Blockchain's Role in Strengthening Security and Privacy

Nir Kshetri

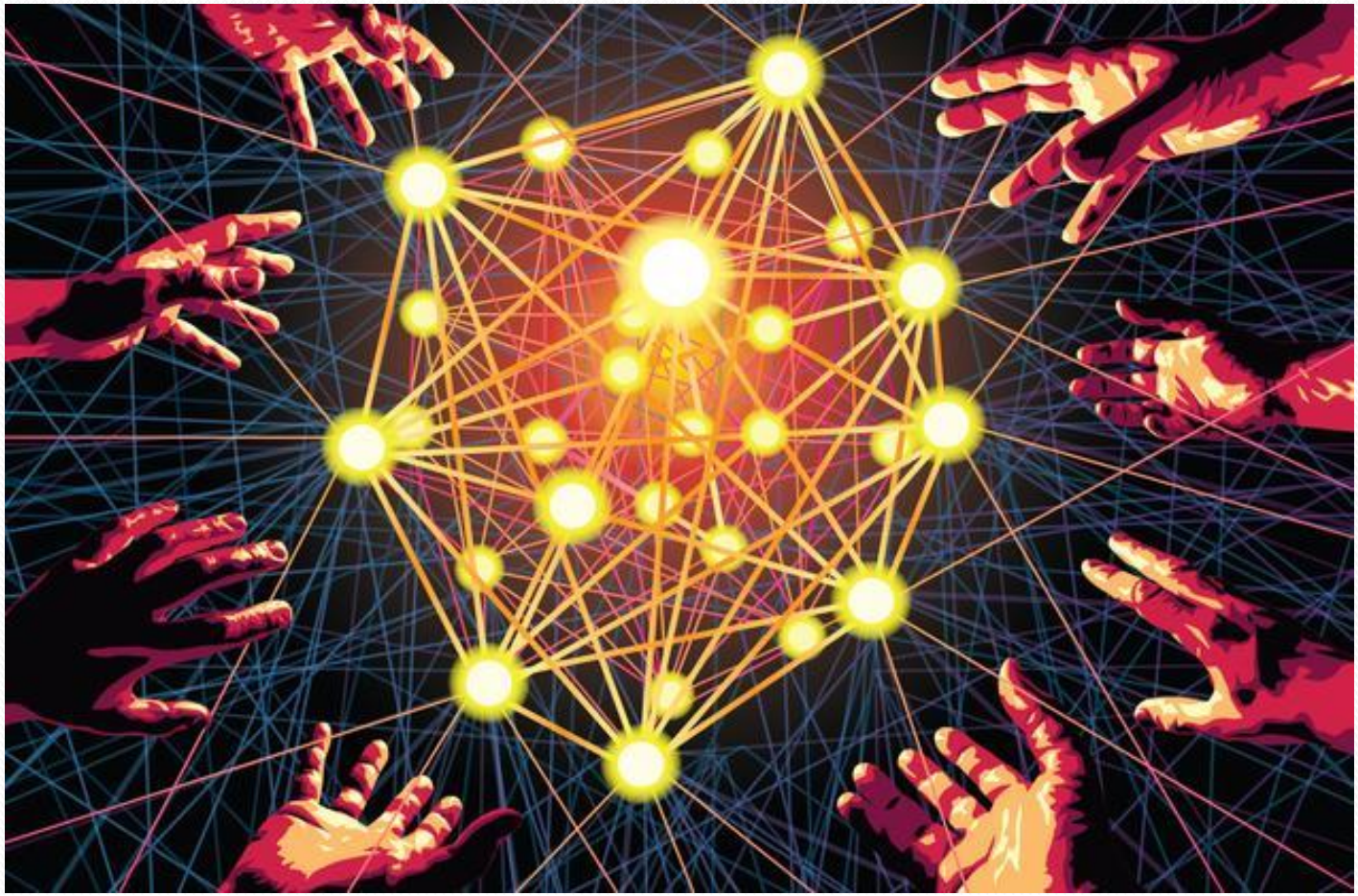
Professor, University of North Carolina—Greensboro

Prepared for the 2018 IEEE Global Blockchain Summit

Outline

- Blockchain in relation to cybersecurity
- Blockchain and IoT security
- Blockchain in enhancing security and privacy of EHR
- Blockchain and secure voting
- Blockchain in preventing ad frauds
- Some challenges and overcoming them

What is blockchain?



