SMART CONTRACTS

What are they and how do they work?

Kate Beretta, Senior Associate
BLOCKCHAIN

High level reminder
WHAT IS BLOCKCHAIN?

A blockchain is:

• A distributed data structure
• Replicated and shared across a network
• Blocks holding a record of transactions
• Validated through a consensus mechanism
• Appended to the network in chronological order [each block timestamped]
• Creating an authoritative ledger of transactions

Security through cryptography and the validation / appending through consensus:

1. Hashing
2. Public/private key encryption (asymmetric cryptography)
block n

hash of
block n−1
transactions

block n+1

hash of
block n
transactions

block n+2

hash of
block n+1
transactions

...
SMART CONTRACTS

What is a smart contract? How does it differ from a traditional contract?
TRADITIONAL CONTRACTS

**meeting of the minds**

A la *The Law of Contract in South Africa* (Hutchison et al), 2012:

1. **Formation**
   - Offer
   - Acceptance

2. **Validity**
   - Capacity
   - Formality
   - Legality
   - Possibility and certainty
function approve(address _spender, uint256 _value) returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

function approveAndCall(address _spender, uint256 _value, bytes _extraData) returns (bool success) {
    tokenRecipient(spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw; // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw; // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw; // Check allowance
    balanceOf[_from] -= _value; // Subtract from the sender
    balanceOf[_to] += _value; // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

function () {
    throw; // Prevents accidental sending of ether
}
SMART CONTRACTS

“a computerized transaction protocol that executes the terms of a contract”

- Nick Szabo

- pre-written logic
- that is stored and replicated on a distributed storage platform
- executed by a network of computers
- and can result in ledger updates

Automated execution of a contract?

Source: https://github.com/cogeorg/teaching
SMART CONTRACTS

Already in use?
Important concepts

1. Independent parties – lack of trust

2. Implementation through **conditions** being met – i.e. if/then statements
   - Event-driven
   - Data-driven
   - Automatic and independent execution
   - No third party required to execute or verify execution
   - Certainty
SMART CONTRACTS

Important concepts

3. Resides on the blockchain
   - Triggered when nodes address transactions to it
   - Can hold assets

4. Immutability (of both the smart contract and the output)

5. Only certain blockchain technology supports smart contracts

6. Spectrum of use
Smart Contracts

- Option contract written as code into a blockchain.
- Contract is part of the public blockchain.
- Parties involved in the contract are anonymous.
- Contract executes itself when the conditions are met.
- Regulators use blockchain to keep an eye on contracts.

Source: https://codebrahma.com
Bob leaves his car and car key in a garage locked with a smart contract controlled smart lock. The car has its own blockchain address (public key) 13849Z stored on the blockchain.

Bob wants to sell his car. He identifies himself with his blockchain address (public key) 757382 and uses a smart contract to define the terms of the sale signing it with his private key.

The smart contract is verified by each node on the blockchain network checking if Bob is the owner of the car and if Alice has enough money to pay Bob.

If the network agrees, that all conditions are true, Alice automatically gets the access code to the smart garage lock. The blockchain registers Alice as the new owner of the car. Bob has 20 000€ more in his account, and Alice 20 000€ less.

Alice wants to buy a car. She finds Bob's car listed on the Internet. She signs the contract with her private key transferring 20 000€ from her blockchain address (public key) 389157 to Bob's blockchain address 757382.

Alice can now pick up her car by unlocking the smart lock with her private key.

Source: https://blockchainhub.net/blog/infographics/smart-contracts-explained/
SMART CONTRACTS

How does it work in practice?

• Smart contract (code)
• Smart contract (plain English explanation)
SMART CONTRACTS

Benefits
• Allow multiple parties who don’t necessarily know (or trust) each other to fully transact
• Certainty, predictability and clarity
• Transparency and auditability
• Ease of enforcement, and decreased time and costs

Risks
• Dependency on off-chain data
• Immutability
• Loss of linguistic nuance
SMART CONTRACTS

What does this mean for us as lawyers?

- General consensus that smart contracts will never replace ‘traditional contracts’
- Whether a smart contract gives rise to legally binding contracts will vary depending on the jurisdiction
- Lawyers don’t need to code, but lawyers do need to understand the concept and how it interacts with traditional contract law

Regulation

- Arizona (HB2417) – May 2017
- Electronic Communications and Transactions Act, 2002 (ECTA) allows contracts to be concluded electronically
SMART CONTRACTS

Use cases

• Cryptocurrency transactions & ICOs
• Digital Identity
• Records
• Securities, Derivatives & related (e.g. Distributions)
• Finance, Syndicated Loans & Financial Data Recording
• Mortgages; Land Title Recording
• Trade Finance, Supply Chain & Logistics
• Creative industry (access to and micropayments for digital content)
• Insurance (including Auto Insurance) – peer to peer; and event-driven
• Loyalty and rewards systems
• Gaming & Gambling
• Utilities

