



PROGRAM MATERIALS

Program #2909

January 11, 2019

Blockchain for Lawyers 101

**Copyright ©2019 by Jason Haislmeier, Esq., Bryan Cave
LLP. All Rights Reserved.
Licensed to Celesq®, Inc.**

Celesq® AttorneysEd Center

www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487

Phone 561-241-1919 Fax 561-241-1969



Blockchain 101

(for lawyers)

January 11, 2019

Jason Haislmaier

Blockchain

What is it?

How does it work?

How is it being used?

What (legal) issues does it raise?

What is it?

NISTIR 8202

Blockchain Technology Overview

Dylan Yaga
Peter Mell
Nik Roby
Karen Scarfone

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8202>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8202

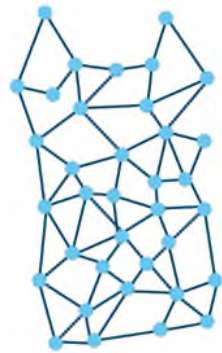
Blockchain Technology Overview

“The use of blockchain technology is still in its early stages, but it is built on widely understood and sound cryptographic principles.”

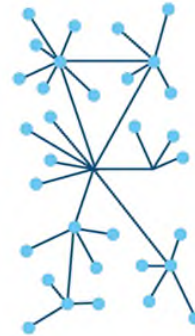
“Currently, there is a lot of hype around the technology, and many proposed uses for it. Moving forward, it is likely that the hype will die down, and blockchain technology will become just another tool that can be used.”

“Distributed Shared Ledger” Technology

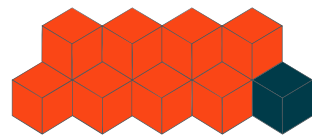
“Distributed Trust” Technology



Distributed



Decentralized



Immutable

Transparent

Platform Technology

Software-implemented Peer-to-peer Network

“The Cloud”
(circa 2010)

I'm not sure my goal for today is going to be to actually explain it to you, but I do want to make sure that people understand that I think everybody in our industry accepts it's the next major transition point in terms of how IT gets done.

Steve Ballmer

Former CEO, Microsoft

Describing “the cloud” as a 2010
Microsoft event in Singapore

Benefits

Security

Cost

Performance

Integrity

Risk

Scalability

Auditability

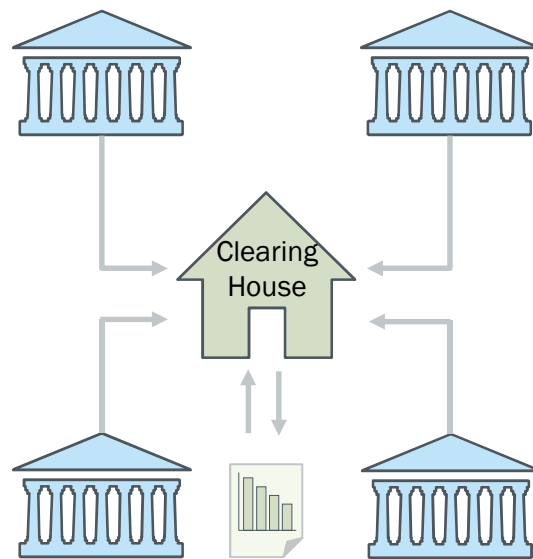
How does it work?

