Smart Contracts and Distributed Ledger Technology: A Lawyer’s Guide

Presented by:
Ken Moyle

www.clearlawinstitute.com

Questions?
Please call us at 703-372-0550 or email us at info@clearlawinstitute.com
All-Access Membership Program

Join thousands of professionals who access our hundreds of courses each year

- Earn continuing education credit (CLE, CPE, SHRM, HRCI, etc.) in all states at no additional cost
- Access courses on a computer, tablet, or smartphone
- Access more than 75 live webinars each month
- Access more than 750 on-demand courses

Register within 7 days after the webinar using promo code “7member” to receive a $200 discount off the $799 base price.

Learn more and register here: http://clearlawinstitute.com/member
Smart Contracts and Distributed Ledger Technology
A Lawyer’s Guide

Agenda

Concepts and Confusion
The Lexicon
- Distributed Ledger
- Blockchain
- Cryptocurrency
- Smart Contracts

Smart Contracts: Theory and Reality
- Legal vs. Technical viewpoints
- Common Accord

Initial Coin Offerings and SAFTs
Regulatory Developments
- State blockchain statutes
- Delaware

Resources
The digital revolution is radically changing the kinds of relationships we can have. What parts of our hard-won legal tradition will still be valuable in the cyberspace era?

- Nick Szabo, 1996

“What is the best way to apply these common law principles to the design of our on-line relationships?”
The Lexicon

Language of distributed ledger technology
Blockchain
- Immutable record
- Record maintained outside parties' control

Smart Contract
- Prescribed outcome based on conditions
- Outside control of interested parties

Legal Agreement
- Enforceable under common law
- Disputes resolved under law
Distributed Ledger

- A distributed ledger is a type of database spread across multiple sites, regions, or participants.
- All of the participants on the distributed ledger can view all of the records in question. The technology provides a verifiable and auditable history of all information stored on that particular dataset.
- A blockchain is a type of distributed ledger.

Blockchain

A continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data.
The first distributed blockchain was conceptualized in 2008 by an anonymous person or group known as Satoshi Nakamoto and implemented in 2009 as a core component of **bitcoin**, where it serves as the public ledger for all transactions.

---

**Distributed Ledger vs. Blockchain**

**Distributed Ledger**

A database that:
- Is decentralized into nodes (participants, sites, regions, etc.)
- Requires consensus of nodes to add data
- Records data with a timestamp and a cryptographic signature

**Blockchain**

A type of distributed ledger that:
- Creates “blocks” of encrypted data that point to the previous blocks
- Uses hash values as signatures
Cryptocurrency

A digital asset designed to work as a medium of exchange using cryptography to 1) secure the transactions, 2) control the creation of additional units, and 3) verify the transfer of assets.

- The invention of the blockchain for bitcoin made it the first digital currency to solve the double spending problem without the need of a trusted authority or central server.
- Blockchain’s “proof of work” consensus mechanism makes it impractical to exploit.
- “Miners” are compensated for solving puzzles in order to create blocks, ensuring participation in the growing network of nodes.
DLT, Blockchain & Cryptocurrency

Distributed Ledger
- Verifiable by multiple participants
- Viewable by all participants

Blockchain
- Immutable record
- Hash as signature

Cryptocurrency
- Proof of work
- Miners/reward

Ethereum
- An open-source, public, blockchain-based distributed computing platform and operating system.
- Cryptocurrency ("Ether")
- Turing-complete computing environment (EVM) featuring “smart contract” functionality
Smart Contract

• Introduced by Nick Szabo in 1996 (before blockchain)
• Problem of immutability left Smart Contracts mostly theoretical
  • Potential for fraud, censorship, third-party interference
• Advent of blockchain revived interest in so-called “self-executing” legal contracts
• Much confusion about the definition and purpose of Smart Contract

Smart Contract: What is it?