Source: techcrunch.com and teepublic.com

THE WALL STREET JOURNAL.

Europe Edition ▾ | May 30, 2018 | Today's Paper | Video

Blockchain Could Be the Answer to Cybersecurity. Maybe.

Why Don't Companies Just Encrypt All Their Data? It ...

Companies Struggle to Stay On Top of Security Patches

Why You Should Consider a Password Manager

BUSINESS | JOURNAL REPORTS: LEADERSHIP

Blockchain Could Be the Answer to Cybersecurity. Maybe.

The technology has a lot going for it, but first it has to clear some major hurdles

By Nir Kshetri

May 29, 2018 10:06 p.m. ET

One of the most promising cybersecurity tools that exists today is something many people have heard about but few fully understand: blockchain technology.

From The Experts

Blockchain May Be

Blockchain's key features

Feature	Explanation	Some uses
Decentralization	Decentralized network of online registries synchronized to track transactions.	Malicious actions can be detected and prevented. Participants verify information themselves.
Immutability	Complete documentation of creation, modification and deletion of records.	Transactions are auditable Improves transparency (e.g., access to data about food). No susceptible to theft, damage, corruption, or fraud.
Cryptography-based digital signatures to verify identities	Users sign transactions with a "private key": Hackers cannot guess Known only to the person who controls the account.	A high level of cybersecurity and privacy protection.

Blockchain and principles of FIPs

FIP principle/ provision	Challenge in a non-blockchain world	How a blockchain model can address?
Transparency principle	Without the knowledge or consent of a consumer, intermediaries may use private information for purposes that the consumer does not expect or understand.	There is no custodian or steward of user data. Data are controlled with private and public keys.
Security provision	Failure to protect PII and unintended or inappropriate disclosure	The owner chooses what information to release to whom and what to withhold.
Individual participation principle	Passive data collection.	Smart contract connects a consumer with all the concerned parties and ensures: explicit participation.
Accountability principle	The lack of audit trail: accountability cannot be assessed.	An audit trail to ensure that accountability has not been neglected

Kshetri, N. (2017).Blockchain's roles in strengthening cybersecurity and protecting privacy *Telecommunications Policy*, 41(10), pp. 1027-1038

SUBSCRIBE

SCIENTIFIC AMERICAN

English Cart 0 Sign In | Registe

THE SCIENCES MIND HEALTH TECH SUSTAINABILITY EDUCATION VIDEO PODCASTS BLOGS STORE

THE CONVERSATION

ELECTRONICS

Using Blockchain to Secure the "Internet of Things"

The ability to better track and distribute security software updates would help fortify insecure IoT devices, which have already contributed to major cyber disasters

By Nir Kshetri, The Conversation US on March 10, 2018

SECURING IT

EDITORS: Rick Kuhn, NIST, kuhn@nist.gov
Tim Weil, Scram Systems, tweil.ieee@gmail.com

