Blockchain and IP law

WIPO Blockchain Workshop | Dr Birgit Clark
Confused by jargon?
Replacing the intermediary

Situation: Amy needs to send money to Bob

**TRADITIONAL APPROACH**

Amy → Amy's Bank → Bob's Bank → Bob

**BLOCKCHAIN APPROACH**

Amy → BLOCKCHAIN → Bob
How a blockchain transaction works

- *User* and *recipient* wish to conduct a transaction (i.e. send data, cryptocurrency, contract, etc.)
- Cryptographic keys assigned to User and Recipient
- Transaction is "broadcast" to and "verified" by a decentralised P2P network ("nodes"); using algorithms
- "Miners" in the network "validate" the transaction
- Creation of a new date stamped block ("proof of work")
- Network balances updated
- New block added to the blockchain
- (Arguably) immutable and transparent record of transaction
- Cryptographic signature assigned
- Transaction complete
Models

Model 1
Previous systems
A centralised system

Model 2
Public blockchain (permissionless)
An open network that anybody can access. The digital ledger of transactions is shared, transparent and run by all participants.

Model 3
Private blockchain (permissioned)
The preferred option of most regulated entities. It is a private system which controls access to certain invited participants.
Use cases

Applications across industries

- Financial Services
- Pharma
- Creative services
- Public sector
- Retail
- EMI
- Real Estate

Nature

- Payments
- Reconciliation
- Securities
- Supply chain
- Record keeping
- Asset management
- Digital identity
- Compliance
- Smart contracts
Blockchain and IP Law: A Match made in Crypto Heaven?
Applications in IP

- Patents
- Trade Secrets
- Smart IP Rights and Registries
- Evidence of Use
- Traceability
- Certification
- Trade marks
- Evidence of Creatorship
- Supply Chain Tracking
- Provenance Authentication
- Smart Contracts
- IP Enforcement
- Anti-counterfeiting
- Digital Rights Management

Evidence of Use
"Smart" IP rights and registries

- Centralized solution - run by the IP office as an accountable authority?
- One global IP registry – a myth?
- Replacing or supplementing the traditional IP register databases
- Robust and trustworthy proof of events in the life of a registered IP right
- Saving time, resources and money
- Simplifying IP audits and due diligence
- Licensing, assignments, chain of title…

- Issue of confidential data ← → Open or private blockchain
Evidence of use

Evidence of use of a trade mark (e.g. evidence of acquired distinctiveness/secondary meaning; defending non-use revocations; renewal; incontestability, etc.)

Data updated and notified to smart IP Registry virtually immediately on the occurrence of a verified event

Lower the burden of cost and administration collecting relevant evidence

Issues: confidentiality of sensitive business data (private vs public blockchain); interoperability of blockchain solutions
Certification and collective marks

Collective marks: for use by a specific group of enterprises, e.g. members of an association

Certification marks: for use by anybody who complies with the standards defined by the owner (i.e. products meet certain established criteria or standards, e.g. Woolmark)

Fake certificates can almost immediately be identified

Entity that applies for registration is considered "competent to certify" the products

Issue for both: public nature of traditional open blockchain;
Evidence of creatorship

Enforcement of unregistered IP rights ("bridge the gap"): difficulties of proving ownership of unregistered trade marks, unregistered designs, goodwill, copyright

Evidence of conception, use, status, qualification requirements (such as originality and the country in which articles made to design were first marketed)

Original design document and details of designer on blockchain create timestamped record and evidence

Deterrent for infringers

"Pioneer" platforms

Cf. authentication of "storytelling" products
China – ahead of the game

We should not reject or impose higher standards simply because it involves new technology… Provided that the technical verification is consistent and other evidence can be mutually verified, such electronic data can be used as evidence for the infringement in the (copyright) case

https://mp.weixin.qq.com/s/W4HhYfwM8JUtBIWpQi2kqQ

China’s Supreme People's Court: evidence stored and verified on blockchain platforms may be used in legal disputes heard by the three internet courts in Hangzhou, Beijing, and Guangzhou (cf. notorisation by public notary)
Smart Contracts and DRM

