ITU Workshop on "Combating Counterfeit Using Conformance and Interoperability Solutions"

Geneva, Switzerland

28 June 2016

Blockchain to Combat Counterfeit Products

Dr. Adrian McCullagh PhD (IT Sec), LLB (Hons)
ODMOB Lawyers
ajmccullagh57@gmail.com

Professor John Flood PhD (Sociology), LLB, LLM
Director of the Law Futures Centre
Griffith University
j.flood@griffith.edu.au

1956 2016 CCITT / ITU-T

ODMOB LAWYERS

Griffith UNIVERSITY

ITU

Agenda

- What is the Blockchain?
- Advantages of the Blockchain
- Blockchain Disadvantages
- Blockchain: Disruptive Technology against Counterfeiters
- Future Research
- Conclusion

Blockchain: The Genesis Thesis

A blockchain is basically a distributed ledger (multiple copies of the same thing) that has the following characteristics:

- Once a transaction is recorded in the blockchain it cannot be deleted or edited without leaving some trace of such deletion or alteration. It becomes in effect a permanent record for eternity
- Any attempted changes to the record will automatically be identified which will cause all parties to investigate what has gone wrong
- In essence, the blockchain becomes a tamper evident record of transactions (immutable)

Blockchain: No Single Point of Failure

- No central party will necessarily control the blockchain; BUT some private blockchains that are being developed will be controlled by a central authority
- Being a distributed ledger, a number of copies will be established which makes it difficult for unauthorised third parties to successfully hack every copy of the ledger
- Therefore, there is no single point of failure. It would require a hacker to simultaneously attack at least 51% of all copies which is just not feasible

Blockchain: Access Control

- Blockchain can be designed as a permissioned blockchain or as a permissionless blockchain (Bitcoin)
- Permissioned blockchains will only allow authorised persons the right to read and add to the blockchain and R3CEV is an example
- Further, with a permissioned blockchain it is possible to allow everyone access to read the blockchain but only a few to add to the blockchain

Blockchain Advantages

The blockchain has the following advantages:

- reliable and available to all participants
- transparent as all participants have read access
- immutable integrity is guaranteed
- deployed in non-face-to-face transactions
- time reduction between the transaction start and settlement
- covers any type of asset (intangible and tangible), not just bitcoin, e.g. diamonds, land, and securities
- reduces friction costs by disintermediating third party involvement

Blockchain Disadvantages

- Blockchains require a software application layered on top to achieve any benefit
- Sir Mark Walport, UK Chief Scientist, says: “the implementation of distributive ledgers with embedded smart contracts should lead to substantial improvements in compliance, cost efficiency and accountability”
- Carefully structured applications can disrupt counterfeiters in the market place

Disruptive Technology Against Counterfeiters

- Having an immutable record of manufacture for a product is only a partial solution
- Instead of preventing counterfeiters producing a product, the blockchain can disrupt their market by arming the user with tools to authenticate their acquired product

Blockchain: Disruptive Scheme

- Each product will need to be marked with a tamper-proof mark which can be scanned by a hand-held device
- The number of smartphone users is forecast to grow from 1.5 billion in 2014 to around **2.5 billion** in 2019, with increased smartphone penetration rates as well
- Smartphones are ideal mobile devices to assist in disrupting the counterfeiter

Blockchain: Disruptive Scheme (cont.)

- QR codes are ideal tamper-evident marks
- QR codes are coded with unique reference codes which are the hash of the following information:
  - Manufacturer details
  - Product details
  - Serial number of the product
  - Manufacture date

Blockchain: Disruptive Scheme (cont.)

- Users will download an authorised smartphone application (**Authentication App**) from the manufacturer's site that has been enhanced with extended validation certificates for SSL communications
- Authentication Apps have specific and restricted/limited functionality

Functionality: Authentication App

- Authentication App functionality:
  - It will read embedded QR codes on the user's device which will be a unique hash code
  - It will only be directed to a specific IP address
  - It will cause the blockchain to be interrogated to deliver the information validating the product in question
- Manufacturer's system will undertake a challenge response to allow the Authentication App access

Blockchain: Authentication App Protocol

The proposed high level protocol is as follows:

- Each manufacturer will register the public key embedded in an X509 v3 certificate that corresponds to their software signing private key with each reputable browser manufacturer
- The Authentication App will be validated through the X509 Cert within the browser

Blockchain: New Protocol Development

- The high level protocol will require counterfeiters to infiltrate every user's smartphone in order to fool the system
- The above is not a fool-proof solution as counterfeiters will try to spoof the manufacturer's website to fool users into downloading false authentication apps
- New security protocols should be investigated to reduce the risk of spoofing attacks

Blockchain: Double Substitution Requirements

- The security of QR codes on each product must be embedded/impressed so they cannot be substituted
- Even if there is a substitution, it will result in failure as the true Authentication App will only interrogate the true blockchain
- In other words, the counterfeiter needs to perform a double substitution to be successful
- It gives more control to the user in authenticating each product as it is received and can be applied to multiple commercial industry sectors including high valued products and pharmaceuticals

Future Research

- The rapid growth globally of the Internet of Things will also need to be investigated, especially where such physical items are connected to a smart contract that is operating on a blockchain
- How the data flows from these items will necessitate appropriate management and regulation
- A series of decentralised autonomous organisations (DAO) could run the process without human intervention
- How the law will deal with the DAO remains outstanding

Future Research (cont)

- The use of smart contracts will need investigation especially from a multi-jurisdiction perspective
- The general proposal for smart contracts is that they will operative purely within a cyber-environment and thus without borders
- There are social and regulatory challenges to these developments, so to what extent will users need to be aware of blockchain/smart contract/DAO activity?
- What entities will be regulated? By whom? Who is the consumer of a DAO? What would be the nature of a DAO? What would the sanctions be for misfeasance?

Future Research (cont)

- Are there competition issues if DAOs/blockchains collaborate with each other?
- How do we educate/train the future generations of professionals for this work? Do we need to establish micro-credentialing via blockchain to do this?

Conclusion

- A private blockchain could greatly assist in reducing the available market for counterfeit products
- The system will allow users to identify in absolute terms whether a product is authentic
- Instead of concentrating on the counterfeiter per se this system concentrates on the user which should obviate the marketability of counterfeit products
- New protocols should be investigated so that a counterfeiter cannot fraudulently impersonate a manufacturer with the downloading of a false Authentication App

Conclusion

- Users must be guaranteed that they only use true Authentication Apps
- This use of the blockchain gives power to the user by allowing them to ensure that what they are paying for is authentic product and not counterfeit product
- That is value for money

?????????

?? ANY QUESTIONS ??

?????????

Dr. Adrian McCullagh & Professor John Flood

Disclaimer

- ***PLEASE NOTE:*** *the information disclosed in the presentation* ***is NOT*** *the provision of* ***Legal advice or Professional Services advice****. If a reader/attendee has an issue then they should seek appropriate legal/technical advice. The author/presenter makes no warranty as to correctness of anything contained in this presentation. The topic of this presentation is ever changing at a rapid rate and as such this presentation is the sole opinion of the author/presenter and must not be relied upon as either legal or technical advice. Every situation is different and as such proper analysis must be undertaken when seeking professional advice.*
- *Consequently, the author/presenter takes no responsibility for any errors that may exist in this paper and certainly takes no responsibility if any reader/attendee takes any actions based on what is (expressly or by implication) contained in this paper/presentation.*
- *All readers/attendees take full responsibility for anything they may do in reliance of anything contained in this paper/presentation.*