**Shared Ledger
Decentralized
Distributed
Transparent
Immutable
Encrypted**

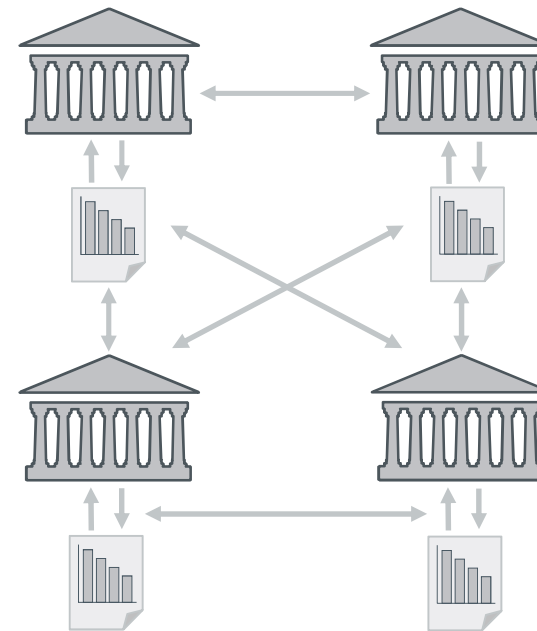
Shared Ledger



Decentralized



Centralized

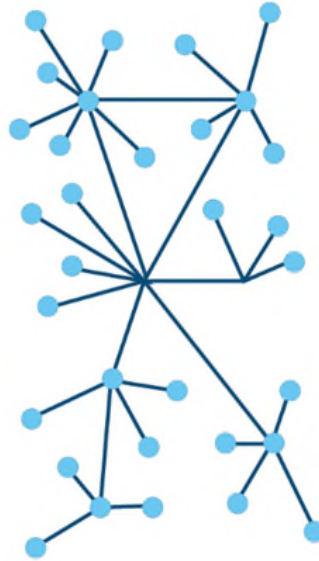


Distributed

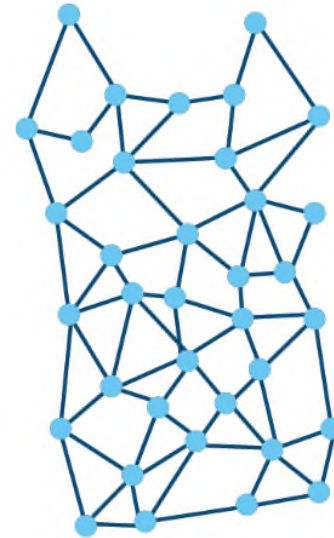
Distributed



Centralized



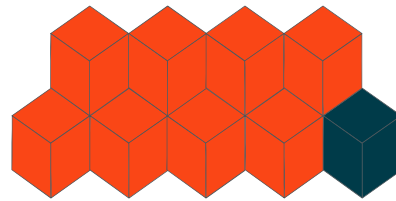
Decentralized



Distributed

Transparent with Pseudonymity

Immutable

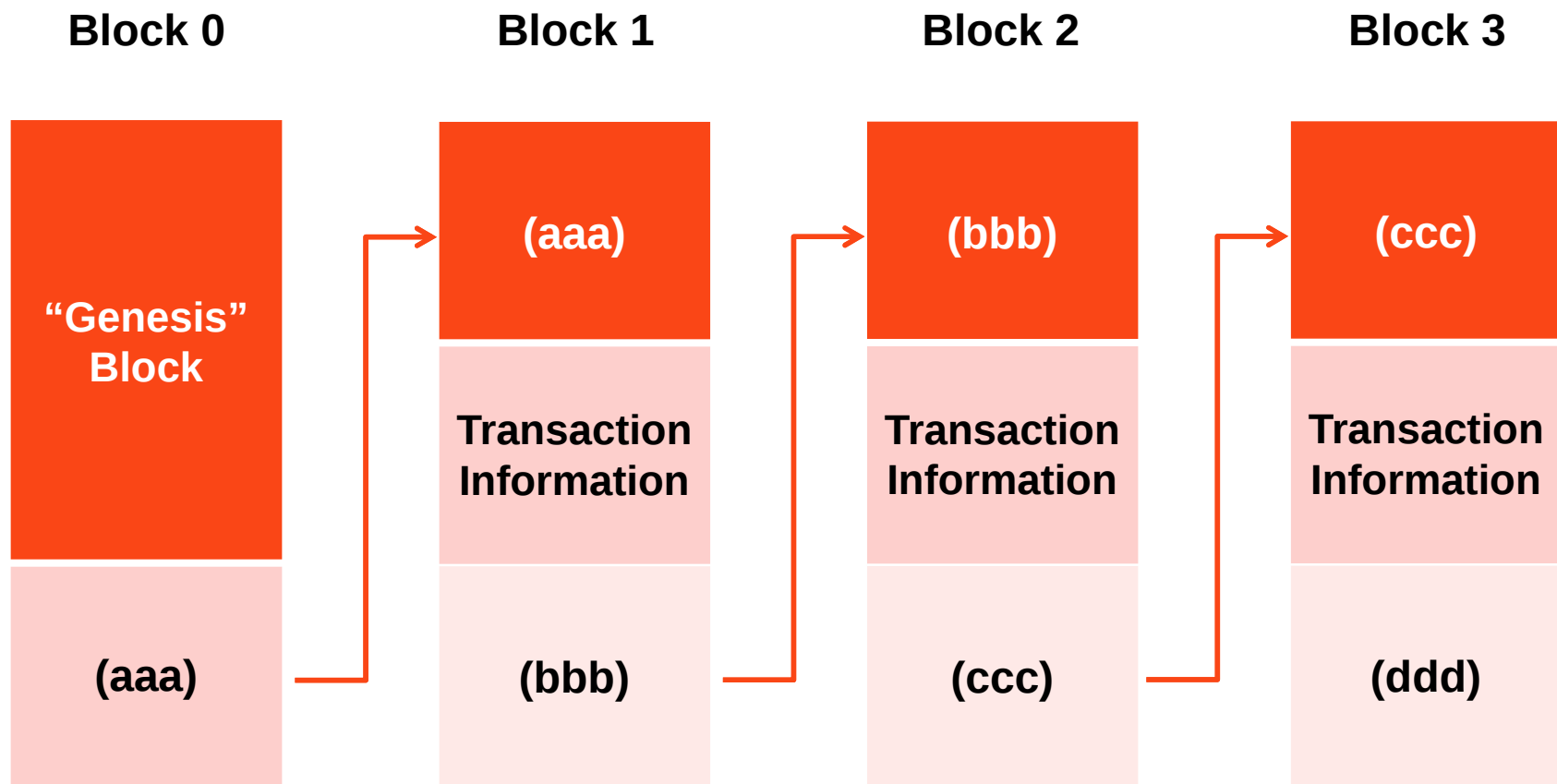


Im-mu-ta-ble

