Issues in Enforcing Cryptocurrency Contracts: A Legal Perspective

Prof. Gautam B. Singh
Professor
Department of Computer Science
and Engineering
Oakland University,
Rochester, MI, USA.

Abstract

This paper examines the interplay of enforcing contracts that are based on cryptocurrency as consideration. The technological basis for implementing cryptocurrency using block-chains are described, and its volatility is discussed from a historical perspective. The underlying legal basis for contract enforceability is discussed as well the issues related to the consideration's adequacy and sufficiency. Validity of cryptocurrency contracts are discussed from a standpoint of the legal theory of illusory contracts. The paper provides some guidance for contract formation within the virtual worlds spanning multiple jurisdictions and utilizing cryptocurrency.

Keywords

Blockchain, Bitcoins, Cryptocurrency, Contract Law, Illusory, Mining Cryptocurrency.

1. Introduction

Blockchain based cryptocurrencies, such as the Bitcoins, has been gaining a general acceptance by the business community. Bitcoins transactions can be made through wiring the currency. The signature of the sender is a unique security code encrypted with 16 distinct symbols that are decoded by a purchaser to obtain the cryptocurrency transferred. Bitcoins can thus be used for buying or selling goods and services. A transaction using Bitcoins as consideration gains its trust and security by utilizing a peer-to-peer the computer network that maintains a distributed ledger protected by a symmetric public key cryptography framework.

The underlying block chain technology is used for bookkeeping. Safeguarding mechanisms are built in to this framework to achieve the authorization, balance verification, prohibition on double spending, prohibition on alterations, and delivery of assets. And generally, the transactions can be completed in minutes. Since cryptography is used to ensure authorization the transactions are secure. So, the question from a legal perspective is the types of issues that could arise in entering a contract that is secured using cryptocurrency such as Bitcoin.

The paper first provides a brief overview of block chain technology and the Bitcoin framework as its specialized use case. Next, the basic requirements of contract formation, its validity, and enforceability is discussed in reference particularly to how the validity and enforceability requirements of contracts may manifest in cryptocurrency based *smartcontracts*. Note that the term *smart-contracts* generally refers to contracts secured by cryptocurrency such as Bitcoins. Finally, the set of guidelines are offered which in the author's opinion, should be followed to minimize risks in cryptocurrency contracts.

2. Blockchains

Blockchain, or a distributed ledger technology, is used for tracking database for Bitcoins transactions. Bitcoin.org defines a blockchain as "a shared public ledger on which the entire Bitcoins network relies." All confirmed transactions are included in the blockchain. Blockchain enables individuals and organizations to process transactions in decentralized manner obviating a need for central bank serving as an intermediary for the transaction verification. Instead, Blockchain utilizes cryptography and consensus to allegorically verify transactions.

While blockchain technology was originally developed for cryptocurrency, it has evolved to a point where it can provide a reliable alternative for many third-party verification use cases where currently trust brokers are utilized as transaction intermediaries. Further, the use of distributed ledger in a blockchain essentially decentralizes this trust. And in doing so, it substantially reduces costs and processing delays of transactions in comparison to traditional broker mediated transactions. There are four main components of a decentralized verification technology such as block chain. These are: (1) A mathematically proven unique voucher serving as the consideration for exchange of goods, services or assets; (2) A peer to peer network essentially comprising of

individual users with connected computers without a central server; (3) A Turing complete virtual machine capable of running any computer program; and (4) A consensus formation algorithm enabling blockchain users to reach a consensus about the current state of the blockchain.