Sources:
https://www.ccn.com/smart-contracts-12-use-cases-for-business-and-beyond/
https://blockchainhub.net/blog/infographics/smart-contracts-explained/
THANK YOU

Further reading:

BLOCKCHAIN IN THE LOGISTICS INDUSTRY

Nicola Nel, Senior Associate
Video: Maersk / IBM
1. CURRENT POSITION

2. DIFFICULTIES

3. SOLUTIONS
1. CURRENT POSITION

2. DIFFICULTIES

3. SOLUTIONS
BLOCKCHAIN AND SHIPPING

THE WORLD AS IT IS (AND ALWAYS HAS BEEN):

- Paper heavy industry
- Multiple parties
- Complex ecosystem
- Duplication & Inefficiency
- Pressure on Costs
- Industry slow to embrace change

SOURCE: https://www.shippo.co.uk/shipping-process/
## CONGENBILL 2016
### BILL OF LADING

To be used with charter parties

---

<table>
<thead>
<tr>
<th>Shipper</th>
<th>Bill of Lading No.</th>
<th>Reference No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consignor</td>
<td>Vessel</td>
<td>Port of loading</td>
</tr>
<tr>
<td>Notify address</td>
<td>Port of discharge</td>
<td></td>
</tr>
</tbody>
</table>

---

**Shipper's description of goods**

_Gross weight_

(of which: on deck at shipper's risk; the carrier is not responsible for loss or damage in transit due to overloading)

<table>
<thead>
<tr>
<th>Freight payable per CHARTER PARTY dated:</th>
<th>SHIPPED at the Port of Loading in apparent good order and condition on the Vessel for carriage to the Port of Discharge or so near thereto as the Vessel may safely get the goods specified above.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight, measure, quality, quantity, condition, contents and value unknown.</td>
<td></td>
</tr>
</tbody>
</table>

**IN WITNESS whereof the Master or Owner or Charterer or Agent of the said vessel has signed the number of Bills of Lading indicated below all of this tenor and date, any one of which being accomplished the others shall be void.**

---

**Conditions of Carriage**

1. All terms and conditions, liberties and exceptions of the Charter Party, dated as above, including the Law and Arbitration Clause/Dispute Resolution Clause, are hereinafter incorporated.

2. **General Parenteral Clause**

   The International Convention for the Uniformity of Certain Rules of Law relating to Bills of Lading signed at Brussels on 23 August 1924 (the Hague Rules) as amended by the Protocol signed at Brussels on 23 February 1950 (the Hague-Visby Rules) and as enacted in the country of shipment shall apply to this Contract. When the Hague-Visby Rules are not enacted in the country of shipment, the corresponding legislation of the country of destination shall apply, irrespective of whether such legislation may only regulate outward shipments.

   When there is no enactment of the Hague-Visby Rules in either the country of shipment or in the country of destination, the Hague Rules as enacted in the country of shipment or if no such enactment is in place, the Hague Rules as enacted in the country of destination apply compulsorily to this Contract.

   The Protocol signed at Brussels on 21 December 1978 (the SDR Protocol 1978) shall apply where the Hague-Visby Rules apply, whether mandatorily or by this Contract.

   The Carrier shall in no case be responsible for loss or damage to cargo arising prior to loading, after discharging, or while the cargo is in the charge of another carrier, or with respect to deck cargo and live animals.

3. **General Average**

   General Average shall be adjusted, stated and settled according to York-Antwerp Rules 2016 in London or another place is agreed in the Charter Party.

   Cargoes contribution to General Average shall be paid to the Carrier even when such average is in the interest of the Master, Pilot or Crew.

4. **New Jason Clause**

   In the event of an accident, damage or disaster before or after the commencement of the voyage, resulting from causes, whether due to negligence or not, for which, or for the consequences of which, the Carrier is not responsible, by statute, contract or otherwise, the cargo, carriage or consignee of the owner of the cargo or any other person or firm, or any of the crew, shall contribute to the Carrier in General Average to the payment of any salvage, loss or expenses of a General Average nature which may be made or incurred and shall pay salvage and special charges incurred in respect of the cargo. A saving vessel or vessel belonging to strangers. Such deposit as the Master or Agent, may deem sufficient to cover the estimated cost of damage incurred in respect of the cargo shall be made to the Carrier by the owner of the cargo, consignee or consignees of the cargo to be delivered in the absence of the Master, Pilot or Crew.

5. **Both-to-Elma Collision Clause**

   If the vessel comes into collision with another vessel as a result of negligence of the other vessel and any act, neglect or default of the Master, Master, Pilot, or the Owners of the vessel in the navigation or the management of the vessel, the Owners of the vessel shall be entitled to contribute in General Average to the payment of any salvage, loss or expenses of a General Average nature which may be made or incurred and shall pay salvage and special charges incurred in respect of the cargo. A saving vessel or vessel belonging to strangers. Such deposit as the Master or Agent, may deem sufficient to cover the estimated cost of damage incurred in respect of the cargo shall be made to the Carrier by the owner of the cargo, consignee or consignees of the cargo to be delivered in the absence of the Master, Pilot or Crew.