i(m)'myoōdəb(ə)l/

adjective

Unchanging over time or unable to be changed. e.g., "an immutable record"



“Faith in Math”

Not in a Central Authority

Hashing

Hash Function

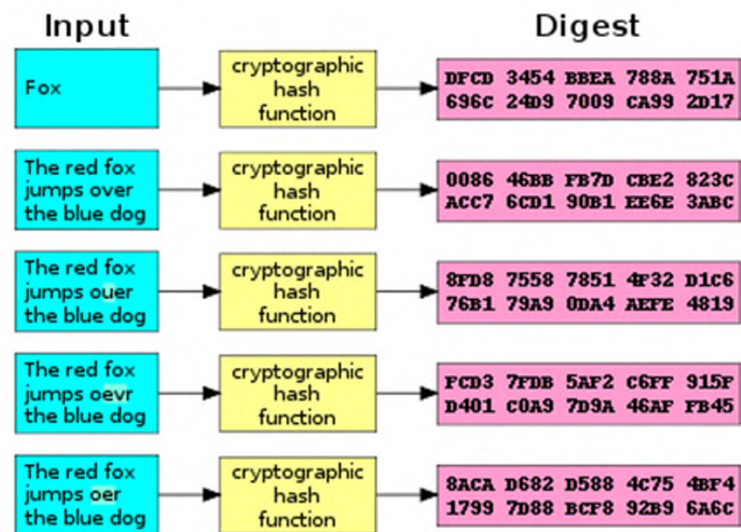
/ˈhæʃ fəŋɡ(k)ʃ(ə)n /

noun

A type of cryptographic security mechanism

A mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a “hash”) and is designed to be a one-way function, that is, a function which is infeasible to invert.

