Legal Systems and Blockchain Interactions

Hegadekatti, Kartik

3 January 2017

LEGAL SYSTEMS AND BLOCKCHAIN INTERACTIONS

Dr.Kartik H

Author's email-dr.kartik.h@gmail.com

ABSTRACT

A large amount of money is spent globally in the litigation process. A significant chunk of litigations can actually be prevented from even arising if the policies, contracts and laws can be fully objectivised. Presently, the interpretation of law, contracts, policies etc. lead to a lot of confusion and ambiguities. This complicates the justice process. This paper deals with simplifying the legal procedures by using Blockchain Technology. Firstly I introduce the concept of Blockchains and Cryptocurrencies. Then we discuss the present legal services. The ways in which Blockchain technology can be applied to legal processes is identified. Civil and Common law systems are the most widespread in the world. The probable impact of Blockchain on law systems is evaluated. The paper concludes by summarizing the consequences and suitability of using Blockchain Technology in Law systems and Legal services.

INTRODUCTION

A cryptocurrency is a medium of exchange using cryptographic techniques to safeguard transactions and also manage the formation of additional units of the currency. They work on the Blockchain method.

A BlockChain is a widely disseminated archive of data that maintains a continually-expanding register of records fully and reliably protected from any alteration or modification. Each block has a timestamp and link to the preceding block.

A Crypto wallet is an encrypted electronic device that allows an individual to make electronic cryptocurrency transactions. Each wallet will have a public key visible to anyone. But it can be operated by only a person who has a private key. Transactions on the cryptocoin network are usually anonymous.

When people send cryptocoins to each other, someone has to keep account of who spent how much at what time. In case of fiat money (or paper money) it is done by banks (known as Trusted Third Parties, for which they charge a commission).But in case of Cryptocoins, it is registered on a ledger called BlockChain (with nil or minimal fees).

The cryptocoin network makes this possible by detailing all the transactions made during a certain timeframe into a list. This list is known as a block. A certain set of people called 'miners' verify these transactions mathematically and register them on the BlockChain. Those bona-fide miners who have successfully verified the transactions are paid freshly created Cryptocoins.

This is how miners are rewarded, and new cryptocoins are generated. This is also the reason why no transaction costs are levied, as the network (in the form of miners) verifies the transactions.

Bitcoin is a peer-to-peer based cryptocoin which is not backed by any commodity and (unlike fiat money) carries no sovereign guarantee whatsoever.

Regulated and Sovereign Backed Cryptocurrencies (RSBC), on the other hand are government backed cryptocurrency akin to paper currency, but in digital form. In this system, the cryptocoins (known as NationCoins) are backed by Sovereign Guarantee. This system is based on the K-Y Protocol [1].

The K-Y Protocol is a set of rules and instructions to implement the Regulated and Sovereign Backed Cryptocurrency (RSBC) system.

They are run on a highly secure Controlled BlockChain (CBC) [2] in which Sovereign backed Cryptocurrencies will be transacted without any hassles. NationCoins are completely managed by the Sovereign Authority i.e the Government.

A Law Firm is a business entity formed by one or more lawyers to engage in the practice of law. Civil and Common law systems are the most widespread in the world.

The primary service rendered by a Law Firm is to advise clients (individuals or corporations) about their legal rights and responsibilities, and to represent clients in civil or criminal cases, business transactions, and other matters in which legal advice and other assistance are sought.

The combined revenue of the world's top 200 law firms exceeded $100bn in 2015. The list includes 144 US, 31 UK, 9 Asian, 7 Canadian and 9 European firms, which collectively brought in $127bn in 2014[3].

The Blockchain concept was first envisaged for only one purpose: shifting cryptocurrency (like Bitcoins) from one person to another. But once it worked and was used widely, people inserted “metadata” in transactions (metadata is a set of data that describes and gives information about other data, i.e. it is data about data).

Such “metadata” serves many functions like digital asset recording, document verification, etc. RSBCs will have this metadata function in-built in their design.

One significant task done by lawyers is to offer proof for the existence of a document, for example- power of attorney, a deed to a building, a will, etc. This process is known as showing Proof-of-Existence.

As it involves signing a document at a specific date and time, the Blockchain can complete similar time stamped operations and preserve them for eternity. Thus Blockchains play an important role in demonstrating Proof-of-Existence.

A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, digests, hash sums, or simply hashes.

Today, it is possible for crypto-law enterprises to transform the contents of a document into hashes and deposit it on the Blockchain. As the hash cannot be altered, the validity of the documents in a block on the Blockchain can be confirmed universally in any court of law at any future date.

This preserves the integrity and credibility of court data, submitted evidence and also makes tampering with such sacrosanct data impossible.

Cryptocurrencies have a fundamental programming language that is built into each transaction, which is known as a 'script' (Antonopoulos, 2014).

