Cloud Crypto Land

Why Smart Contracts and Crypto Assets Won't Change the World

Edmund Schuster

London School of Economics

Motivation

Blockchain technology raises many intriguing *legal* questions

- When are cryptotokens securities / transferable financial instruments?
- Is it possible to create a GDPR-compliant blockchain?
- How should we characterise the legal relationship between a coder/node/initiator/etc and the users of cryptoassets/ cryptocurrencies
- Is a DAO a legal person? Should it be?
- Is it a crime to "steal" from a poorly implemented brainwallet?

Krugman on Interstellar Trade?

Overview

The status quo
- Misleading promises of the blockchain
- What are blockchains to a lawyer?
- Categorising blockchain projects – naked vs. non-naked tokens/coins

Legal obstacles for "smart assets" and "smart contracts"
- A simple argument for why the law would have to adapt for making it all work

Will or should the law adapt to a blockchain future?
- The promise of cryptoassets and smart contracts
- Checking against reality…

Can this be extended to cryptocurrencies?
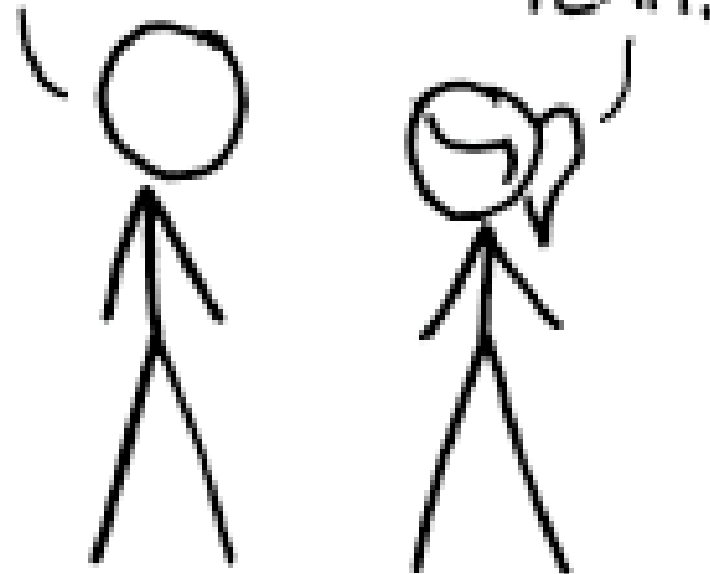
The mythical powers of the Blockchain

"I don't claim to be an expert on it but the most obvious technology is blockchain"

The empty promise of the blockchain

Why do the promises sound so attractive?

- Cost of change and the right comparator
- **We don't do things the way we do because everyone is stupid**
- Change is hard – starting from scratch is lazy

Important to keep trade-offs in mind

- Distributed databases with consensus rules are necessarily inefficient
- May be a price worth paying for decentralisation!

Legal analogues of blockchains

The "physical world"
- Value embodied in physical objects (and control over these objects – "possession")
- Peer-to-peer transactions
- "No double spending" enforced by the law of physics
- *Correlation between possession and legal rights is (and has long been) reflected in legal rules*

The world of intangibles and registered rights
- Transacting in intangibles:
1. P2P + (some) trust – e.g. assigning rights
2. Central ledger, and trust only in the record-keeper – e.g. securities, land register
3. Now: Blockchains – solve the double-spending problem at the heart of 1. and 2.

A simple Blockchain simulator

Legal analogues of blockchains

So in this sense, blockchains replicate features of the physical world

Tokenizing assets is, of course, nothing new

We have been here before

- Negotiable instruments and *lex mercatoria*
- Intrinsically worthless physical objects as representations of valuable rights
- Establishing negotiability – early version of "code is law"?
- But less useful because you need to be online

Cryptoassets

My definition of "cryptoassets"

- Distinguish "naked" blockchains from crypto-tokens as representations of legally rights – "cryptoassets"
- Cryptocurrencies are "naked" in this sense
  - Like merchants deciding to care about the actual pieces of paper, rather than anything they may represent
  - But there are other examples – (CryptoKitties!)
- Other tokens stand in for *something* – are meant to convey rights of some sort
  - E.g. "security tokens", putting assets on the blockchains, etc

→ This type of cryptoasset must be tethered to legal reality to fulfil its purpose

"Smart contracts"

Terminological problems
- this is neither the "contract" itself nor "smart"

Potential benefits of cryptoassets and smart contracts
- How smart can smart contracts be?
- Complexity and usefulness
- Lawyers do **not** spend most of their time suing people for breach of crystal-clear obligations

Algorithms/computer code vs natural legal language

As long as everything is self-contained within the protocol, it can even be "self-executing"
- Small problem: it never is

