

BIG DATA /BLOCK CHAIN TECHNOLOGY –LEGAL ISSUES

Prof Vivekanandan

Doug Laney – on Big Data

- **Volume.** Organizations collect data from a variety of sources, including business transactions, social media and information from sensor or machine-to-machine data. In the past, storing it would've been a problem – but new technologies (such as Hadoop) have eased the burden.

Doug Laney

- **Velocity.** Data streams in at an unprecedented speed and must be dealt with in a timely manner. RFID tags, sensors and smart metering are driving the need to deal with torrents of data in near-real time.

Doug Laney

- **Variety.** Data comes in all types of formats – from structured, numeric data in traditional databases to unstructured text documents, email, video, audio, stock ticker data and financial transactions.

Doug Laney

- **Veracity**
- It is the extended definition for big data, which refers to the data quality and the data value. The data quality of captured data can vary greatly, affecting the accurate analysis

What to do with data

- The importance of big data doesn't revolve around how much data you have, but what you do with it.
- You can take data from any source and analyze it to find answers that enable
 - 1) cost reductions,
 - 2) time reductions,
 - 3) new product development and optimized offerings, and
 - 4) smart decision making.

Big Data for whom ?

- [Banking](#)
- With large amounts of information streaming in from countless sources, banks are faced with finding new and innovative ways to manage big data. While it's important to understand customers and boost their satisfaction, it's equally important to minimize risk and fraud while maintaining regulatory compliance. Big data brings big insights, but it also requires financial institutions to stay one step ahead of the game with advanced analytics.

Big Data for whom ?

- [Education](#)
- Educators armed with data-driven insight can make a significant impact on school systems, students and curriculums. By analyzing big data, they can identify at-risk students, make sure students are making adequate progress, and can implement a better system for evaluation and support of teachers and principals.

Big Data for whom ?

- Government
- When government agencies are able to harness and apply analytics to their big data, they gain significant ground when it comes to managing utilities, running agencies, dealing with traffic congestion or preventing crime. But while there are many advantages to big data, governments must also address issues of transparency and privacy.

Big Data for whom ?

- Health Care
- Patient records. Treatment plans. Prescription information. When it comes to health care, everything needs to be done quickly, accurately – and, in some cases, with enough transparency to satisfy stringent industry regulations. When big data is managed effectively, health care providers can uncover hidden insights that improve patient care.

Big Data for whom ?

- [Manufacturing](#)
- Armed with insight that big data can provide, manufacturers can boost quality and output while minimizing waste – processes that are key in today's highly competitive market. More and more manufacturers are working in an analytics-based culture, which means they can solve problems faster and make more agile business decisions.

Big Data for whom ?

- [Retail](#)
- Customer relationship building is critical to the retail industry – and the best way to manage that is to manage big data. Retailers need to know the best way to market to customers, the most effective way to handle transactions, and the most strategic way to bring back lapsed business. Big data remains at the heart of all those things

Legal issues of Big Data

- While law is semantic, Big Data is syntactic.
- Law is abstract, values-based, and built on compromise.
- Big Data is empirical, algorithmic, and deterministic.
- Also, Big Data is inherently acontextual.
- Big Data cannot interpret itself, nor can it discern the indeterminate boundaries of legal principles.
- Moreover, Big Data cannot discern or create novelty, unlike humans, who can update their “frames” or paradigms as their environment changes.
- Big Data cannot innovate beyond the paradigms imposed by its creators.
- Even the most sophisticated machine learning techniques cannot tell us what factors might become relevant in response to new challenges

Critique on Big Data for legal systems

- First, Big Data's asserted objectivity is a myth. Data require theory in order to be interpreted and applied, and any single interpretation of data is rarely conclusive.
- Second, the behavioral and predictive models that employ Big Data are incapable of adapting to the creative evolution of the legal system. These models cannot measure or predict all of the relevant variables that may influence the legal system, such as changes in values or novel uses of the law.
- Finally, as a result of these shortcomings, rather than Big Data reflecting the legal system, the legal system recursively will come to reflect Big Data

Some example of Big data vs Legal analysis

- The story of the steel manufacturer
- The story of the horse thief
- The story of Real Mother

What is blockchain?

- The first four decades of the Internet brought us the e-mail, the World Wide Web, dot-coms, social media, big data, cloud computing and the early days of the Internet of Things.
- The Blockchain is the Internet of Value rather than the Internet of Information. It's a platform for everyone to know what is true. It provides an open decentralized database of any transaction involving value.