Hashing



Encrypted

Pub·lic key cryp·tog·ra·phy

/ 'pəblik kē krip 'təgrəfē/

noun

An encryption technique that uses a paired public and private key (or asymmetric key) algorithm for secure data communication in which a message sender uses a recipient's public key to encrypt a message. To decrypt the sender's message, only the recipient's private key may be used. *aka* “PKC”

Public Private Hybrid

Public	Permissionless	Fully Decentralized	Consensus- driven	Identity not known	Trustless	Slower Speed
Private	Permissioned	Centralized Control	Rules- driven	Identity known	Trusted	Faster Speed
Hybrid	Semi- Permissioned	Partly Decentralized	Varies	Varies	Trust- building	Higher Speed

✓ not
How is it being used?



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for

Blockchain

≠





	Bitcoin (BTC)	Virtual Currency Payment	Public	Open Source	Fully Decentralized
	Ethereum (ETR)	Smart contracts	Public	Open Source	Fully Decentralized
	Zcash (ZEC)	Privacy Anonymity	Public	Open Source	Mostly Decentralized
	Ripple (XRP)	Payment Network	Public	Open Source	Somewhat Decentralized

“Blockwashing”

Block·wash·ing

/ 'bläkwôSHiNG, 'bläkwäSHiNG/

verb

The practice of touting something that was entirely possible without a blockchain as particularly special because you are using a blockchain.

Smart Contracts
Real Estate
Financial Transactions
Music Industry
Healthcare
Identity Management
Online Privacy

Smart Contracts

<i>Traditional contracts</i>	<i>Smart contracts</i>
 1-3 Days	 Minutes
 Manual remittance	 Automatic remittance
 Escrow necessary	 Escrow may not be necessary
 Expensive	 Fraction of the cost
 Physical presence (wet signature)	 Virtual presence (digital signature)
 Lawyers necessary	 Lawyers may not be necessary

Smart Contracts



Real Estate

“Our main takeaway is that it could reform the entire way that government develops and procures technology,”

John Mirkovic,
Deputy Recorder of
Deeds



BLOCKCHAIN PILOT PROGRAM FINAL REPORT

May 30, 2017

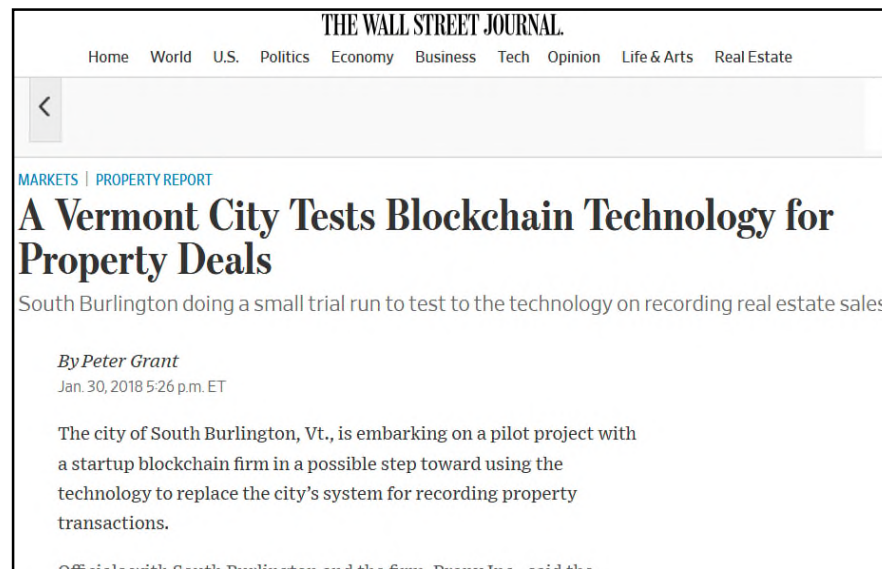
Karen A. Yarbrough
Cook County Recorder of Deeds

by **John Mirkovic**

Deputy Recorder of Deeds (Communications/IT)

REPORT AND ADDITIONAL RESOURCES AVAILABLE AT COOKRECORDER.COM/BLOCKCHAIN

Real Estate



Real Estate

BusinessWire
A Berkshire Hathaway Company

Log In Sign Up

Q

≡

New Blockchain Law Passed in Vermont Following Propy's Successful Title Registry Project

