P.R.I.M.E. Finance

Panel of **R**ecognized **I**nternational **M**arket **E**xperts in **F**inance

BLOCKCHAIN / SMART CONTRACT & ICO

P.R.I.M.E. FINANCE
Panel of Recognised International Market Experts in Finance

HUBERT DE VAUPLANE

P.R.I.M.E. Finance Annual Conference 2018

22 & 23 January, Peace Palace, The Hague

SUMMARY

WHAT IS BLOCKCHAIN ?

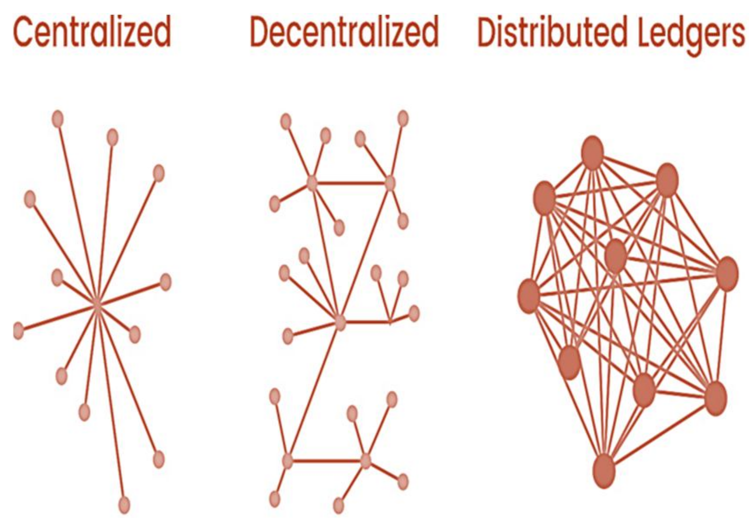
WHAT IS BLOCKCHAIN ?

Blockchain combines the **openness of the internet** with the **security of cryptography** to give everyone a **faster, safer way to verify key information and establish trust**

A **Distributed** and verifiable datastore

A network of computers having an **identical copy of the database** and **changing its state** (records) by a **common agreement** based on pure **mathematics**

- No central server
- No agent to trust
- Operation **based solely on the network**



WHAT IS BLOCKCHAIN ?

Base of **cryptocurrencies** :

BITCOIN ?

- has been dominant in the cryptocurrency field for a long time
- Launched with the intention to **bypass government regulations** and create online payments **without the need of intermediary to confirm transactions**

ETHEREUM ?

- much **greater possibilities**
- introduced the “**smart contracts**” and a way to perform actions by the rules defined in the contract

WHAT IS BLOCKCHAIN ?

HOW DOESIT WORK ?

- Each transaction in the Blockchain is signed **by the rightful owner** of the resource being traded in the transaction & when new resources are created they are assigned to an owner.
- This owner can prepare new transactions that send those resources to others by **simply embedding the new owner's public key in the transaction** and then signing the transaction with his or her private-key.
- To **prevent the double-spending problem**, Blockchain use the "**proof-of-work**".
- he proof-of-work is a **procedure** that establishes **a cost** for grouping transactions in a certain order and adding them to the Blockchain = "blocks"

WHAT IS “SMART CONTRACT” ?

WHAT IS “SMART CONTRACT” ?

Many **competing conceptions** of what a smart contract is.

Smart legal contracts:

- Resonates most with lawyers;
- This is where the term smart contract is used **to refer to legal contracts, or elements of legal contracts**, being represented and executed by software.

