

# Smart Contracts and Blockchain: the Next Wave of ODR

Simon Boehme, Ethan Katsh,

Orna Rabinovich-Einy & Amy Schmitz

# Blockchain Boom

- RISE OF BITCOIN & OVER 1600 CRYPTOCURRENCIES
- GROWTH OF ETHEREUM AND DISTRIBUTED LEDGERS
- MAINSTREAMING OF SMART CONTRACTS (ROCKETLAWYER, LAW FIRMS, ETC.)
- CORPORATE FUNDING OF OVER \$2.1 BILLION IN 2018
- DRAMATIC INCREASE IN HIRING FOR BLOCKCHAIN-RELATED JOBS (TRIPLED OVER THE LAST YEAR!)

# What is Blockchain?

- New system for building trust
  - Convert vehicle for trust from one form to another
- Reliance on a distributed ledger
  - One version of a database record on many computers
  - Trusted because can't be changed
  - Trusted because public
  - Data integrity
  - Identity authentication

# Core Concepts

- Distributed Ledger
  - No central authority to hold ledger or be attacked.
  - All computers (aka nodes) have complete ledger.
- Transparent but anonymous ledger
  - Ledger can be public while concealing identity.
  - Private or permissioned ledgers are growing in use.
- Append only Ledger
  - Each entry (aka block) is linked to the previous entry via some algorithm (aka hash)
  - Some nodes (aka miners) are paid for performing calculations (aka proof of work)
- Immutable Ledger
  - Attacks to a ledger are impractical due to need for majority of nodes (aka 51% attack) to agree to a change and the computational power required.

# Some examples

- Bitcoin
  - Employs the blockchain model – ledger, etc.
  - Investment
- Transactions
  - smart contracts
  - Criminal activity

# Another example: The Alt-Right's Favorite Social Network: Gab's Plan To Use Blockchain To Make Itself Indestructible

- Gab.com
- Main forum used by Pittsburgh synagogue shooter
- September 2018 – FILED APPLICATION FOR ICO for \$10 million
- Available Blockchain Alternatives to
  - Domain name servers
  - Web hosting
  - Payment systems
  - Social networks, etc.

# Disruption

- Shipping (belt-n-road initiative in Hong Kong)
- Finance (banks seeking security)
- Records (Estonia & India leading the way)
- Healthcare (securing and tracking data)
- Law (smart contracts and blockchain courts)
- .....

# Smart Contracts?

- In 1994, Nick Szabo, a legal scholar, and cryptographer, realized that the decentralized ledger could be used for smart contracts (on blockchain).
- In this format, contracts could be converted to computer code, stored and supervised by a network of computers.
- Vending machine structure per “if/then” correlations makes them self-enforcing & nearly unchangeable.
- Automatic payment systems replace complex financing & automatic enforcement eliminates lawyers & courts.



# Benefits of a Smart Contract

Smart contracts are protocols that automate the performance of contractual terms based on the existence and/or occurrence of pre-defined conditions.



## Speed & Efficiency

Smart contracts automatically self-execute, saving time, money and human input.



## Encryption & Security

Transaction data can be encrypted so that it is only accessible with the appropriate key.



## Autonomy

No need to rely on (or pay) third parties.



## Immutability

Transaction data is immutable, duplicated many times and cannot be lost



## Trust & Transparency

Transaction data is shared with and audited by network participants.

# Smart Contract Examples

## Sharing Economy

P2P Payments - matching of parties in P2P markets and automated value transfer.

## Supply Chain

Provenance/Track & Trace - smart contracts and transaction data stored as a blockchain evidence log can be used to track custody of goods in real time, verify provenance and automate payments.

## Financial Services

Micro-Transactions - automated usage-based micro-payments.

## Insurance

Automated Claims Processing - occurrence of insured event automatically triggers claims process.

## Construction

Project Finance - escrow and automated/self-enforceable payments based on performance subject to contractual conditions precedent.

## Telecoms

Mobile Wallets & Digital Asset Transactions - telecom providers can integrate smart contracts into digital wallets to facilitate micro transactions using digital assets.

# Are Smart Contracts “Contracts”?

- Algorithmic code = unclear offer, acceptance & consideration
- Decentralized = no identifiable jurisdiction
- Anonymous = unclear who & where the parties are
- Coding = unclear documentation (civil law) and status under Statute of Frauds (common law)

# Issues with Smart Contract Enforcement

- **Breach/Failed Performance**

Like any commercial agreement, disputes may arise if either party to a smart contract fails to perform.