• “A smart contract is a computer protocol intended to facilitate, verify, or enforce the negotiation or performance of a contract.” – Wikipedia
• “A smart contract is a computer protocol that facilitates the transfer of digital assets between parties under the agreed-upon stipulations or terms.” – Techopedia
• Smart Contracts are “autonomous agents” that live inside of the ... execution environment, always executing a specific piece of code when “poked” by a message or transaction, and having direct control over their own [token] balance and their own key/value store to keep track of persistent variables. - Ethereum
• Smart Contract is an event driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger that can take custody over and instruct transfer of assets on that ledger. – AZ HB 2417
• A smart contract is an agreement in digital form that is self-executing and self-enforcing. – Wharton Law Professor
• “Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network.” – Investopia
Blockchain

Smart Contracts + Blockchains

AKA the Technologists' view

Smart Contract

This is an actual Smart Contract, written on the Ethereum blockchain

Source: https://www.ethereum.org/token

/* Allow another contract to send some tokens on your behalf */
function approve(address _spender, uint256 _value)
returns (bool success) {
    _allowed[_spender][msg.sender] += _value;
    return true;
}

/* Approve and then disburse the approved contract in a simple tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
returns (bool success) {
    _spender.increaseApproval(msg.sender, _value, _extraData);
    return true;
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value)
returns (bool success) {
    if (_balances[_from] < _value) throw; // Check if the sender has enough
    if (_balances[_to] + _value < balancesOf(_to)) throw; // Check for overflows
    _balances[_from] -= _value;
    balancesOf(_from) += _value;
    balancesOf(_to) += _value;
    balancesOf(_from)[msg.sender] += _value;
    balancesOf(_to)[msg.sender] -= _value;
    balancesOf(_from) -= _value;
    balanceOf(_to) += _value;
    return true;
}

/* This assume function is called whenever someone tries to send ether to it */
function () {
    throw; // Prevent accidental sending of ether
}
Smart Contracts + Legal Agreements

AKA the Lawyers’ view

Smart Contract

Legal Agreement

Blockchain + Legal Agreements

AKA the Real-Estate view

Blockchain

Legal Agreement

This Photo by Unknown Author is licensed under CC BY
Smart Contract

“a set of promises, specified in digital form, including protocols within which the parties perform on these promises” without the use of artificial intelligence. – Nick Szabo
Common Accord

• http://www.commonaccord.org/
• Attempting to bridge the gap between smart contracts and legal contracts
• “Wise” contracts

How Smart Contracts Work

Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman. Built upon a distributed ledger, a smart contract is usually:

1. Pre-written logic in the form of computer code
2. Stored and replicated on the distributed ledger
3. Executed and run by the network of computers running the ledger
4. Can result in updates to accounts on the ledger (i.e. payment for an executed contract)
How Smart Contracts Work

Using the Ethereum platform, smart contracts can be programmed using basic logic. On the most basic level, they can:

1. Perform calculations (i.e. calculating interest)
2. Store information (i.e. membership records)
3. Send transactions to other accounts (i.e. payment for a good or service)

But most importantly, smart contracts are *autonomous*. They are not controlled by anyone — instead, they self-execute based on a set of instructions that the parties have agreed to (i.e. the code).

Source: Etherparty.io
How Smart Contracts Can Break

• Prodigal contract
  • Contract gives away Ether to an arbitrary address which is not an owner, has never deposited Ether in the contract, and has provided no data that is difficult to fabricate by an arbitrary observer

• Suicidal contract
  • Contract can be killed by any arbitrary account
  • Can sometimes continue to add to contract balance (posthumous contract)

• Greedy contract
  • Contract remains alive and locks Ether indefinitely, allowing it be released under no conditions

Token sales, or “ICOs”

• ICOs are similar to initial public offerings, or IPOs, in that they are a way for companies to raise money from the public. In an IPO, a company sells stock, or ownership stakes, to the public; in an ICO, a company sells its tokens. After an ICO, the public can buy, sell, or hold the tokens in much the same way they can stock.