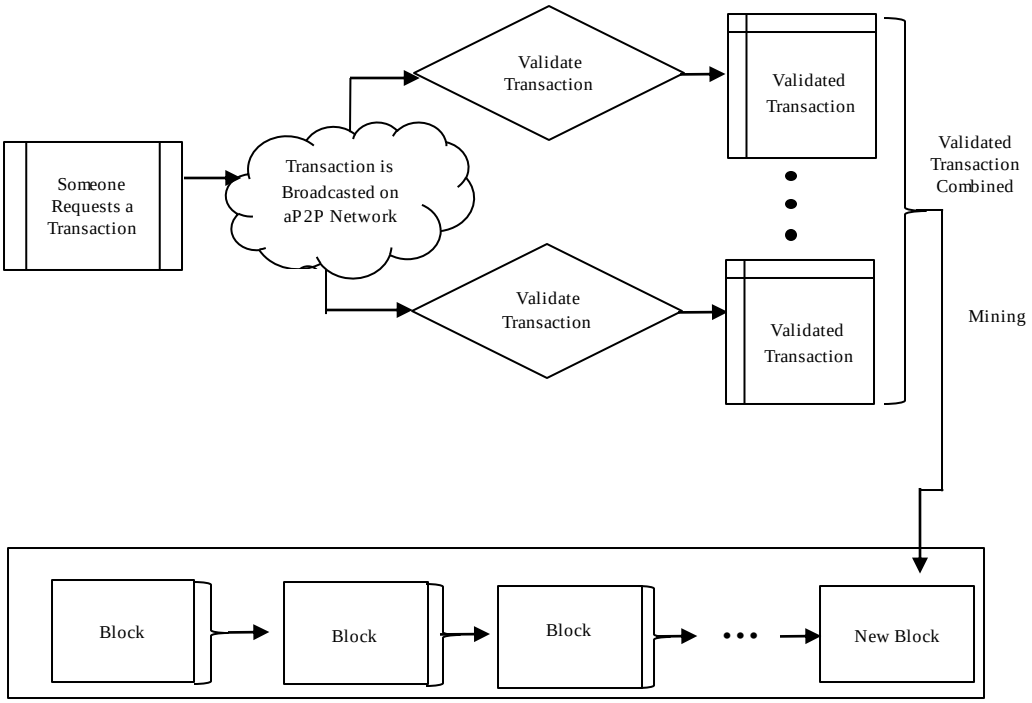

Figure 1: Result of Applying a Transaction

The distributed cryptocurrency ledger is modeled as a state machine where the ledger in a given state has a specific collection of Bitcoins owned by a given set of 20-byte cryptographic addresses (or owners). These Bitcoins that have been mined but not yet spent is referred to as UTXO or "unspent transaction outputs." Each UTXO has a denomination and an associated owner address.

A transaction contains a reference to an existing UTXO and a cryptographic signature. The cryptographic signature is generated through the use of the private key for the UTXO-owner's cryptographic address. Each transaction produces one or more UTXOs to be added to the new state (i.e. the recipients of the Bitcoins). A transaction is applied only when it is able to sustain the ledger's integrity. That is, when the

sum of all the input UXTOs equal to or greater than the sum of all the output UTXOs.

As an example of the protocol, consider the following example. Suppose Adam wants to send 3.4 BTC to Betty. First, Adam will look for a set of available UTXO that he owns which total up to more than 3.4 BTC. Then he creates a transaction with all those inputs. With 3.4 output, BTC assigned to Betty, any left over BTC will be assigned to as output to back to Adam as left over change from the transaction.

The challenge is to implement this transaction using a distributed ledger such that a consensus is maintained at each stage of any transaction. As the blockchain underlying Bitcoins has to maintain and enforce this consensus, its peer-to-peer network produces a "block" of transactions every ten minutes. Each new block in the blockchain contains a timestamp, a nonce, a reference to the hash of the previous block, and a list of transactions occurring after the previous block. Thus, a persistent blockchain representing the latest state of Bitcoins ledger is maintained.

The algorithm for adding a new block requires ensuring that (a) the previous block being referenced by this block exists, (b) is valid, (c) the timestamp of the current block is greater than that of the previous block, and (d) the current block includes a valid "proof of work." The concept of a proof of work relies on Bitcoins mining and is vital to the progressive addition of blocks to the Bitcoins blockchain as further explained below. Bitcoins mining is the process of determining a target hash to be used in addition of a new block to the Bitcoins blockchain. It entails the execution of a hashing algorithm by first taking the timestamp and the hash value of the header information in the most recent block. Further, the list of transactions to be encoded into the new page are added and with the hash value of block contents computed as a Merkle Tree. A miner must add a "nonce" – a 4-byte number used once – to this value and compute the resulting hash value. If this resulting hash value is less than the target hash value, the newly encoded block is added to the block-chain. It is a process of computing this nonce that is referred to as the proof of work. The miner who accomplishes this task gets to add a new block to the blockchain and paid in cryptocurrency for their efforts.