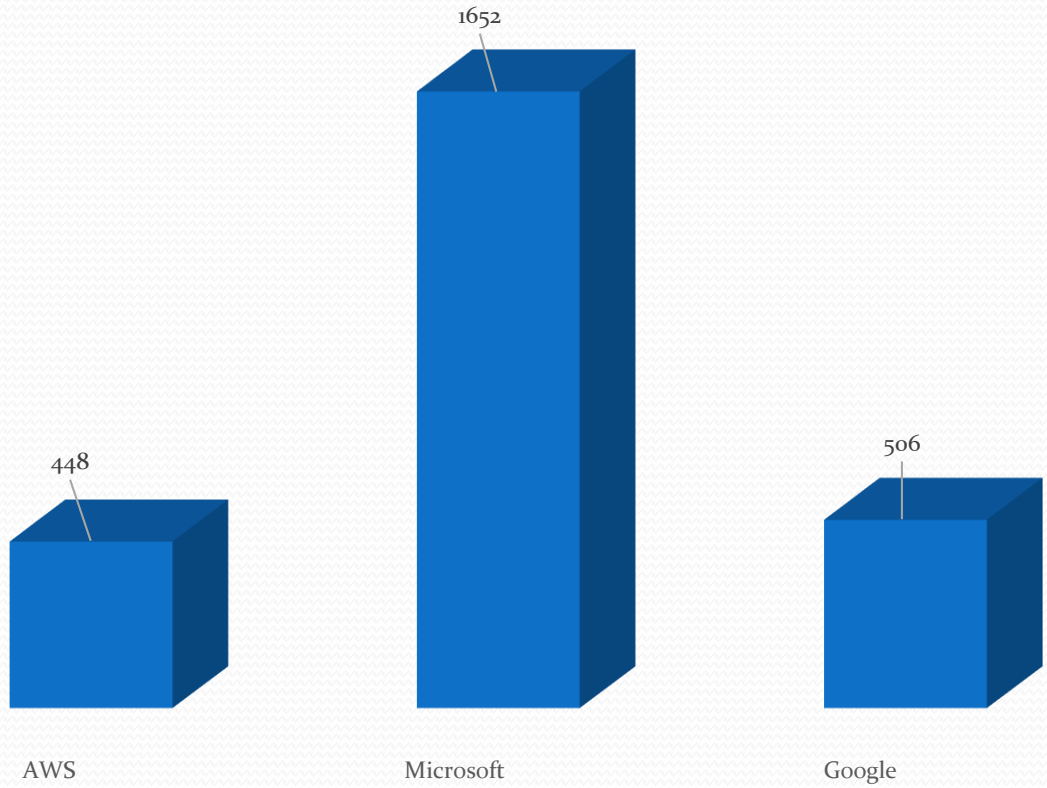
Can Blockchain Strengthen the Internet of Things?

Nir Kshetri, *University of North Carolina at Greensboro*

Current challenges

- Immature
- Cheap sensors = zero security
  - Identity validation challenge
- Capacity constraint: Data growth = 2 *(bandwidth growth) (IBM)
- Centralized cloud model: susceptible to manipulation
- Cloud downtime

Cloud downtime of major CSPs (early 2015-early 2017) (Minutes)



IoT insecurity a key concern

- October 2016 cyberattacks on Dyn.
- Attacks originated from "tens of millions of IP addresses".
  - Some malicious traffic from IoT devices:
    - Webcams, baby monitors, home routers and DVRs.
- Infected with Mirai.
- IP spoofing attacks in the later versions.

A comparison of cloud and blockchain

	Cloud	Blockchain
Mechanisms related to efficiency, and cost-effectiveness	Pay as you go model: better than legacy system (building capacity by buying more computers, more software and hiring more people) Cloud's IaaS	Removes the need for third parties in transactions by creating a distributed record which is possessed and verified by other users.
Deployment models	Private, community and public	Permissionless/permissioned chains: security, privacy, and other requirements Possible to target specific members: regulators and auditors
Some mechanisms to strengthen cybersecurity	Cyber risk free zone": constant monitoring for suspicious activities and real time response. Data encrypted Some companies employ "Zero Trust" network: fine-grained control	Data fully encrypted Cryptographic hash functions
Some challenges	Many rely rely on the firewall model.	Newness: well-developed security mechanisms have not developed for some systems