Smart contract code:

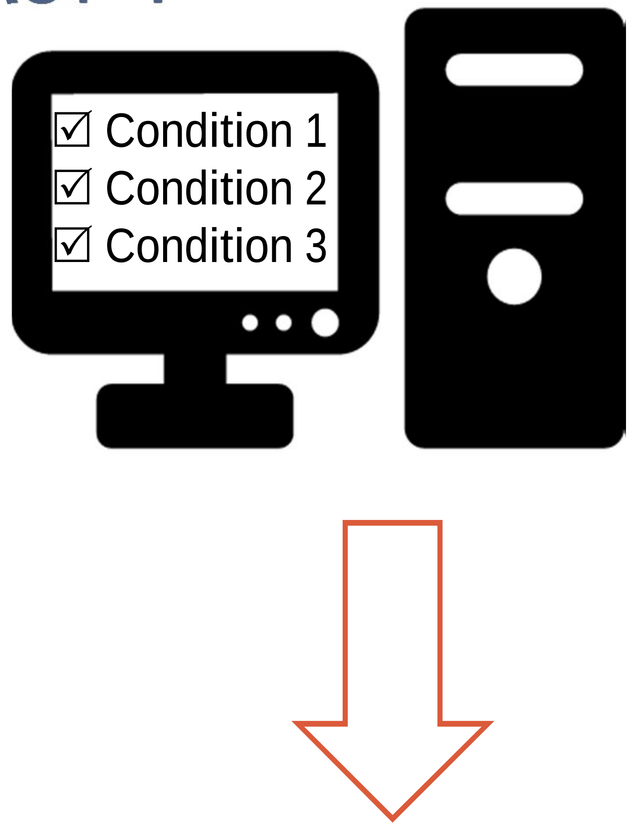
- Relates **less to contracts as a lawyer**
- Relates to a **piece of code** that is designed to **execute certain tasks if pre-defined conditions** are met. Such tasks are often embedded within, and performed on, a distributed ledger.

As a result, every smart legal contract can be said to contain one or more pieces of smart contract code, but not every piece of smart contract code comprises a smart legal contract.

WHAT IS "SMART CONTRACT" ?

HOW DOES IT WORK ?

- transactions **trust free**
- They are **computer protocols** that are **verifying** and **enforce** the **performance** of a contract
- Smart contracts are self-governing and self-performing and through this makes any trust in **any contracting party unnecessary**
- Smart contracts are **self-executing contracts** with the terms of the contract directly **written into lines of code** = if required conditions are met, certain actions are executed
- A smart contract is stored in the blockchain network

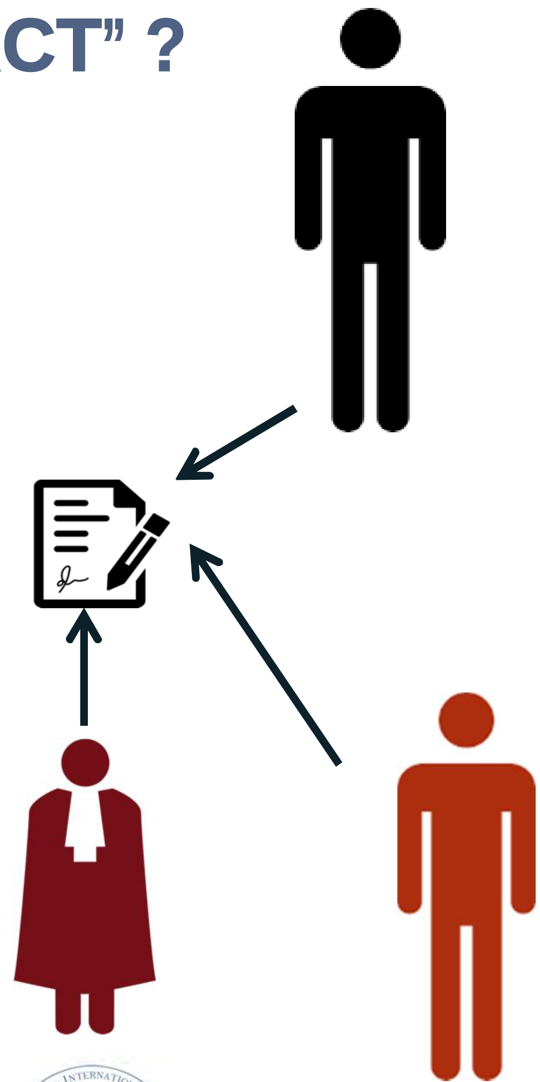


Automatic transfer of payment to the seller

WHAT IS "SMART CONTRACT" ?