3. Research Methodology

The process of adding a new block to the block chain entails the selection of all the transactions that the miner wants to include into the new block, plus a single coinbase, or coin-generation, transaction to their own address. They may include any transactions they want and form a tree of transactions hashed into the Merkle root and referenced by the header of the new block.

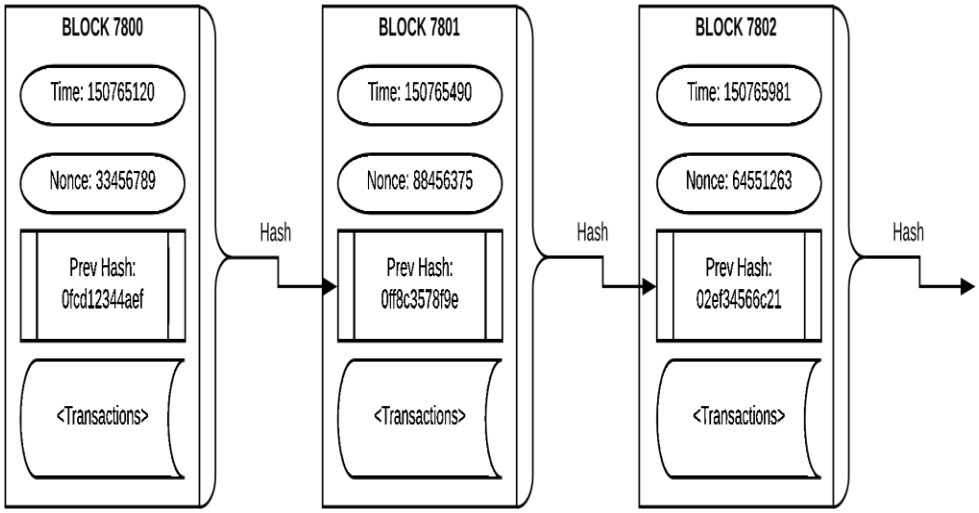

Figure 2: Mining a New Block to Insert into Blockchain

The blockchain, or the network of distributed ledgers, only accept those blocks that contain valid transactions. A valid transaction defined as the one that contains valid inputs with unspent UTXOs with valid cryptographic signatures.

A new block comprises of a 4-byte version number, a 32-byte hash value of the previous block, a 32-byte hash representing the Merkle root for the tree of the current block's transactions, a 4-byte timestamp representing the number of seconds elapsed since 1970-01-01 00:00, a 4-byte number representing the current mining difficulty level, and a 4-byte nonce representing mining.

Thus, when a miner enters the game, it tries a nonce of 0 and checks if the hash in under the current target. If the current target is not met, the miner increments the nonce and hash again and tries again. This process is continued until the block hash falls below the current target. At this point, the miner's block's header and its associated transactions are added to the block chain. And, the amount of Bitcoins specified in the coin base for the newly added block are credited to the miner's address.

4. Smart Contracts

Smart contracts facilitate business transactions enabling an exchange of anything of value such as goods, money, shares, and property with the use of a blockchain. Being on the blockchain the transactions are fully transparent and help prevent fraudulent double sales. And do this in conflict-free manner without necessitating the services and expenses of a retaining a broker or a middleman. Smart contract transactions are thus lightweight and facilitated electronically. When Bitcoins, or any agreed upon consideration, gets credited into the seller's account, the corresponding benefit of the bargain is credited into the buyer's account. Moreover, since smart contracts maintain this ledger transparently, the block chain can also automatically enforce the obligations of the contract with the rules and penalties agreed upon by the parties.

Smart contracts are computer programs, or agents, that autonomously execute the terms of a contract. Smart contracts can enforce the terms such as for example, if the payment of a specific asset is not made timely, an enforcement software program may revoke the access to the resource. Therefore, the realm of the cyber-world is extended to the physical world through interface to the IoT devices.

Cryptocurrency such as Bitcoins provides a fair and automated access to consideration in a secure decentralized transaction mechanism such as blockchains can programmatically enforce any agreed upon terms of a contract. As an example, the Ethereum framework supports the Turing-complete code. This, in turn, enables the enforcement of decentralized smart contracts. Ethereum is fed by source data from trustworthy secondary sources such as websites that provide relevant data about the physical world such as the location of real objects, such as an automobile or a machine, which is needed for automated enforcement of contracts.