- **Coding Error/Mistake of Fact**

Disputes may arise because of failed performance or incorrect outcome due to a fundamental error in the coding of the smart contract.

- **Remediation**

Disputes may arise if a smart contract needs to be cancelled, reversed or amended.

- **Lack of Capacity**

Disputes may arise where a smart contract is entered into by someone who lacks capacity and the smart contract self-executes.

- **Incomplete Contract**

Disputes may arise because of inflexible self-execution (or lack thereof) that does not account for exceptions or nuances in a given relationship.

- **Enforcement**

Enforcement of smart contracts through traditional channels (e.g., litigation, ADR, etc.) may be impossible because the parties may be anonymous and/or in different jurisdictions, or impractical because of the time and resources required to do so.

- **Adjudicator Expertise**

Legacy dispute adjudicators are not likely to have the technical knowledge to manage smart contract-related disputes.

# Blockchain Dispute Resolution

- Arbitration on the Blockchain (sagewise, openbazaar)
- Crowdsourced dispute resolution – tokenized voting on the blockchain (“mob justice” or gamification?)
  - Kleros
  - Jur
  - Aragon
  - Delphi, Rhubarb And more!
- Automated “bot” resolutions
- Are these processes designed with DSD principles in mind?

# Dispute Systems Design Principles

- **Leaders**

- Initiative; implementation and adoption; quality control

- **Design Process**

- Involving stakeholders; identifying problems; mapping current processes, challenges and barriers

- **Process pluralism**

- Tying process to system goals and values; preference for interests; Efficiency and fairness; preference for interest-based; loop-backs

- **Ongoing commitment**

- Providing resources, incentives and motivation; learning and improvement

# Blockchain and Challenges for DSD

- **Decentralization**

- No middlemen, no central authority, minimal governance
- **BUT:** need initiative, execution & oversight

- **Immutability**

- No problems can arise? No solutions can be devised?
- **BUT:** problems are inevitable, solutions require flexibility

- **Trustless**

- Technological solutions displace need for trust
- **BUT:** technology isn't foolproof, need to engender trust and re-establish where broken

- **Anonymity**

- Important for individual privacy and control over data
- **BUT:** need identity for effective participation and redress

# Dispute Systems Design for Blockchain

- Identify the new middlemen
- Create incentives for the implementation of dispute systems in-house
- Awareness of resolution avenues by users and incentives for use and compliance
- Dispute systems to provide fair and effective avenues of redress (watch for conflict of interest, bias and power relations)
- Dispute systems inherent component of trust
- Use blockchain traits to enhance dispute processes (integrity of data, enforcement of resolution)
- Use dispute data for improvement and prevention
- The devil is in the design



# Is this the Internet all over again?

- The Internet (1996):

- “Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.”

- Bitcoin (2014):

- “Bitcoin is inherently anti-establishment, anti-system, and anti-state. Bitcoin undermines governments and disrupts institutions because bitcoin is fundamentally humanitarian. There’s an elimination of 3rd party intrusion. It’s purely peer-to-peer. The blockchain is free speech. It’s decentralized, voluntary, and non-aggressive. Bitcoin is not supposed to work within our current mechanisms. Bitcoin needs not entities of authority to acknowledge it, incorporate it, regulate it, and tax it. Bitcoin does not pander to power structures, it undermines them.”

# Is this the internet all over again?

- Who's in charge?
- Trust among strangers?
- Focus on major catastrophes, and intentional fraud
- Reality of many small scale, often unintentional disputes
- Can technology escape government regulation?
- From “take it or leave it” to assuming (some) responsibility
- From arbitration to facilitation
- From human 3<sup>rd</sup> party to automated 4<sup>th</sup> party
- From dispute resolution to dispute prevention

# Building Optimal ODR in the Blockchain

- Clear need for ODR to resolve smart contract disputes
- Impracticability to code for all possible breaches of contract (bugs, fraud, unconscionability, unpredictable behavior)
- Importance of preserving anonymity and efficiency
- Insistence on ethical design and execution
- Application of ICODR principles and standards

# Blockchain technology for Dispute Resolution

- Like ODR, moving beyond blockchain-related disputes
  - Formal and informal
  - Online and offline
  - Dispute data, integrity of resolutions, enforcement