6. **International Group of P&I Clubs/BIMCO Mutual Clause for bills of lading and other contracts 2014**

   For the purposes of this contract, the term 'Carrier' includes the owners, managers, operators and agents of vessels (other than the Carrier), including masters, owners of the vessel which the vessel is to load and deliver, who have agreed to perform the contract whether in direct or indirect manner in the Charter or not.

   It is hereby agreed that no Contest shall in any circumstances whatsoever be under any liability whatsoever to the vessel, carriage, receiver, holder, or other party to this contract (hereinafter referred to as 'the Merchant') for any loss, damage or delay of whatsoever kind arising directly or indirectly from any act, neglect or default on the part of the Carrier and no Contest shall be held liable for any loss, damage or delay of whatsoever kind arising directly or indirectly from any act, neglect or default on the part of the Carrier for any loss, damage or delay of whatsoever kind arising directly or indirectly from any act, neglect or default on the part of the Carrier.

   Without prejudice to the generality of the foregoing provisions in this clause, every exemption, limitation, condition and liability contained herein (other than Art III Rule 6 of the Hague-Visby Rules (as interpreted herein) and every right, exemption from liability, defense and immunity of whatsoever nature applicable to the carrier or to which the carrier is entitled hereunder including the right to arbitration or jurisdiction or provision contained herein shall also be and shall at all times be construed and interpreted so as not to detract from the rights of the carrier and the ship under this clause nor to affect the rights of the carrier under any other provisions of this clause.

   The Merchant undertakes that no claim or allegation whether arising in contract, bailment, tort or otherwise shall be made against or on behalf of any servant or representative of the carrier which imposes or attempts to impose upon any of them any liability whatsoever in connection with this contract whether or not arising out of negligence on the part of such servant or representative. The carrier shall be entitled to enforce the foregoing against the Merchant and against any servant or representative of the carrier.

   In the event of any such claim or allegation or damage or delay of whatsoever kind arising directly or indirectly from any act, neglect or default of the Carrier, the carrier shall be entitled to pursue the same against the Merchant.

   The Merchant undertakes that if any such claim or allegation should nevertheless be made, it will indemnify the carrier against all consequences thereof.

   For the purpose of sub-paragraphs (a)–(c) of this clause the Carrier shall be deemed to be acting as agent or trustee on behalf of and for the benefit of all persons mentioned in sub-(a)–(c) above who are its servants and all such persons shall to the extent to be or to be deemed to be parties to this contract.

---

**Signature:**

_Master|Agent|Owner|Charterer_

_(Delete as appropriate)_

If signed by an Agent indicate with a tick ☑ whether for and on behalf of:

- [ ] Master,
- [ ] Owner,
- [ ] Charterer

Source: www.bimco.org
ROLE OF THE BILL OF LADING

• **Original** bill of lading to **sell** cargo

• **Original** bill of lading to **finance** purchase of cargo by Letters of Credit

• **Original** bill of lading to **receive** cargo at discharge port

• Sent by courier **separately** from the ship
1. CURRENT POSITION

2. DIFFICULTIES

3. SOLUTIONS
DIFFICULTIES ARISE FROM...

- Multiple stakeholders
- Documents
- Trust
- The costs of trade documentation processing and administration are estimated to be up to one-fifth of the actual transportation costs.

SOURCE: https://www.ibm.com/blockchain
1. CURRENT POSITION

2. DIFFICULTIES

3. SOLUTIONS
THE MAERSK / IBM LOGISTICS PROJECT:
SHIPPING A CONSIGNMENT OF FRESH FLOWERS

Stakeholders/ Participants in the Blockchain:

1. Seller’s Bank
2. Kenyan Flower grower
3. Freight Forwarder
4. Export Authorities in Kenya
5. Port of Mombasa
6. Port of Rotterdam
7. Dutch Customs
8. Flower market
9. Buyer’s Bank

Distributed database with single interface for documents and real time information visible to all stakeholders
SMART CONTRACTS & ‘SMART’ BILLS OF LADING

- Blockchain removes reliance on central system
- Transact directly
- All have a copy

- Stores rules for negotiating terms
- Automatically verifies
- Executes when conditions met

SOURCE: https://youtu.be/FkeLDPZ-v8g
ACCOUNTABILITY & SECURITY

- **Chronological storage**
- **Audit trail**
- **Changes** can be detected and prevented

- **System continues** despite failure of any party
- **No loss** of data or integrity

SOURCE: https://youtu.be/FkeLDPZ-v8g
VALUE

• Creates a single large secure computer
• Removes risk
• Reduces costs
• No middle man
• No need to trust a 3rd party
• Automatically executed & enforced

SOURCE: https://youtu.be/FkeLDPZ-v8g
ANY QUESTIONS?