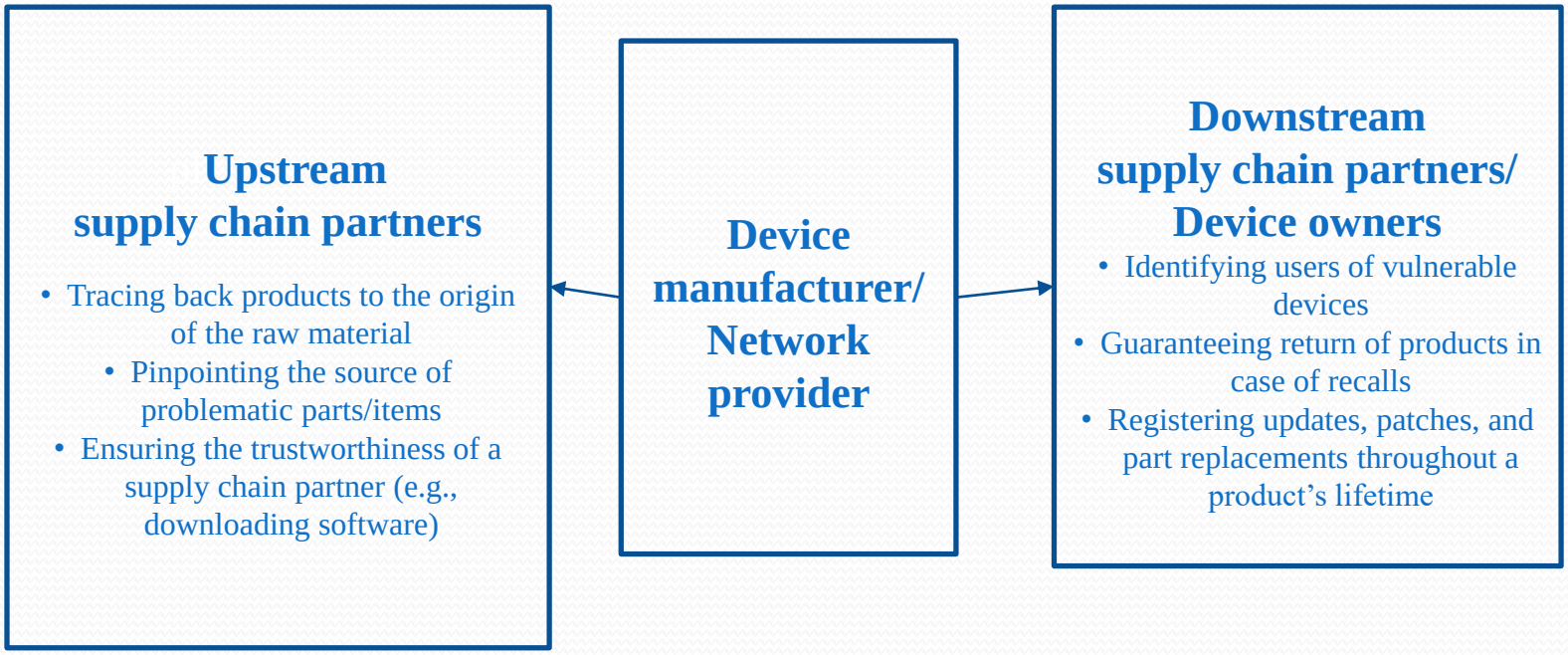
Blockchain's potential to address key challenges associated with cloud-based IoT

Challenge of cloud-based IoT	Explanation	How blockchain can help to address the problem
Costs and capacity constraints	Exponential growth in IoT devices: by 2020, a network capacity at least 1k times 2016 level needed.	No need of a centralized entity: Devices can communicate securely, exchange value and execute actions through smart contracts.
Deficient architecture	Each block of IoT architecture acts as a bottleneck/point of failure: vulnerability to DDoS attacks, hackings, data thefts, and remote hijackings.	Secure messaging between devices: validity of a device's identity is verified, transactions are signed and verified cryptographically
Server downtime and unavailability of services	Servers are down due to cyberattacks, bugs, power, cooling or other problems.	No single point of failure: records on many computers/devices, identical information.
Susceptibility to manipulation	Information is likely to be manipulated and put to inappropriate uses	Decentralized access and immutability: malicious actions can be detected and prevented.

