reads to execute its transactions. E.g. If a cargo company tracks the source of all delivered goods, how can we make certain that the entity registering the source does not provide false information?

7. In parallel, we expect a Smart city and Internet of Things management systems will also have to be developed that will integrate and monitor all the nodes and participants of this global network.

8. While some of these issues can be solved with technology, many can only be solved by policy and conventions that live outside of the Blockchain technology itself. A framework for this policy is necessary and yet does not exist.

9. Finally, there is a significant issue that when the systems based on Blockchain do breakdown there is no way to debug them due to their tamper-proof immutable nature. How do we trace back the results that are largely unreadable to humans to obtain layers of information and intent? This capability and framework must also be developed.



Human readable Intention

Translated activity on Blockchain is not human readable

Results cannot be interpreted, debugged, argued, fixed. Aggravated by scale

Illustration of a Long Term Concern:
Blockchain intention is not easily human readable

A Note on Blockchain’s Future:

If we compare the state of the Internet in 2000 to the state of the Internet in 2010, we will see that the firms that led the first round of technological breakthroughs largely did not survive and further the key players by 2010 were not all even developed in the first round. For example, Netscape who developed the first Browser and Sun who created Java both lost their lead. Some firms like Amazon and Netflix increased in power. And many firms from Facebook and Google became leaders only after the second iteration of Internet technology had been developed and adopted. It stands to the same reason that the leading players in Blockchain today, who are building infrastructure and developing fundamental protocols, are not necessarily the players that will dominate the next Blockchain landscape—there is plenty of room for new companies to emerge.