- The Blockchain has no single central database, so no single person can defraud or hack the system. Someone speaks about the blockchain as the global trust machine. It is essentially “*a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties*”.

Advantage Block Chain

- The verification through Blockchain technology creates the trustworthiness of the information we receive. Each transaction in the public ledger is verified by consensus of most of the participants in the system.
- It is encrypted and contains a certain and verifiable record of every single transaction ever made.
- Bitcoin, the decentralized peer to peer digital currency, is the most popular example that uses blockchain technology. Indeed, the Bitcoin was created using a process known as blockchain.

The Benefits -Smart contracts.

- One key emerging use case of blockchain technology involves “*smart contracts*”.
- A smart contract is an agreement between two parties that is stored in the Blockchain. Indeed, a smart contract is a computer program that makes possible to exchange an asset without third parties being aware of the transfer; this automates the execution of the terms of the contracts and opens up the possibility of creating a new form of virtual agreements.
- When a pre-configured condition in a smart contract among participating entities is met then the parties involved in a contractual agreement can be automatically made payments in a transparent manner and the need of an intermediary could become unnecessary or limited.
- Smart Property is another related concept “*which is regarding controlling the ownership of a property or asset via blockchain using Smart Contracts*[. *The property can be physical such as car, house, smartphone etc. or it can be non-physical such as shares of a company*”.

. Decentralized proof of existence.

- Validating the existence or the possession of signed documents is very important in any legal solution. The traditional document validation models rely on central authorities for storing and validating the documents.
- The blockchain technology provides an alternative model to proof of existence and possession of legal documents.
- By leveraging the blockchain, a user can simply store the signature and timestamp associated with a legal document in the blockchain and validate it anytime using native blockchain mechanisms.
- The existence of the document is validated using blockchain that does not depend on a single centralized entity.
- *“Proof of Existence is a simple service that allows one to anonymously and securely store online proof of the existence of any document. This service simply stores the cryptographic digest of the file, linked to the time in which a user submits his/her document. It is to be noted here that cryptographic digest or fingerprint, not the actual document, is stored in the blockchain, so the user need not be worried about the privacy aspect”*

Blockchain and IP law.

- One of the most applications of blockchain technology is as a registry of IP rights, to catalog and store original works. As Birgit Clark said the potential use cases include: evidence of authorship and provenance authentication, registering and clearing IP rights, controlling and tracking the distribution of (un)registered IP, providing evidence of genuine and/or first use in trade and/or commerce, digital rights management, establishing and enforcing IP agreements, licenses or exclusive distribution networks through smart contracts and transmitting payments in real-time to IP owners.
- Blockchain technology can also play an important role within the context of unregistered IP rights such as copyright and unregistered design rights, since it can provide evidence of their conception, use, qualification requirements and status. Indeed, it also helps to give clarity to copyright authors, owners and users. Uploading an original design or work and details of its designer or author to a blockchain will create a time-stamped record and solid evidence to prove these matters.

Blockchain Security Issues

- A blockchain draws its security benefits from the decentralized nature of its nodes (i.e. the computers that verify transactions on the blockchain). Because the ledger (record of transactions) is public, no one can secretly make changes. And when a change is made, the other nodes on the system all need to agree to the change before it enters the record.
- A **51 percent attack** occurs when a hacker (or group of hackers) produces more than 50 percent of a blockchain's computing power. In doing so, they become the network majority and can assume control of the entire blockchain, allowing the hacker(s) to double-spend coins, prevent other miners from creating blocks, and preventing transactions altogether.
- The risk level is greater for smaller blockchains with fewer miners since the amount of computing power needed to control 51 percent is lower.

Blockchain Privacy Issues

- If a blockchain is public, every transaction ever recorded on the blockchain is available for anyone to look at.
- Of course, that doesn't necessarily mean that someone will be able to identify you. However, the very fact that so much information is available in the public domain runs against longstanding norms, especially in the financial, legal, and healthcare sectors, all of which typically have robust privacy requirements.
- For example, consider this: should a patient's medical records be available publicly, even in a pseudonymous setting like a blockchain? As Arran Stewart, co-founder of Job.com, says, "Someone somewhere will list information publicly that is sensitive, and someone else will spend a lot of time figuring out how to get it."
- **Note:** Permissioned and private blockchains do not necessarily suffer from these same privacy issues. It's one of the many [differences between public and private blockchains](#).