Propy's Land Records Project Advances With Signing of New Blockchain Law

Act 205 Solidifies Vermont and Propy as Leading Public-Private Blockchain Partners

August 28, 2018 06:55 AM Eastern Daylight Time

PALO ALTO, Calif.--(BUSINESS WIRE)--Vermont Governor Phil Scott today ceremonially signed into law bill S.269 (Act 205), legislation supporting the development of blockchain businesses in Vermont. The new law mandates the review of blockchain technology usage for the recording of land records and other public records. Propy CEO Natalia Karayaneva was featured at the public signing ceremony, speaking on Propy's role in providing blockchain education and in creating the first property deed in the United States bearing blockchain information.

Financial Services

RegTech
(KYC/AML)

Financial Services

Share Trading

Financial Services

How IBM Blockchain World Wire works



Using blockchain technology and the Stellar protocol, IBM Blockchain World Wire makes it possible for financial institutions to clear and settle cross-border payments in seconds.



Two financial institutions transacting together agree to use a stable coin, central bank digital currency or other digital asset as the bridge asset between any two fiat currencies. The digital asset facilitates the trade and supplies important settlement instructions.*



The institutions use their existing payment systems – seamlessly connected to World Wire's APIs – to convert the first fiat currency into the digital asset.

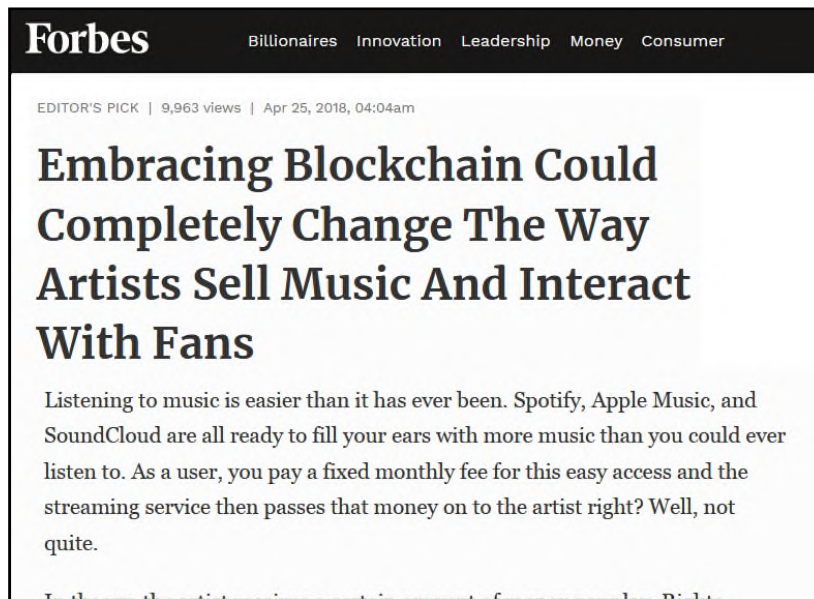


World Wire then simultaneously converts the digital asset into the second fiat currency, completing the transaction. All transaction details are recorded onto an immutable blockchain for clearing.

[PDF Download the infographic \(442KB\)](#)

Let's talk

Music Industry



Healthcare

TechRepublic SEARCH AI IoT Cybersecurity More Newsletters Forums Resource Library [Get the Free Trial](#)

SECURITY

BlackBerry's new blockchain tools could boost security for medical IoT

Fresh off the announcement of its Spark platform, BlackBerry unveiled a host of tools aimed at improving data privacy in healthcare.

