B★SCHOOL *for*
PUBLIC POLICY

Better-informed policymaking through a deeper understanding of economics.

Summary: Blockchain, The Rise of Trustless Trust?

Seminar by Professor Kevin Werbach

Blockchain is a term that is used for a family of distributed ledger technologies (DLT). Although there is one virtual ledger, every participant in the network has a copy, allowing for local control of data and transparency while ensuring all ledgers remain in sync.

SIGNIFICANCE OF BLOCKCHAIN

There has been speculation that blockchain will disrupt the status quo in a vast number of industries, from finance to digital identity and medical R&D to the tracking and collection of taxes. Regardless of the extent to which this hypothetical disruption may or may not play out, blockchain certainly poses new questions for policymakers and regulators. Much in the same way that the Internet opened up a host of questions about how to regulate transactions on the web, the new transactional structure of blockchain introduces uncharted territory for legal scholars and regulators.

Blockchain is important and potentially revolutionary because blockchain provides a novel architecture for trust. In a time when trust in institutions and authority figures is waning, a new system of trust is desperately needed.

> "Trust in all four institutions—business, government, NGOs, and media—to do what is right declined broadly in 2017."

Traditionally, trust has centered around either a central authority figure that upholds the rule of law, or, trust has been established through peer to peer relationships where the system of trust is based on shared values. Blockchain creates a new architecture for trust, one that is distributed. The trust is not placed on any one actor in the system, but, rather, is placed in the system as a whole.

The technology of blockchain makes it possible to reliably trust that everyone in the system is sharing the same information; what appears in one ledger will match every other instance. By relocating the agency of trust to the cryptographically verifiable system, the need to trust any single person is removed. It is thus a system of "trustless trust."

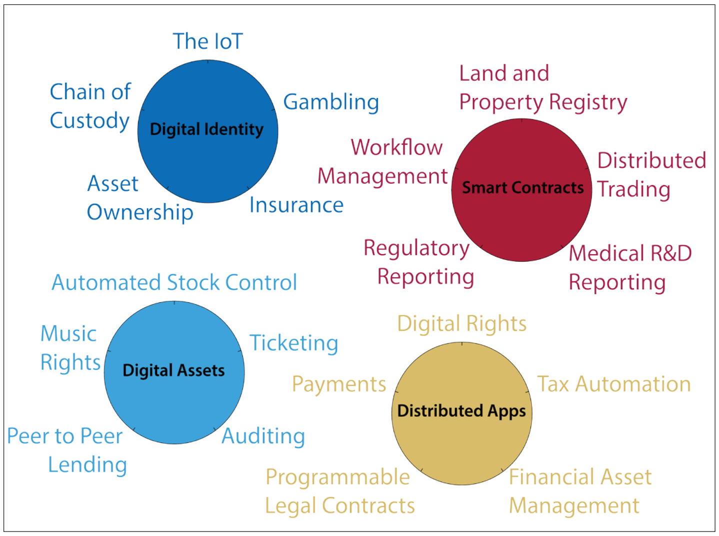

Figure 1: Possible Areas for Disruption by Blockchain

PENN WHARTON
UNIVERSITY *of* PENNSYLVANIA

PUBLIC POLICY
INITIATIVE

More on classes:
http://bit.ly/BSchoolPublicPolicy

WHY DO WE NEED A SYSTEM OF TRUSTLESS TRUST?

One benefit of using blockchain is the elimination of reliance on a central authority figure. This was the primary impetus for establishing Bitcoin. The founding developers of Bitcoin wanted a means to distribute currency anonymously, independent of any government structure. Even if there isn't an ideological reason to oppose a centralized governing structure, there are some instances where this centralized control just won't suffice--for example, when the application requires an environment that simply cannot work on one platform, typically for competitive reasons.

A less obvious reason why a system of trustless trust might be needed is when the current system is rife with inefficiencies that could be avoided by having universal consensus. Any time there are multiple parties keeping their own records of a transaction, such as in the case of a syndicated loan where you have 10 major banks contributing to a major multi-billion-dollar exchange, there is a tremendous expense in overhead, duplication, delay, as well as risk of error. The distributed ledger technology of blockchain could, in this instance, offer a cheaper, more efficient alternative. Once a blockchain is established, the digital infrastructure creates possibilities for automation across organizations and industries. Because everything is on a common platform, everyone involved is able to enjoy the same level of visibility and transparency.

APPLICATIONS OF BLOCKCHAIN: PERMISSION NETWORKS AND SMART CONTRACTS

There are many applications for blockchain technology beyond digital currency. In the last few years, a lot of innovation has occurred around the use of blockchain to create permission networks. These private clubs allow big companies, such as IBM and Walmart, to create a "members only" network where participants join in a syndicated fashion. See the case example below.

Case Example: Walmart Tests Blockchain to Track Pork from China

Walmart is in the business of selling a large quantity of pork sourced from hundreds of different farms around China. They need a way to track each transaction, starting at the pork farms, following the pigs to the meat packing plant, all the way down the line to the package of meat sold at the check-out register in any one of Walmart's stores. Walmart is currently testing a permissioned network built using the Hyperledger distributed ledger system. Each entity involved in the process of supplying and distributing the pork would be required to log their step into the ledger, allowing Walmart to track each transaction and create a transparent record for each package of pork it sells. In addition to being a benefit for Walmart's business, this blockchain tracking mechanism has the potential to help regulators and other officials trace problems back to their source—for instance, an incidence of tainted meat.

SMART CONTRACTS

Another application of Blockchain that goes beyond digital currency is smart contracts. The distributed ledger technology of a blockchain is dynamic and the computers in the network are constantly processing the data. In order for there to be consensus in the blockchain, it is requisite that every machine on the network run the same code. The code can be anything, and if the system is robust enough with sufficiently complex syntax, any set of instructions could theoretically be written into a computer program. A smart contract is one which renders an instruction automatically, deterministically, and at the appropriate time. In other words, smart contracts are self-executing, automated systems. This can be incredibly efficient and open new opportunities. However, there are potential liabilities with smart contracts. Executing instructions without human intervention or control can obviously lead to potential problems and risks; these need to be examined more fully by legal scholars.

LEGAL AND REGULATORY IMPLICATIONS OF BLOCKCHAIN

Similar to what happened in government 20 years ago when decisions were being made about regulating the Internet, the key to understanding the legal and regulatory aspects of blockchain will be to separate out the specific players involved and the types of transactions being made. Once the different functions of the various actors in a blockchain are ascertained, the regulatory questions become: what are the rules that exist and what is the right place to apply these rules in the system of actors that are fulfilling that existing role?

More significant to the discussion of blockchain, however, is how blockchains can serve as regulatory structures in and of themselves. Blockchain systems constrain behavior, allowing certain transactions to be trackable and others not. Blockchain creates visibility, opening up opportunities for taxation and many other things that would typically be governed by a legal institution. In some ways blockchains act similarly to public legal institutions but don't necessarily start with the same traditions, governance mechanisms, and checks and balances. So the question becomes how to build governance mechanisms into the blockchain software and code.

There are three basic ways blockchain will possibly interact with the law. First, blockchain could supplement an already functioning legal environment to reduce transaction and coordination costs. Secondly, blockchain could complement existing legal structures to address a breakdown in the implementation of legal authority, and third, blockchain could entirely substitute an existing authoritative structure to create trusted interactions in an environment where the rule of law is not adequately functioning.

In the future, work needs to be done on blockchain governance, devising standards and templates for agreements to ensure that blockchain contracts are written in such a way that they are legally solvent and the contract serves the best intentions of the parties involved.