The transaction script stipulates instructions to be obeyed in order for the currency (or token) to change proprietorship, i.e. ownership of the coin. Most of the rules are fairly simple, e.g., the next holder must demonstrate the ownership of her private key to the crypto address where the funds are kept.

Other guidelines can also be programmed like multi-signature situations and time lock conditions. These features and the related commercial models make up the heart of 'smart contracts'.

Many legal services can be offered using this type of technology, like-

1) Translating contract (with complicated outcomes, for example, the breach of penalty) into code.

2) Concurring which code to use where.

Some other uses of smart contracts are for auctions. A contract can be automated to sell an article at a particular price.

The buyers make their bid and transmit their payments; but the contract only takes the maximum offer and sends back the rest of the money to the wallets it came from, thus offering instantaneous trading.

SMART CONTRACTS AND SMART PROPERTIES

Escrow services are third party services used to enable transactions and settle contract disputes between two transacting participants. As a Blockchain token is inscribed with the 'script', such services can be programmed into the tokens. This has led to the conception of smart contracts and smart properties.

Smart contracts mean that the contract execution takes place on a Blockchain.

A smart contract is basically, a software package that is encoded with definite conditions and outcomes (Buterin, 2014).

In the existing Blockchain technology, smart contracts bring together four important things.

They are-

(a) Writing a business or legal process as a computer program- Here, the entire sequence of events of a transaction or business dealing is expressed in computer language so that the computer can understand it.

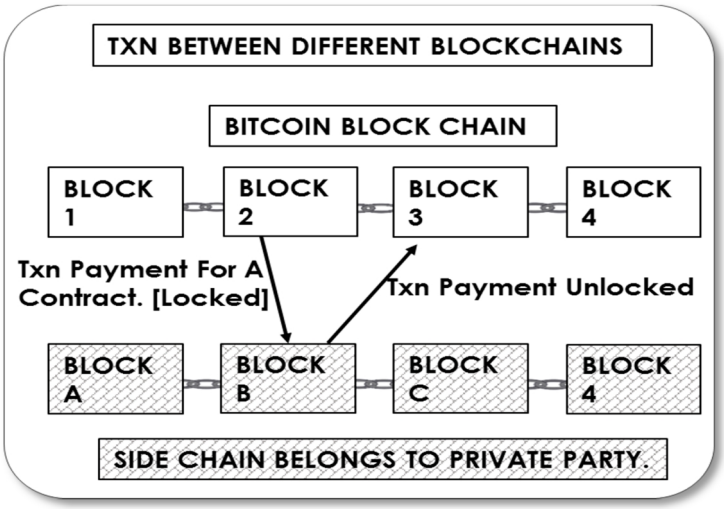
(b) Expressing the events which trigger the payment or activity, as messages to the program- This means that a particular event, like the completion of a work activates the payment procedure, and the party is automatically paid.

(c) Using digital signatures to verify who sent the messages, and

(d) Placing all the above on a Blockchain.

HOW SMART CONTRACTS WORK

Contracts will be run on the Blockchain. But not on the main Blockchain. It will run as a 'sidechain', where if anything happens to the sidechain, it will not affect the main Blockchain.



TXN-Transactions

Smart Contracts effectively automate the contracting process with the rules of the contract governing the transactions or activities.

The policy is decided upon by the contracting parties in advance. The smart contract considers both their (or multiple parties') interests. The programmed guidelines act as a set of rules and can take the form of a law, business logic, or even a mission statement.

As the rules are inscribed in a programming language, the contracts can network with anything that admits cryptographically endorsed

orders, like a 'token' that has been programmed to receive these instructions and perform specific actions on receiving such orders. (Buterin, 2014).

In the future, if a consumer desires to buy a car, they can use a smart contract. It will record the change in the car's ownership as soon as the transaction is completed. Once the transaction is confirmed and broadcasted on the Blockchain, the criteria of the contract will be met.

Since the transaction will be time stamped on the Blockchain, the procedure is irrevocable and the entire network can authenticate its legality. The status of ownership can now be verified, by any gadget linked to the Internet and the Blockchain, in this instance, the car.

The car obtains this information and localizes its new owner using the mobile phone number associated with the mobile wallet. If it is a driverless car, it will drive itself to the new owner. This illustration demonstrates the concept of Smart Property. The scope of the idea can be enlarged to include a host of various transactions like real estate acquisition, property selling, etc.

The Internet of things (IoT) is the network of physical devices, vehicles, buildings and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

Today, the line between the physical and virtual world is blurring at a rapid pace. The centralized approach to build an IoT model, in a centralized setup is quite expensive. It fails to deal with the issues of scale and complexity. A centralised system is vulnerable to hijack and hacking. And thus it lacks privacy.

A resultant effect of the Internet of Things is that it will also give birth to an economy where everything is connected to everything else.

Every object capable of connecting to the Internet becomes a party to a transaction.