<u>EXAMPLE</u> : YOU WANT TO SHIP A PALLET OF GOODS TO YOUR FRIEND BOB.

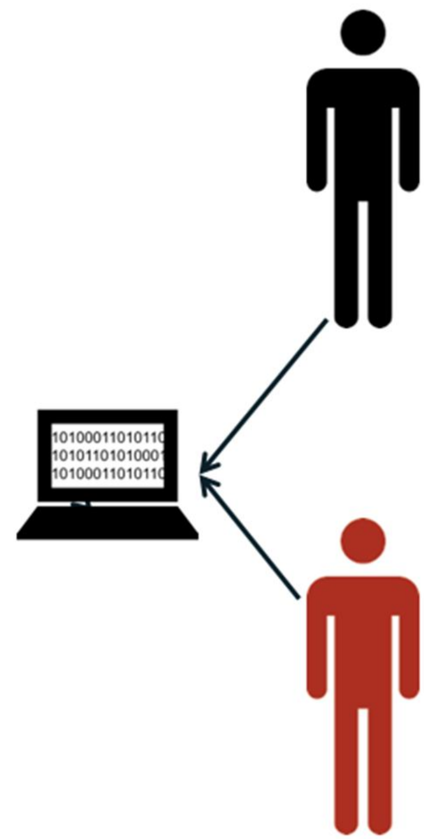
- will carry your pallet
- Tom does **not trust you** as well (maybe you won't pay him)
- Therefore, you **have to sign an agreement with Tom** that you will pay for the shipment in a few days after delivery
- Usually **third party is involved in this process**, legal papers, contracts are scanned, printed, signed



WHAT IS “SMART CONTRACT” ?

<u>EXAMPLE</u> : YOU WANT TO SHIP A PALLET OF GOODS TO YOUR FRIEND BOB.

- With the help of smart contracts we could **define those rules in code** = You make a payment for shipment to smart contract on a day of loading
- It holds payment till shipment delivery is confirmed by Bob
- Then smart contract **releases the payment** and **money is transferred to Tom <u>automatically</u>**
- *if we would have a GPS tracker attached to the pallet then we simply could eliminate Bob from this process and just release the payment automatically, when the location rule is met*



WHAT IS “SMART CONTRACT” ?

BENEFITS:

For a wide range of potential applications, Blockchain-based smart contracts could offer a number of benefits:

- **Speed and real-time updates**. Because smart contracts use software code to automate tasks that are typically accomplished through manual means, they can increase the speed of a wide variety of business processes.
- **Accuracy.** Automated transactions are not only faster, but less prone to manual error.
- **Lower execution risk**. The decentralized process of execution virtually eliminates the risk of manipulation, nonperformance, or errors, since execution is managed automatically by the network rather than an individual party.
- **Fewer intermediaries**. Smart contracts can reduce or eliminate reliance on third-party intermediaries that provide “trust” services such as escrow between counterparties.
- **Lower cost**. New processes enabled by smart contracts require less human intervention and fewer intermediaries and will therefore, reduce costs.
- **New business or operational models**. Because smart contracts provide a low-cost way of ensuring that the transactions are reliably performed as agreed upon, they will enable new kinds of businesses, from peer-to-peer renewable energy trading to automated access to vehicles and storage units.

WHAT IS “SMART CONTRACT” ?