"Smart contracts"

There is no necessary link between smart contracts and the blockchain apart from "trustlessness"
- Small problem: this has never been a concern of anyone
- Also: Technology has always been available, but rarely used for entire agreements

Another central question: what are the inputs?
- If no inputs (or only passage of time), there's no need for a any of this
- (Lawyers have long had solutions for this)
- But if there are inputs, these also need to be "trustless" - or else there's no point in doing any of this

Massive computational overhead
- Solving this means centralising

Blockchains and the Law as a Synchronisation Problem

A simple argument against the feasibility of cryptoassets and smart contracts:

1. To the extent that cryptoassets represent legal rights, their enforcement depends at least in part on the legal system
2. The law places limits on what can be agreed, even between sophisticated parties
   - Capacity, fraud, duress, *ordre public*, …
3. Legal rules cannot fully be encoded in any formal algorithmic system, so this cannot be solved by and in code

➔ If you want to put anything that is tethered to legal reality on the blockchain, you need a system of legal realignment:

The blockchain must sync with the law

Cryptoassets: Current Legal Obstacles

The alternative?

- State of the blockchain and "state of the real world" as seen by the law *slowly* drift apart
- Cryptoassets *quickly* lose their usefulness as representations of the real world

Cryptoassets: Current Legal Obstacles

Possible approaches to synchronisation

a) Give the state "write permission"! A *super* key valid for all transfers

   - State (e.g. judges) can rectify the blockchain where appropriate

→ But what you now have is simply a very slow and costly database!

Cryptoassets: Current Legal Obstacles

Possible approaches to synchronisation

a) ~~Give the state "write permission"! A *super* key valid for all transfers~~

  ▪ State (e.g. judges) can rectify the blockchain where appropriate

b) ~~Choice of law / contract?~~

c) ~~Oracles? "garbage in – garbage out"; equivalent to a)!~~

d) ~~Adjudication on the blockchain~~

Cryptoassets: Current Legal Obstacles

Choice between rock & hard place?

- Create a centralised blockchain system – all the overhead, none of the advantages
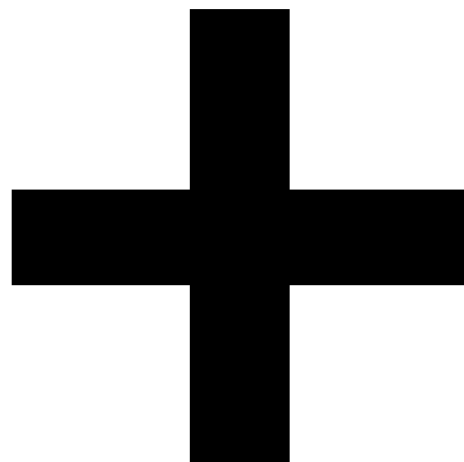
Cryptoassets: Current Legal Obstacles

Choice between rock & hard place?

- Create a centralised blockchain system – all the overhead, none of the advantages *OR*
- Certainty that tokens will not be treated as real representations of *anything*

→Choose one: pointlessness or uselessness

- No justification for inefficient design if feature that necessitates inefficiency no longer present

Cryptoassets: A Legal Fix?

Objections
- I know a guy…
- AI?
- IoT?
- It worked with paper

Law could embrace Blockchain technology
- In principle, "code is law" (or something very close to this) could be adopted by the/a relevant legislator
- Problem: The endorsement would have to be (very nearly) absolute
- Smallest exceptions would hurt

Cutting Out the *Boring, Really Efficient* Middlemen?

Land register E&W

- around £ 5.5 trillion in assets on a ledger
- Cost to users? Around 0.006%, including profit to taxpayer and services

BNY Mellon

- $33.3 trillion in assets under custody
- Total revenue $11bn (0.03%)

Self-execution only *really* works in a credit-free world

Cryptoassets: No Legal Fix in Sight

So could (should/will) the law "give in"?

- Cost/benefit
- History?
- Democracy?
- Turkeys and Christmas?

What about naked blockchains (cryptocurrencies)?

- Fundamental objections do not apply in full
- *Law* does not render meaningful implementation *impossible*
- But: hard to see how they can be *useful* given the existing legal rules
- Admittedly somewhat weaker case on legal fix

Conclusion

A truly blockchain-based economy is incompatible with the current legal systems of virtually all countries

Giving the state special privileges renders blockchain solutions entirely pointless and inefficient

Smart contracts can only reflect rights and obligations that do not in reality create significant friction

Law will *not* adapt to the extent necessary, nor should it

Edmund Schuster
LSE Law Department
E.Schuster@lse.ac.uk
@Edmund_Schuster