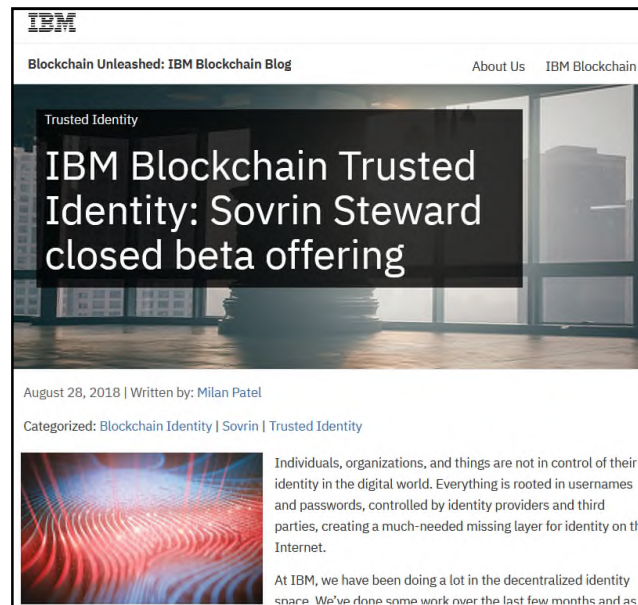
By [Canner Forest](#) | October 4, 2018, 11:39 AM PST

	HIE Pain Points	Blockchain Opportunities
	Establishing a Trust Network depends on the HIE as an intermediary to establish point-to-point sharing and "book-keeping" of what data was exchanged.	Disintermediation of Trust likely would not require an HIE operator because all participants would have access to the distributed ledger to maintain a secure exchange without complex brokered trust.
	Cost Per Transaction , given low transaction volumes, reduces the business case for central systems or new edge networks for participating groups.	Reduced Transaction Costs due to disintermediation, as well as near-real time processing, would make the system more efficient.
	Master Patient Index (MPI) challenges arise from the need to synchronize multiple patient identifiers between systems while securing patient privacy.	Distributed framework for patient digital identities , which uses private and public identifiers secured through cryptography, creates a singular, more secure method of protecting patient identity.
	Varying Data Standards reduce interoperability because records are not compatible between systems.	Shared data enables near real-time updates across the network to all parties.
	Limited Access to Population Health Data , as HIE is one of the few sources of integrated records.	Distributed, secure access to patient longitudinal health data across the distributed ledger.
	Inconsistent Rules and Permissions inhibit the right health organization from accessing the right patient data at the right time.	Smart Contracts create a consistent, rule-based method for accessing patient data that can be permissioned to selected health organizations.

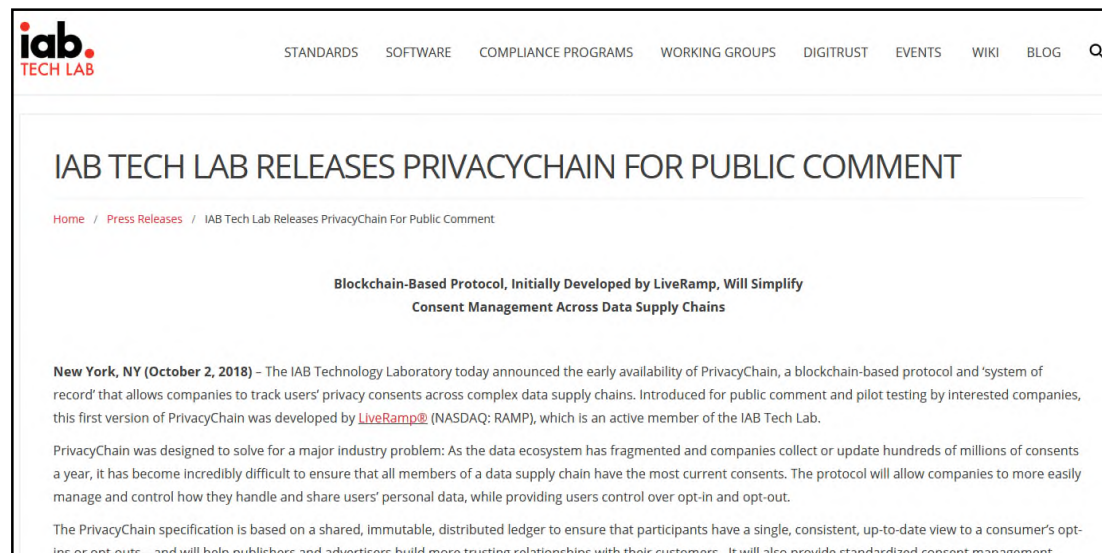
Identity Management



Identity Management



Online Privacy



What (legal) issues does it raise?