The reliability and availability of these data feeds sometimes referred to as "oracles," continues to be a challenge and is an obstacle for the full realization of the power of implementing decentralized smart contracts.

5. Crowdfunding – Trading with Trust

Crowdsourcing has generally been referred to as a firm solving a business problem using ideas, feedback, and solutions for internet users. Along the same vein, Crowdfunding is the practice of raising funds from a number of Internet users and has been defined as an open call by a company to its Internet users to provide financial resources either as donations or in exchange for some rights in the company. Crowdfunding is a common mechanism utilized by starting entrepreneurs looking to fund new ventures with the support of small contributions from a large pool of individuals. Crowdfunding is facilitated by the internet and obviates the need to engage financial intermediaries.

Unified blockchain based equity crowd-funding platforms provide distributed ledger where a company could exchange shares directly with a number of investors in a secure and transparent manner with complete data-integrity with substantial immunity to data tampering. Using a blockchain, issues such as double payment for single security are resolved and transfers of the company shares are permanent. Further, the blockchain maintains the ownership of the assets which dispenses the need for maintaining paper certificates of ownerships.

5.1 Security and Exchange Commissions

One advantage of the ability to transfer funds from investors to entrepreneurs' account using a peer-to-peer platform is that the need to set up a trading platform where a centralized tracking of assets is eliminated. With persistent transactions retained by the Blockchain, a stock ownerships levels and registration of stockholders for exercising their voting rights are automated and error-free and transparently accomplished at the conclusion of the fund raising phase.

One key advantage of using blockchain is that the need to utilize a secure broker for strict compliance with regulatory framework for investing can be eliminated. There is no need to maintain a capital pool, as in a centralized investing scenario, since the consideration and the quid-pro-quo moves directly between the parties with no need for a middleman. This saves the additional cost and the potential risk associated with a centralized broker.

6. Issues and Legal Challenges

The traditional requirements for contract formation include a mutual assent, offer, acceptance, and consideration. Within the context of cryptocurrency and smart contracts, two issues are significant. First, whether when a contract is entered into a blockchain through the interactions of agents, is there legally cognizable mutual assent – that is does the parties actually had the intention to enter the contract that the software agents entered into. And second, is whether the contract is supported by adequate consideration, or rather legally recognized consideration.

6.1 Mutual Assent

With regards to the first issue, a business is cautioned to verify that the software agents, working under the agency law, have the level of authority necessary to bind their principal. And second, how can a smart-contract offeror and offeree in fact verify that the agents have such binding authority. Within the context of online shopping, a business initiating a transaction must make sure that the obligee has been contractually bound before making an irreversible transfer of the consideration. This is significant because the obligee can repudiate on grounds that they never intended to be bound by the contract given that there is no legal enforceability of smart contracts entered into by agents, the situation is more akin to that of a trust based economy.

6.2 Consideration

Every legal contract must be supported by adequate consideration. Courts are not generally concerned with the sufficiency of consideration as the aspect of mutual assent, another requirement for contract formation discussed above, inherently accounts for consideration's sufficiency. However, parties can seek a judicial

review of the adequacy of contract's consideration – particularly to ensure that the contract is not illusory. That is, what appears to be a benefit of a bargain is in fact just an illusion. For this reasons, contract for prediction of future or accurate *tantric* readings are considered illusory and unenforceable.

Within the context of contracts supported by cryptocurrency, the logical question to ask is whether a court could potentially consider these to be illusory as well. To answer this question, we must compare the cryptocurrency with other non-cryptocurrency based consideration such as cash, promissory notes, or negotiable instruments. The common theme we find is that a collateral backs up non-cryptocurrency contracts. For example, all cash transactions are guaranteed by the country's reserve bank, negotiable instruments guaranteed by the maker's bank and the bank's insurance company, and typically notes are backed by a collateral, and securities by the issuer's assets. There is no such centralized collateral that backs up cryptocurrency. The exchange of bitcoins is essentially similar to a barter system where the valuation of commodity being exchanged is determined by the entities exchanging the commodity taking the transaction out of the realm of regulatory schemes of consumer protection.