STILL MANY QUESTIONS::

- Will it be possible to capture all the elements of a ‘traditional’ contract in a set of computer-coded instructions?
- How will coders capture concepts and principles that require a degree of subjectivity or judgement on a case-by-case basis?
- How about capturing a non-exhaustive list of circumstances, such as force majeure events?
- Even if that is possible, how will smart contracts cope with events that occur outside their underlying code (in the ‘real world’)?
- If, for example, circumstances arise that would frustrate a contract or make its performance illegal or even contrary to business common sense, is it possible to hardwire that into the code of the smart contract, so that it does not automatically perform itself in those circumstances?

P.R.I.M.E. FINANCE
Panel of Recognised International Market Experts in Finance

WHAT IS "SMART CONTRACT" ?

DERIVATIVES MARKETS AND SMART CONTRACT:

- Publication of a paper concerning the use of smart contract in derivatives markets by ISDA with Linklaters;
- ISDA indicates in its website that smart contracts have the **potential to unlock value in the derivatives market by offering significant cost and efficiency benefits**;
- A not straightforward translation of ISDA documentation into a smart contract context: while certain operational clauses – those related to payments or deliveries, for instance – might lend themselves to being automated, **others are more subjective or require interpretation or discretion, and will therefore prove more challenging**.
- To lead these developments, a new ISDA legal working group has been set up specifically to focus on smart contracts and distributed ledger.
- This is in addition to another ISDA initiative to establish the common data and process standards to help drive interoperability of these new technologies.

CONFLICT OF LAWS IN BLOCKCHAIN

CONFLICT OF LAWS IN BLOCKCHAIN

BLOCKCHAIN AND RIGHT OF OWNERSHIP:

- the question posed by the Blockchain is to consider whether it is **only a piece of evidence of a legal act or fact**, or if it constitutes **the legal act or fact itself**
- Ownership is most often described by law as materialising a direct legal relationship between a good (a right) and a subject of law, while possession reflects a factual relationship between these same entities
- **Limits** of this classic approach when it comes to the Blockchain:
    - o the elements recorded in the Blockchain constitute real rights or personal rights;
    - o the proof of the right, does not lie in a register but in all registers at the same time
- The distributed register differs from traditional registers only by the fact that it is **distributed**: there are a **multitude of registers all having the same "probative value“**
- what is "shared" is the public key : the possession of a good (or a right) registered in the blockchain **requires the combination of the public key and of a private key** . The private key remains in the possession of its holder, and is not distributed (or shared) between several blocks.

CONFLICT OF LAWS IN BLOCKCHAIN

PRIVATE KEY:

- What holds the jurist's attention here is that the private key, to retain its entire security dimension, must only/can only be in the possession of its sole owner = **If the private key is lost or stolen, the property registered in the blockchain are lost forever.**
- a **relationship between the possession of the private key and the owner of the digital assets** (bitcoins, or others) **recorded in the blockchain**.
- the possession of the private key is a **physical, palpable, material element**: this private key is stored in a computer, on a USB medium, in a wallet or elsewhere, but it is "somewhere".
- the right (of a claim or ownership) that constitutes a registration in the blockchain is **divided in two**:
    - o on the one hand **in the public** key, that is to say in the internet network and its various servers; and
    - o on the other hand **in the private key**, which is a physical object.
- A partially "embedded" right in a physical object and at the same time in the internet network.

PRIVATE KEY

PUBLIC KEY

CONFLICT OF LAWS IN BLOCKCHAIN

WHAT CONFLICT OF LAWS RULES SHOULD APPLY FOR SECURITIES RECORDED IN A BLOCKCHAIN?

Analyze through the case of "**intermediated securities**";

- the Blockchain technology is able to attribute an asset to a user without the need for intermediation;
- The "thing" is represented by a **unique piece of code.** The value of this piece of code can be freely determined;
- **absence of an account** & **absence of intermediaries** or account providers = "intermediated securities holding";

CONFLICT OF LAWS IN BLOCKCHAIN

THE CONFLICT OF LAW ISSUE IN THE BLOCKCHAIN:

Harmonised conflict of laws rules :

- **Settlement Finality Directive** in relation to book entry securities provided as collateral to participants of settlement systems, ECB or central bank from Member States;
- **Financial Collateral Directive** in relation to book entry securities provided under financial arrangements;
- **Winding up directive** concerning the enforcement of proprietary rights in book-entry securities in insolvency proceedings of credit institutions and investments firms.