Legal Issues

- Security
- Privacy
- Intellectual Property
- Governance
- Liability

Security

“Even when developers use tried-and-true cryptographic tools, it is easy to accidentally put them together in ways that are not secure.”

Neha Narula
Director, MIT Digital Currency
Initiative

Security



WIRED

LILY HAY NEWMAN SECURITY 03.07.18 08:00 AM

THE LEAKED NSA SPY TOOL THAT HACKED THE WORLD

AN ELITE RUSSIAN hacking team, a historic ransomware attack, an espionage group in the Middle East, and countless small time cryptojackers all have one thing in common. Though their methods and objectives vary, they all lean on leaked NSA hacking tool EternalBlue to infiltrate target computers and spread malware across networks.

Leaked to the public not quite a year ago, EternalBlue has joined

Security

Bloomberg Law

> Privacy & Data Security News

News Insights

Hackers Target Bitcoin with Leaked NSA Software Tip, Report Says

Sep. 19, 2018 9:56AM

- *Cyber Threat Alliance releases report on cryptocurrency mining*
- *Illicit cryptocurrency mining surged 459 percent in 2018*

Hackers are illegally generating Monero, Bitcoin and other cryptocurrencies by exploiting a software flaw that was leaked from the U.S. government, according to new research, raising questions about the security of one of the fastest-growing corners of financial markets.

Detected cases of illicit cryptocurrency mining—the digital equivalent of minting money—have surged 459 percent in 2018 compared to last year, Cyber Threat

Privacy

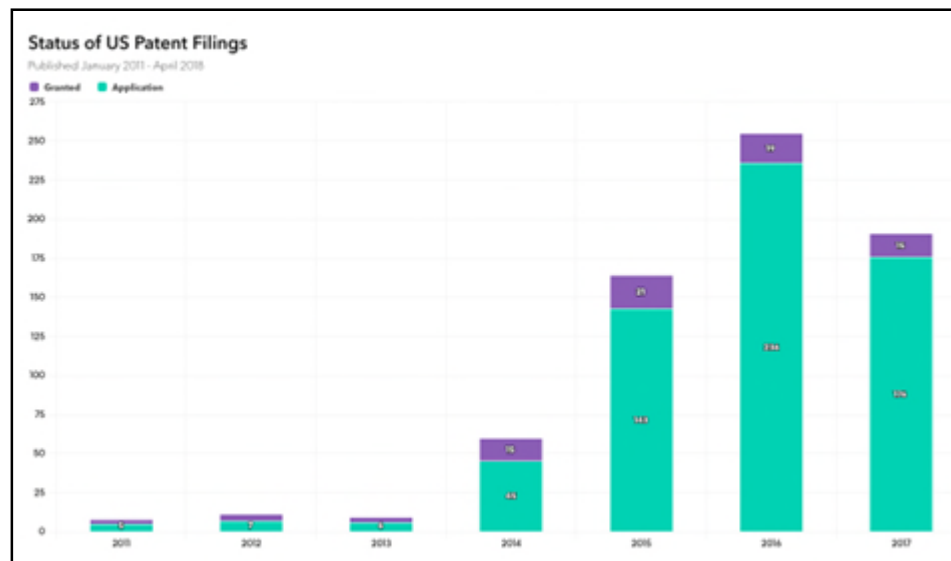
4.5.2016	EN	Official Journal of the European Union	L 119/1
REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)			

- (7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- (8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Privacy

4.5.2016	EN	Official Journal of the European Union	L 119/1
REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)			
<i>Article 15</i> Right of access by the data subject 1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case access to the personal data and the following information:			
<i>Article 16</i> Right to rectification The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a			
<i>Article 17</i> Right to erasure ('right to be forgotten') 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:			

Intellectual Property



Intellectual Property

Open Source

Intellectual Property

Ownership

Governance



Liability

Where to next?

Closing thoughts...

BRYAN
CAVE
LEIGHTON PAISNER

Jason Haislmaier
jason.haislmaier@bclplaw.com

bclplaw.com