Smart Contracts and the Future of Arbitration

Dr Jonathan Ercanbrack
Reader in Transnational Financial Law
SOAS, University of London

Blockchain @ HTW Conference
Berlin
13 June 2025

The significance of smart contracts (SC)

SOAS University of London
100 Years

Contract

- ‘Formalisation of human exchange based on trust’
- Legal institutions normally instil trust in contractual relationships
- Alternatively, we rely on reputation and dense networks
- In both cases, ways to enforce contracts or promises are needed

Blockchain

- A new form of governance – offers an alternative institutional architecture (no intermediaries)
- Replaces trust in human relationships with trust in machines
- SC are machine readable programs that self execute when set of predetermined terms are met (ensuring performance)
- E.g. automatically release payment when goods have been delivered
- Blockchain executes and records SCs in blockchain – difficult, if not impossible, to revoke or modify ex post

Autonomous performance

- Most distinctive and controversial feature, a form of ex ante private ordering
- Parties use SC to increase the legal certainty of their automated assessments
- SC minimise transaction costs of contract negotiation, monitoring, and dispute resolution

A New Mode of Contractual Governance?

- **Code is law**
  - Software and hardware provide the architecture of cyberspace and regulate it
- ***Lex cryptographica***
  - 'A self-ordering and autonomous non-state body of law'
  - Like the medieval *lex mercatoria*
- **Interpretation**
  Courts are asked to interpret the coded terms of a smart legal contract when:
  - Parties disagree about the meaning of terms in a contract (usually where one party has failed to do something)
  - Where the code performs differently to how one or both of the parties had expected
  - Where the code is altered by a third party acting in bad faith (hacked)
  - Where there are errors or bugs in the code or in the oracles (information feeds) relied on
- Most claims in English commercial courts involving finance are contractual
  - Issues of contract interpretation, breach of contract, fraud and negligence prevalent

Arbitration and Smart Contracts

SOAS University of London 100 Years

- **Litigation less attractive?**
  - Absence of legislation, borderless nature (cross-border jurisdictional hurdles), potential lack of expertise of domestic judges, pseudonymous parties, cost and length of time
- **Arbitration**
  - 'a private process in which parties who are in dispute have agreed, either in their contract or after a dispute has arisen, to submit their dispute to an experienced person who they believe will exercise good judgment and impartiality in resolving their conflict'
  - Preferred means of resolving SC disputes?
    - Choice of governing law, seat of arbitration, ability to prohibit class proceedings, provide multi-state dispute resolution mechanism amongst most important reasons
    - Smart contract disputes likely to involve evidence about proprietary software and/or hardware
    - Confidential arbitration will limit disclosure, avoiding material commercial ramifications
  - Where disputes are technical in nature, parties can agree arbitration clause that allows them to appoint technical expert
    - Arbitral institutions: likely to adopt specialist pools of arbitrators with relevant experience
    - Publish blockchain-tailored procedures

Decentralised Arbitration

- **Multisig technologies**
  - Can be a means for arbitrating SC disputes
  - An entirely new paradigm of dispute resolution
  - A“floating form” of private adjudication that has no cooperation with national legal systems
- Custody of bitcoin or other cryptocurrency involves controlling private keys
- **Singlesig wallet** - one way of holding your own keys
  - One master private key can generate addresses for receiving bitcoin
  - If bitcoin is sent to one of those addresses, the amount will be counted towards the wallet balance, and it can only be removed from the wallet after approval from someone who has the private key.
- **Multisig wallet** - a method of securing bitcoin that can require signatures from multiple private keys in order to spend bitcoin
  - Funds stored in bitcoin address (unlike escrow - held by a dispute resolution service provider)
  - Works like a 2 out of 3 keys lock: the adjudicator and each of the two contracting parties have a key, but lock does not open unless at least 2 keys are used

Multisig Arbitration

- Adjudicator cannot autonomously unlock bitcoins in the multi-signature address
- When no dispute arises, parties agree to release payment and transferred to recipient with no adjudicator involvement
- When dispute arises, adjudicator asked to determine whether bitcoins should be transferred to recipient or given back to original sender
- Upon delivering arbitral award, the arbitrator can transfer the virtual currency stored in the blockchain to the successful party by using the private key
- The substantive and procedural rules of the arbitration can be included in the arbitral clause of the SC
- Multisig has '**enforcement jurisdiction**', ie the power to enforce its own norms, an indicator of an autonomous legal order

Considerations

- Under the NY convention, a multisig award would have to be deemed a ‘duly authenticated original award’
  - ‘authenticated’ meaning the process of confirming authenticity of arbitrators’ signature
- Raw transaction data of a multisig transaction can represent a final and binding award in a jurisdiction such as the UK or Switzerland.
- In civil law jurisdictions, multisig transactions may not be viewed as final and binding
- Important because if multisig not capable of being recognized, could be challenged in any court with competent jurisdiction
- Consent to arbitrate - where computer entered into agreement/or law does not recognise as legally binding contract
- Transnational nature of SC makes choosing seat important; avoid dispute; check whether law of chosen seat does not render SC illegal or unenforceable

Danke für Ihre Aufmerksamkeit