↳ based on a similar approach: the PRIMA concept defined in the Hague Convention

↳ can be summarised as a register, an account, or a centralised deposit system.

↳ However, the concepts of "register" or "account" are not defined or are poorly defined.

↳ These conflict of law rules do not specify where the account/register, centralised deposit system is "located" or "maintained".

CONFLICT OF LAWS IN BLOCKCHAIN

CONNECTING FACTORS:

- **First: the entry point to the chain:** the more pragmatic answer and factual factor but this approach will not create legal certainty;
- **Second: the law of the issuer of the securities** (*lex societatis*): create significant legal uncertainty as the applicable law will be multiple in the case of an international portfolio in the electronic vault;
- **Third: The the law of the jurisdiction where the system (the blockchain) is located or supervised** (*lex systematis*): it should work for a private (or permissioned) Blockchain, it seems to have no sense in a public chain like Bitcoin or Ethereum;
- **Fourth: the location of the private key** (*lex rei sitae*): the place of custody of the private key will be considered as the connecting factor to determine the law applicable to the transaction in the blockchain. The problem, lies in the fact that third parties do not know this place of detention or can change at any time (if the private key is kept in the form of a USB key or in a laptop);

So whart ? there is **no satisfactory answer** to determine the connecting factor to the applicable law.

P.R.I.M.E. FINANCE
Panel of Recognised International Market Experts in Finance

CONFLICT OF LAWS IN BLOCKCHAIN

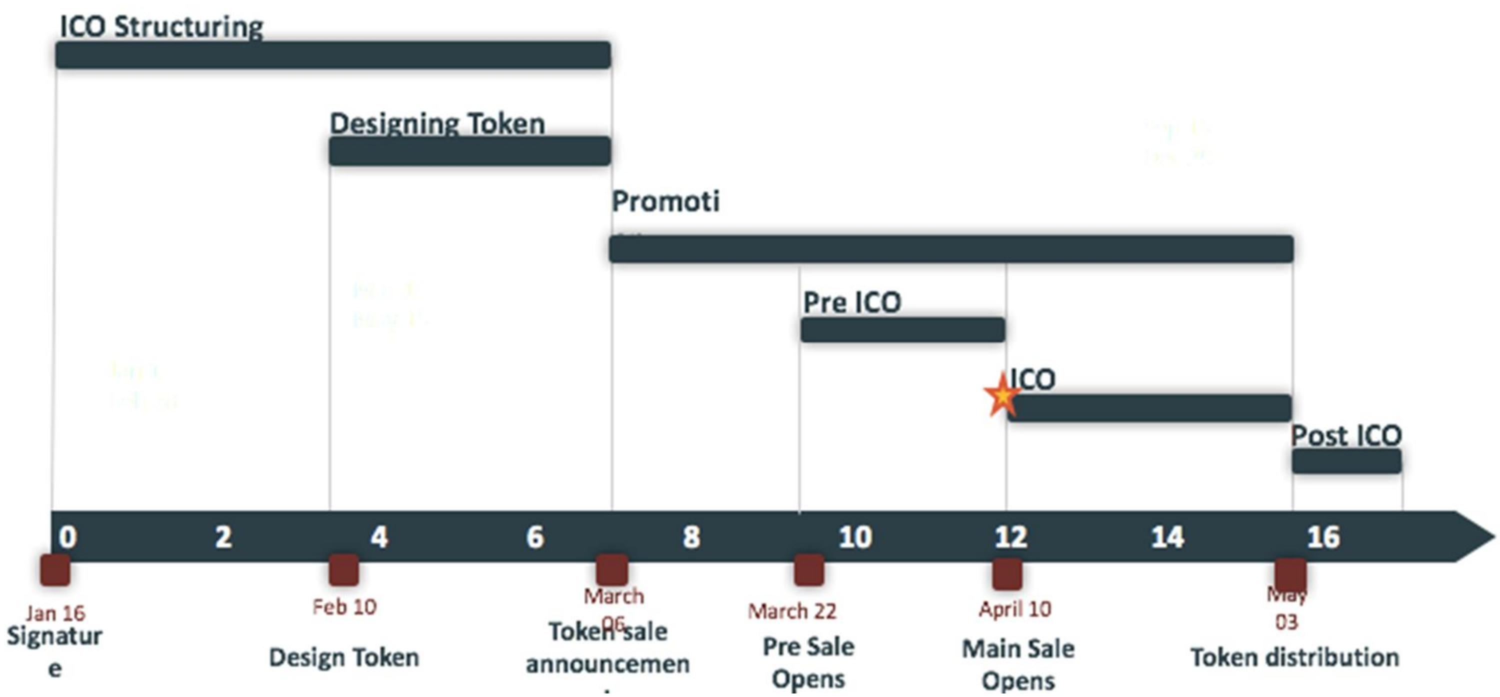
WHAT CAN BE CONCLUDED?