6.3 Adhesion Clauses

Adhesion contracts are generally unenforceable because the courts view them as lacking mutual assent. When one party is forced to accept the terms of a contract, there is, in court's view, no quid-pro-quo and therefore no meeting of the minds.

Blockchain contracts have a semblance of adhesion contract. When the terms are agreed upon, the exchange is complete, and a record is made into a distributed ledger. This being an irreversible step makes the transaction akin to an adhesion clause in a contract. On the flip side, however, theoretically, the transaction may be reversed upon the initiative of the recipient however under a court order. However, the pre-condition of the reversal transactions are met will not be in the control of a court, but rather in the control of the state of the blockchain.

For these reasons, a blockchain transaction should be viewed as an agreement to an adhesion clause within a contract.

7. Illusory Contracts

In *Century 21 American Landmark, Inc. v. McIntyre,* 68 Ohio App.2d 126, 427 N.E.2d 534 (1980), an Ohio court provided a means of an illusory contract. In that case, the court stated that "a contract is illusory only when by its terms the promisor retains an unlimited right to determine the nature or extent of his performance; the unlimited right, in effect, destroys his promise and thus makes it merely illusory." *Id.* at 536-37.

This would be the case when the contract between two parties was terminated by the actions of the third party. An illusory promise, one which "by its terms makes performance entirely optional with the promisor," cannot form the basis for a valid contract, *Pardieck v. Pardieck*, 676 N.E.2d 359, 364 n. 3 (Ind.Ct.App.1997), because "a contract is unenforceable if it fails to obligate [one party] to do anything." *Indiana-American Water Co. v. Town of Seelyville*, 698 N.E.2d 1255, 1260 (Ind.Ct.App. 1998).

At a fundamental level, the enforceability of any legal contract has to be assumed for society to place reliance and faith into the promise. However, this enforceability must be outside the blockchain which in essence is a tamper-free distributed ledger system.

In the civilized world, the courts enforce contracts. In order to enforce a contract, however, a court must have personal jurisdiction i.e. enforcement powers–over contracting parties. With geographical boundaries becoming fuzzy on the blockchain, this becomes a difficult proposition for a smart contract to guarantee. Consequently, with no guarantee of enforceability, it can be argued that smart contracts and other crowd funding contracts are in fact illusory. Care must be therefore taken to ensure that the contract language is incorporated with the blockchain transactions where parties' agent submits themselves to an agreed upon jurisdiction and venue.

8. Conclusions

The paper presented an overview of the blockchain technologies and the role of cryptocurrency, such as bitcoins, within the context of business transactions. Some typical applications such as smart contracts and crowdfunding using blockchain were discussed. Legal issues relate to the enforcement of such transactions were then described. In conclusion, it should state that the blockchain base system is a trust based, barter system where the value of a good or service is essentially levied with a commodity, namely the Bitcoins. While exchanges exist for converting bitcoins into currencies, there is no authoritative guarantor for this commodity the value of which is established by the value that peers place on it.

References

1. Buterin, V., et al. (2014, Last Accessed 09/30/19). A next-generation smart contract and decentralized application platform. Ethereum *White Paper*, 3, 37. https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf.
2. *Century 21 American Landmark, Inc. v. McIntyre*, 68 Ohio App.2d 126, 427 N.E.2d 534 (Ohio Appeals Court, 1980)
3. *Indiana-American Water Co. v. Town of Seelyville*, 698 N.E.2d 1255, 1260 (Indiana Court of Appeals, 1998)
4. *Pine River State Bank v. Mettille*, 333 N.W.2d 622 (Minnesota Supreme Court, 1983)
5. Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM* , *61*(7), 95–102.
6. Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2014). Is bitcoin a decentralized currency? *IEEE security & privacy*, *12*(3), 54–60.
7. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
8. Reid, F., & Harrigan, M. (2011). An analysis of anonymity in the bitcoin system. In *Privacy, security, risk and trust (passat) and 2011 ieee third inernational conference on social computing (socialcom), 2011 ieee third international conference on* (pp. 1318–1326).

9. *Pardieck v. Pardieck*, 676 N.E.2d 359, 364 n. 3 (Indiana Court of Appeals, 1997)
10. Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Current opinion in environmental sustainability*, *28*, 1–9.