This will lead to value addition for consumers in an inclusive economy. In this way, a concerted digital economy-a decentralized model, where value addition is in the hands of the consumer, is a better model to follow. This decentralized model eliminates the problems of having a single point of failure intrinsic to present day client-server kind of business models.

In a decentralized arrangement, the addition of more nodes reduces the risk of the system failing. If one node fails; the whole network is not weakened. Blockchain is an ideal, reliable decentralised system The IoT can be thus be enabled by Blockchain technology. It can be optimized and made even more secure and reliable by using RSBC networks.

We have seen Blockchain systems in terms of digital currency. But this is just a tiny part of a larger and more fascinating application. The scripting language of Blockchains can be used to communicate and execute immensely complex transactions. One such complex entity is programmable money- money that can be instructed to do a certain task.

In the future, money can be programmed to return back to the owner's account if a contract is breached, fraud (by service provider), poor quality of service etc. Blockchain allows for such programmable Digital currencies.

The impact of Blockchain Technology on legal services and law enforcement are immense and far-reaching:

1) Law firms will see a large amount of work like drafting, petition appeal etc. to be automated as Blockchain technology makes the Internet-of-Things a reality.

2) Court procedures will be greatly simplified due to quick verification of legality (and credibility) of certificates, evidence, audits, reports, documents etc. through the Blockchain.

3) Criminal records, put on the Blockchain will make identification and case-solving easier and less cumbersome.

3) Contract execution will be objectivised and become simpler for execution as Smart Contracts work on the Blockchain. This will lead to a fall in petty litigation, thus saving the precious time of courts and authorities.

4) Law firms will have to rebrand themselves into specialist niches and focus on specific sectors to maximize their business potential.

5) It will be possible to bring into the ambit of law even informal word-of-mouth contracts which was hitherto not possible due to tedious paperwork involving contract processes.

RSBCs will play a more important role when it comes to legal functions and Contract related tasks. Using Unregulated Blockchains (like Bitcoin or Ethereum) on which the Government (or Sovereign Authority) has no control, can lead to problems in standardisation, security and authenticity when it comes to contract execution. Moreover Law enforcement on a Blockchain is unthinkable when it comes to enforcement on a Private (Unregulated Blockchain). Thus a Government Regulated Blockchain (Controlled Blockchain) is a must in such situations. And RSBCs will be ideal platforms on which public services can be provided in a secure manner.

The various parameters of comparison (for both Blockchains) vis-a-vis suitability to be used for legal functions and systems are as follows:

	CONTROLLED BLOCKCHAIN (RSBCs)	**UNREGULATED BLOCKCHAIN (BITCOIN,ETHEREUM)**
Contract Execution	Possible (based on K-Y Protocol)	Possible in only some Blockchains
Sovereign Guarantee	Provided by Government	Not provided by governments
Legal Recognition	Can be mandated by legislation	Gives scope for ambiguity
Security	Highly Secure	Depends on the Blockchain and its development team
Turing completeness	Yes	Depends on the Blockchain. (Bitcoin is Turing Incomplete)
Trust	Trustless Network guaranteed by Sovereign Authority	Presumed Trustless Network not guaranteed by Sovereign Authority
Price Manipulation	Very Difficult, as Price is monitored by the Sovereign Authority and managed in effort to maintain Parity with Fiat currency	Can be easily speculated and manipulated by unscrupulous elements

We can see that Controlled Blockchain has all the essential characters that make it suitable to be used for legal systems and functions.

CONCLUSION

If we adopt Blockchain technology in the field of law and legal services, we see that it will have a cascading impact in many areas. Entire business processes will undergo a sea transformation. Litigation process itself will get simplified. The burden on courts will be drastically reduced.

More and more economic activities can be brought under the ambit of contract law. Many jobs will obviously be automated. But it will open up new areas where law is applied. The Justice process can focus more on niche areas like criminal law where subjective interpretation of human actions is a necessary part of the Natural Justice system.

But all this disruptive change can be brought about in an orderly manner only if Controlled Blockchains are deployed. Instead of destroying existing systems, we can shift existing systems to newer platforms with minimal disruption and maximal continuity. Unregulated Blockchains can indeed be destructive. On the other hand, Controlled Blockchains allow the power of Blockchain technology to be harnessed in the best and smoothest way possible.

REFERENCES

[1] Hegadekatti, Kartik and S G, Yatish, The K-Y Protocol: The First Protocol for the Regulation of Crypto Currencies (E.g.-Bitcoin) (February 13, 2016). Available at SSRN: https://ssrn.com/abstract=2735267

[2] Hegadekatti, Kartik and S G, Yatish, Roadmap for a Controlled Block Chain Architecture (August 13, 2016). Available at SSRN: https://ssrn.com/abstract=2822667

[3] Joanne Harris (23 June 2016). "Revealed: Global 200 deliver £81bn revenue in 2015".