Blockchain's role in improving security in supply chain networks

- IoT-linked crises could behandled in a better way.
- Hangzhou Xiongmai Technologies recalled products
  - Difficult to track down the owners/contact.
- Blockchain: register time, location, price, parties involved, and other relevant information.
  - Track raw materials, transformed into circuit boards/ electronic components, integrated into products, sold.
  - Register updates, patches, and part replacements

Blockchain's role in strengthening security in a supply chain network

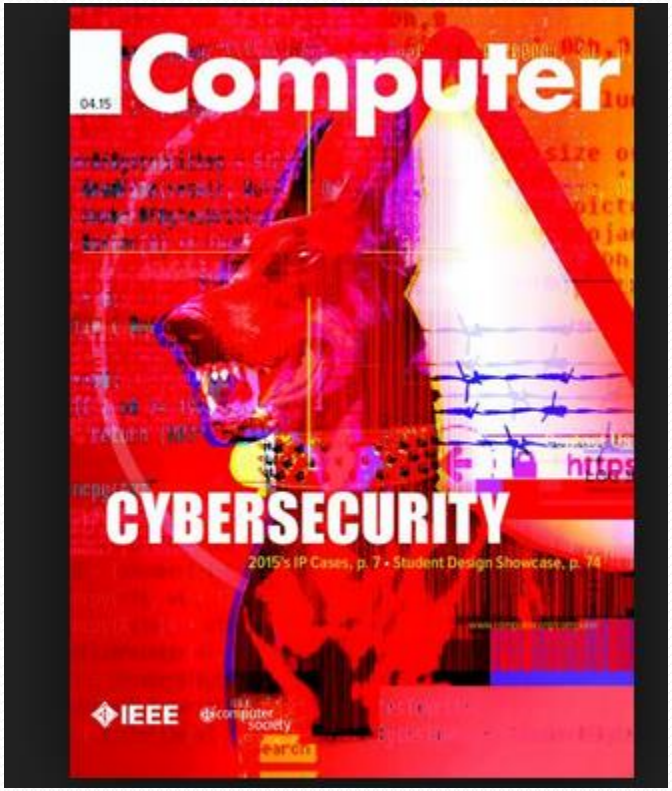


Kshetri, N. (2017)."Can Blockchain Strengthen IoT?" *IEEE IT Professional*, 19(4), 68-72.

Some initiatives

- Technology and financial companies: standard for securing IoT applications using blockchain.
  - Cisco
  - Bosch
  - BNY Mellon
  - Foxconn Technology
  - Gemalto
  - Consensus Systems
  - BitSE
  - Chronicled.
- Aim : Blockchain protocol as a shared platform to protect IoT.
- April 2017: API supported technologies offered by major blockchain systems.
- Users register multiple weaker identities: serial numbers, QR codes, and UPC code
  - Bind them to stronger cryptographic identities.

Improving security of healthcare data



Kshetri, N. and Voas, J. (2018)." Blockchain and Electronic Healthcare Records ", IEEE *Computer* (November).

Challenges in current healthcare data handling practices

- Data not audited in a standardized way.
- Push model: if a patient is transferred to a different hospital, the new hospital may not be able to access the data that was "pushed" to the first hospital.
- Pull model: consents on an informal/ad hoc basis.
- Lack of audit trails: no guarantee of data integrity from the point of data generation to the point of data use.
- Regulations and policies: vary across jurisdictions

Blockchain's benefits

- Share medical records securely across providers during the lifetime of a patient
- No organization between the patient and the records.
- Time-stamped and audit trails
- No need to create custom functionality for each EHR vendor.
- A consumer makes a change to her/his data
  - Communicated to the public ledger.

Blockchain in information and access management in healthcare data

	Explanation and examples	Challenges with the current system	Blockchain's potential
Information authenticating the subject's identity	Information to verify that someone is who he/she claims to be.	Reliance on password-based systems: exchanged and stored on insecure systems.	Each transaction signed by the private key.
Information describing the information	Info. about different pieces of data flow (e.g., users' preferences : how data can be used, consent management records)	No audit trails of who accessed patients' data. Some rely on paper medical records	Audit trail: complete documentation of events related to the creation, modification, and deletion
Actions that various participants are authorized to perform	Access rights and privileges of each participant (e.g., insurance companies can't have access to confidential medical records).	Various parties take actions based on patients' data. Patients : no control over data.	Prevents unauthorized and illegitimate access. Patients hold ownership and ultimate control