- Regarding securities circulating in the blockchain, there is **no satisfactory answer to determine the law applicable to transactions**.
- It is essential in the event of the development of these transactions via a public blockchain to define in a **separate deed the legal regime of the transfer of ownership of the securities sold in this blockchain**.

WHAT ARE LEGAL ISSUES IN ICO ?

WHAT ARE LEGAL ISSUES IN ICO ?

Initial Coin Offerings (ICOs), also known as "token sale" or "token generating event", refers to the operations by which organizations **sell digital tokens to finance their development**.



WHAT ARE LEGAL ISSUES IN ICO ?

- Tokens are usually bought in **cryptocurrency** (bitcoin, ether, etc.)

- Tokens are **the digital representation of a set of rights**. The rights represented by the token can be varied:
  - **utility** token, Token that can be exchanged for **goods or services**
  - **equity** token, token representing rights to a **share of profits or voting rights**
  - **community** token, Token that can be **exchanged** within a community
  - **asset** token, token **secured by an asset**

P.R.I.M.E. FINANCE
Panel of Recognised International Market Experts in Finance

WHAT ARE LEGAL ISSUES IN ICO ?

WHAT ABOUT THE QUALIFICATION OF TOKENS?

- The analysis of tokens in civil law makes it possible to retain two potential qualifications:
  - Assets
  - Intangible assets
- In addition, according to their structure and their utilities, tokens are likely to receive legal qualifications under various special rights:
  - Distance Selling of goods or serices
  - Financial securities
  - Payment Services
  - Investment Funds
  - Derivatives

WHAT ARE LEGAL ISSUES IN ICO ?

SECURITIES AND EXCHANGE COMMISSION, DECEMBER 11, 2017, RELEASE NO. 10445

- SEC has **clarified the situation for utility token** as such Munchee

- *"Munchee offered MUN tokens in order to raise capital to build a profitable enterprise,"* [...] *"Munchee said that it would be used for the development of its business, including hiring people to develop its product, promoting the Munchee App, and ensuring the smooth operation of the MUN token ecosystem"*

- In the US any ICO must be structured as Security offering with a SAFT contract and comply with US Security law = **investors must be registered for the Pre ICO**.

CONTACT

Hubert De Vauplane

Associé, Avocat au Barreau de Paris

T +33 (0)1 44 09 46 80 **F** +33 (0)1 44 09 46 01

M +33 (0)6 80 11 74 82

hdevauplane@kramerlevin.com

Kramer Levin Naftalis & Frankel LLP
47 avenue Hoche
75008 Paris