Blockchain Legal Issues

- Blockchain technology is facing lots of legal questions, many of which don't yet have a resolution. Some of the critical issues facing the community include:
- **Jurisdiction:** In a decentralized environment where nodes exist around the planet, how do we establish the correct set of rules and laws to apply? Different countries have very different approaches to titles, ownership, contracts, and liabilities.
- **Decentralized Autonomous Organizations (DAOs):** Consider a typical legal system where both individuals and organizations participate. In many cases, they even have similar rights. How does that apply to DAOs? They run on smart contracts and require almost zero input from users—they are just lines of code—and yet they can perform tasks like traditional companies. In the case of conflict resolution, who is responsible? Who, or what, can a claim be made against?
- **Contract enforceability:** Much has been made of smart contracts' ability to cut out the middleman, thus slashing costs and increasing security when undertaking complex legal processes. But given that smart contracts are also pure computer code, it's debatable about whether they meet the definition of a contract in the traditional sense. In the event of a contract dispute, how enforceable would a smart contract be in a court of law? Quite simply, we don't know. At the very least, you need to make sure all smart contracts you enter at this stage have a very clear dispute resolution process attached to them.
- **Leaving a blockchain:** Let's suppose you've been [using a blockchain in the healthcare sector](#). What happens if you decide to stop using the service that supplies the blockchain and you don't hold a copy of the data on the ledger? There needs to be provisions and processes in place that ensure the vendor hands over all your information and a complete record of all the transactions on the blockchain that are linked to your name.

Blockchain Regulatory Issues

- Cryptocurrencies are now starting to face regulatory pressures. As their market capitalization continues to grow, governments are taking an increased level of interest.
- Regulatory uncertainty comes in many forms and will have many consequences.
- For example, some governments have, or have threatened to, make cryptocurrencies illegal in their territories.
- Bitcoin is only entirely unrestricted in 110 countries and is outright banned in Algeria, Morocco, Ecuador, Iran, Pakistan, and more. In Bangladesh, police have reportedly arrested Bitcoin owners.

Blockchain Ethical Issues

- Blockchain technology raises some ethical issues, with the two most prominent problems being 1) its effect on the environment and 2) its apparent enabling of criminal activity.
- **Firstly, the environment.** raw computing power is what drives the technology. And because blockchain networks rely on encryption and the solving of complex mathematical puzzles, the amount of computing power needed to run them is enormous.
- The stats are mindboggling:
- [According to Morgan Stanley](#), the Bitcoin blockchain alone will use as much power in 2018 as the entire nation of Argentina.
- Bitcoin's current estimated annual electricity consumption is 61.4 TWh. That's 1.5 percent of the United States' annual consumption.
- UK-based energy comparison service [PowerCompare](#) says the total annual electricity usage of the Bitcoin blockchain exceeds that of 159 nations.
- Bitcoin is now responsible for 0.6 percent of the world's entire electricity usage.
- In a world that's increasingly conscious of skyrocketing energy usage, developers need to find a way to verify transactions much more efficiently.

Cyber Crime

- **cybercrime.** Looking back at the early days of Bitcoin, one could argue that the cryptocurrency's price increases were driven almost exclusively by criminal activity.
- Using dark web websites, cybercriminals could sell drugs, weapons, and other banned items safely and anonymously with Bitcoin—not to mention the obvious benefits that untraceable financial transactions offer to money launderers.
- Fast-forward to today and the problem still exists.
- Yes, mainstream adoption has increased, but cryptocurrencies are still the payment method of choice for anyone acting illegally. For example, if you've ever been unlucky enough to suffer from a ransomware attack, you'll almost certainly have seen Bitcoin as the payment method. Even less dangerous criminals, such as those selling NZB indexing services, now want to be paid in crypto.

Sources

- Wikipedia
- https://www.sas.com/en_in/insights/big-data/what-is-big-data.html
- <https://www.lawschool.cornell.edu/research/JLPP/upload/Devins-et-al-final.pdf>
- <https://www.cyberlaws.it/2018/blockchain-technology-challenges-legal-issues/>
- <https://blocksdecoded.com/blockchain-issues-security-privacy-legal-regulatory-ethical/>