• Ultimately, investors and VCs hope that the tokens gain enough value that they’ll be able to cash out their tokens for a profit.

• The first ICO was held in 2013, but the technique has boomed in recent months. Startups have raised nearly $4 billion since mid-2016, and most of that has been raised since last May.

• There's growing concern about how well companies that are choosing to use ICOs for fundraising are being vetted and how well the public is being informed about the process. Controversy has swirled recently around Centra and Tezos, both of which raised money through ICOs last year.
SAFTs

• Simple Agreements for Future Tokens
• SAFTs are venture capital’s way of adapting to the boom in ICOs.
• In traditional venture capital investing, investors give a startup money in exchange for an ownership stake in the company. But with SAFTs, venture capitalists receive the rights to future tokens instead.
• Typically, the VCs get the rights to a certain portion of the tokens a company issues in an ICO.

Regulatory Developments

Federal agencies respond to DLT
Internal Revenue Service has determined cryptocurrencies should be classified and treated as **property** for federal tax purposes.

Cryptocurrency payments are subject to reporting, and owners must keep track of capital gains or losses associated with any given transaction.

FinCEN issued interpretive guidance in 2013 on money services businesses transmitting/transferring virtual currencies (tokens)

In October 2014, FinCEN released new guidance for custodial bitcoin exchanges and payment processors, ruling that such companies may be considered money services businesses under US law

In July 2017, assessed a $110,003,314 civil money penalty against BTC-e for willfully violating U.S. anti-money laundering laws.
CFTC found Bitcoin to be a commodity for the purposes of Section 4c of the CEA and Part 32 of the CFTC’s Regulations.

Enforcement action *In re Coinflip, Inc.* (2015) directed defendants to cease and desist designating put and call options for the delivery of Bitcoins as eligible for trading.

SEC formed Cyber Unit early 2017 to investigate cyber fraud, hacking, misconduct. Specifically lists violations involving distributed ledger technology and initial coin offerings.

Issued guidance in July 2017 that tokens may be classified as “investment contracts” under Article 8 of the Uniform Commercial Code, and therefore subject to Federal securities laws.

On November 16, 2017, SEC Chairman Jay Clayton announced in a symposium on cybersecurity and financial crimes that the SEC would start taking enforcement action against coin offering issuers who fail to register with the SEC.
On Feb. 28, The Wall Street Journal reported that the SEC had sent subpoenas in recent weeks to dozens of tech companies and individuals who are involved in cryptocurrency. The targets of the subpoenas include companies that have launched initial coin offerings (ICOs), the cryptocurrency equivalent of IPOs, as well as their lawyers and advisers. The subpoenas reportedly include requests for information on how ICO sales and pre-sales are structured. The SEC is also requesting the identities of the investors who bought digital tokens.
Delaware Blockchain Initiative

- Amendments to DGCL effective August 1, 2017 allow companies to create and maintain corporate records, including stock ledgers, on a blockchain.
- Delaware Public Archives seeking to store state archival records on a distributed ledger.
- Delaware has announced that it expects to introduce “smart UCC” filings that “will automate the release or renewal of UCC filings and related collateral.”

Vermont Blockchain Laws

- H.868 (enacted 2016) provides that a blockchain-based digital record will be considered a business record under the Vermont Rules of Evidence
Colorado SB 86

Directs Colorado's chief information security officer to evaluate the costs and benefits of using distributed ledgers in various government systems, and to determine blockchain's capability in handling cyberattacks compared to traditional computer systems.

Wyoming HB 0070

“Open Blockchain Tokens – exemptions,” dubbed the “utility token bill,” would provide that a blockchain token that is not deemed a security is specifically exempt from securities legislation as well as money transmitter laws.
Arizona Blockchain Laws

- HB 2417 amended state e-signature law in March 2017 to clarify that electronic records, signatures, and smart contracts — guaranteed via blockchain technology and governed by UCC Articles 2, 2A, and 7 — are treated as legal electronic signatures.
- HB 2216, enacted April 2017, prohibits the use of blockchain technology to track firearm information.