Smart contracts

No universal definition

Programmable transactions — computerised transaction protocols that recognise fulfilment of conditions and automatically execute terms of a contract (cf. "Oracles")

Digital Rights Management: (micro-)payments to IP owners in real time

Delay in payments issue
Anti-counterfeiting and enforcement

Scannable tags or chips immutable information (cf. QR codes and NFC tags)

If genuine products are embedded with original tag, then its absence or incorrect/duplicate data will be an easy way for customs to check whether a product is counterfeit

Educate and involve customs and customers

Rethinking customs programs to prevent global trade in counterfeits

Eliminating fakes

Provenance Authentication

Engaging customers in the process of verifying whether a product is genuine – won't change attitude of those that intentionally buy fakes?
Supply Chain and Traceability

Fragmented supply chains, parallel imports, grey goods, selective distribution networks

Legal traceability requirements (e.g. Falsified Medicines Directive (FMD), US Drug Supply Chain Security Act (DSCSA))

Tracking the movements of a physical product, where it was placed on the market, shipped etc.

Example:

monitoring the authenticity of ingredients during all stages of production: raw material sourcing, manufacturing of the active pharmaceutical ingredients and the manufacturing of the final products
## Tracking Goods in the Supply Chain

<table>
<thead>
<tr>
<th>Why (private) blockchain?</th>
<th>How does it work?</th>
<th>Remaining problems:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain a secure record of the entire supply chain</td>
<td>At each step, all parties verify the existence and conditions of goods</td>
<td>Every party at every step must be involved</td>
</tr>
<tr>
<td>Information on when and where a product is made, processed, shipped, storage conditions etc.</td>
<td>Information is digitally linked to goods</td>
<td>Differences between &quot;real world&quot; and digital world</td>
</tr>
<tr>
<td>Speed up administration</td>
<td></td>
<td>Who pays and what will incentivise everyone to play their part?</td>
</tr>
<tr>
<td>Valuable supply chain information not visible to competitors</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Trade Secrets

Increasingly common for businesses (especially SMEs) to protect their inventions as trade secrets

Alternative to innovation patents

Definition:
information which is (i) secret, (ii) has commercial value and which (iii) has been subject to reasonable steps to keep it secret (cf. Article 39 TRIPS, US Defend Trade Secrets Act 2016, EU Trade Secrets Directive,) – only valuable to the extent they are kept secret;

Proof that information has been kept secret in case of misappropriation (encryption, hashing, proof of existence)

Means of securely sharing information with third parties

Blockchain as secure means of sharing trade secrets: "smart NDAs"

Untested in courts
Who owns blockchain?

- Patents
- Open source approach
- Hybrid approaches
- Trade marks
- Copyright
- Trade secrets
- Selecting and managing relationships with providers
- Contractual considerations
Will blockchain live up to the hype?

HURDLES TO LARGE SCALE APPLICATION

1. High cost per transaction
2. Time delay
3. High energy usage
4. Compatibility and standards
5. Public’s confidence in technology and participants
6. Anti-trust / privacy concerns

But solutions are being developed
- Addressing bandwidth issues by reducing computing power required by each user computer / node
- Addressing storage issues by using hybrid models, in which not all data is stored on the blockchain (storing less significant data "off chain")
Relevant tracking applications: examples

01 **Provenance: "Everledger"**
- Verify origins and ownership of diamonds
- Number on diamond / features of diamond and ownership on a blockchain

02 **Marketing / consumer engagement: "Babyghost"**
- RFID tags in clothing interact with blockchain
- Allowed clothes to 'tell their own story' – those scanning tag could access details about the design
- Possible application in sustainability messaging, promotions, authenticity checks
- RFID / QR Code technology also developing fast

https://www.youtube.com/watch?v=GAdjL-nultl
**Relevant Tracking Applications**

03 **Anti-counterfeiting**
- Interaction with RFID tags / other identifiers in physical world
- Potentially help identification by customs
- Benefit of a global solution

04 **Parallel trade**
- Identify where diversions out of legitimate supply chain occur
- Trace origin of products
- Consumer trust / reliance on warranties etc
Questions