Nevada Blockchain Law (SB398)

- Enacted June 5, 2017, amends state e-signature law to clarify legal recognition of the use of blockchain technology for electronic signatures and records
- Prohibits a local government from: 1) imposing a tax or fee on the use of a blockchain; (2) requiring a certificate, license or permit to use a blockchain; and (3) imposing any other requirement relating to the use of a blockchain.
Tennessee SB 1662

Amends TN Uniform Electronic Transactions Act:
- A signature that is secured through blockchain technology is considered to be in an electronic form and to be an electronic signature.
- A record or contract that is secured through blockchain technology is considered to be in an electronic form and to be an electronic record.
- Smart contracts may exist in commerce. No contract relating to a transaction shall be denied legal effect, validity, or enforceability solely because that contract contains a smart contract term.

California AB 2658

Amends California Uniform Electronic Transactions Act (UETA):
- the definition of “electronic” record and “electronic signature” would be expanded to encompass those secured via the blockchain
- the legal definition of “contract” would be expanded to encompass a smart contract
- data ownership/use would extend to someone performing interstate or foreign commerce on the blockchain in California “with respect to that information as before the person secured the information using blockchain technology.”
Redefining Contracts and Signatures?

- “Smart Contract” means an event driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger that can take custody over and instruct transfer of assets on that ledger.
- “Blockchain technology” means distributed ledger technology that uses a distributed, decentralized, shared, and reciprocal ledger, that may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable, is auditable, and provides an uncensored truth.

- A signature that is secured through blockchain technology is considered to be an electronic signature be in an electronic form and to be an electronic signature.
- A record or contract that is secured through blockchain technology is considered to be in an electronic form and to be an electronic record.
- Smart contracts may exist in commerce. No contract relating to a transaction shall be denied legal effect, validity, or enforceability solely because that contract contains a smart contract term.
- “Contract” includes a smart contract (California).
Modernization of Government Technology Act

- MGT is part of National Defense Authorization Act (NDAA), currently in conference committee
- Under the MGT provision, government agencies are authorized to spend their working capital funds for modernization initiatives falling in three categories, namely, migrating legacy systems to the cloud services, cybersecurity and other innovative and disruptive technologies and platforms.
- Although it was not categorically stated in the bill, Blockchain technology is qualified as a potential direction for the allocation of funds for further advancement beyond the proof-of-concept stage at the agency level.

Congressional Hearings

- On February 14, the House Subcommittee on Research and Technology and the Subcommittee on Oversight held a hearing discussing the applications and use cases for blockchain technology. A major theme of the hearing, titled "Beyond Bitcoin: Emerging Applications for Blockchain Technology," was to distinguish Bitcoin from the underlying blockchain technology and to evaluate which applications and use cases hold the most promise.
- Feat. Jerry Cuomo, IBM fellow & VP Blockchain technologies, IBM Cloud
Reference Materials

- Smart Contract Infographic, courtesy Etherparty.io. at http://www.visualcapitalist.com/smart-contracts-blockchain

Other Resources

ESRA (Electronic Signature and Records Association)
With expansive membership and cross-functional representation, ESRA is uniquely positioned to stay on top of current and future conversations around electronic signatures and records.
http://www.esignrecords.org

Chamber of Digital Commerce
Mission to promote the acceptance and use of digital assets and blockchain-based technologies
https://digitalchamber.org/

Common Accord
initiative to create global codes for legal transactions by codifying and automating legal documents
http://www.commonaccord.org/

K6 Partners / K6 Legal Blog
Blockchain law and policy
http://www.k6blog.com
Thank You!

Ken Moyle
ken@k6legal.com
@moyleken
www.linkedin.com/in/kenmoyle