Privacy and security in voting/elections

Blockchain-Enabled E-Voting

Nir Kshetri and Jeffrey Voas

0740-7459/18/$33.00 © 2018 IEEE

CSDL Home » IEEE Software » 2018 vol. 35 » Issue No. 04 - July/August

IEEE Software

Might address two of the most prevalent concerns:

- voter access
- voter fraud

Table 1. Blockchain-based solutions deployed for voting at the community, city, and national levels.

Setting	The context	Remarks
The city of Moscow's Active Citizen program	In December 2017, the program started using a blockchain for voting and to make the voting results publicly auditable. Each question discussed by the community and put up for voting is moved to the e-voting system using a blockchain. After the voting is complete, the results are listed on a ledger containing all the previous polls.	The most popular polls were reported to have 137,000 to 220,000 participants.[10] In one such case on the Ethereum platform, citizens indicated their preferences for temporary relocation if the building in which they were living would be demolished and replaced by a better building. The platform reached a peak of approximately 1,000 transactions per minute. It's not clear whether the platform can handle the volume if a higher proportion of Moscow's 12 million citizens participate in the voting.
The South Korean province of Gyeonggi-do's community projects	The province used a blockchain-based voting system to gather votes on community projects. 9,000 residents voted.	The Korean financial-technology startup Block developed the blockchain platform.
The annual general meeting of the Estonian tech company LVH Group	Shareholders can log in using their verified national online ID and vote at the meeting.	The voting system issues voting-right assets and voting-token assets to shareholders. A user can spend voting tokens to vote on meeting agenda items if that user owns the related voting-right asset. Nasdaq designed the system.
Sierra Leone's March 2018 general elections	Swiss startup Agora carried out tallying in two districts. After the voting, a team of accredited observers from different locations manually entered approximately 400,000 ballots into Agora's blockchain system.	This test was considered a partial deployment of a blockchain.[11] The elections were only verified by blockchain, not blockchain powered. Agora provided an independent vote count, which was compared with the main tally.

Protecting from external and internal attacks

- BEVs are trustworthy
- PwC's audit commissioned by the City of Moscow.
  - Looked at the possibility that the outcome could be manipulated
    - By internal employees and external attacks.
- No reason to be concerned for polls that involved ~ 300k votes.

Tamper-proof audit trails for voting

- Ensures that no vote has been changed or removed
  - No fraudulent and illegitimate votes were added.
- Hackers to compromise the network:
  - Hack a majority of the “blocks”
  - Complete the hack before new blocks were introduced.
- Individual votes: publicly available
  - Voters masked behind an encrypted key.
- Reduces voter suppression
  - Bad actors cannot identify voters

Prevalence of Ad frauds

- Ad fraud—US$19b in 2018
- Click fraud: among most lucrative activities for botnet
  - Monthly profit of a botmaster with a network of 30k bots
    - US$26k by launching DDoS attacks
    - > US$18m in bank frauds
    - > US$20m in click fraud.
- Difficult for advertisers, demand-side platforms (DSPs) and others to find or locate the perpetrators.
- PPC providers' secretive techniques to detect invalid clicks
  - Provide only aggregated statistics about clicks.

Blockchain's potential

- Add a layer of transparency to the programmatic ad-buying process
  - Identify fraudulent traffic
- Possible to know who did what and when.
- Smart contract to connect relevant parties together.
  - Advertising viewer, advertiser, phone company and location information provider (e.g., Google)
- Viewers may be paid
- Verify ad delivery and increase personalization without breaching privacy laws

An example: MetaX's AdChain

- Advertiser buys impressions thro' a real-time buying platform.
- The platform finds target audiences in ad exchanges
  - Access to inventory of online publishers (e.g., ad space on websites).
- Adds a tracking beacon
- Stores impressions, clicks, and audience data in blockchain,
  - Shared among parties in an ad campaign.
- Data are encrypted and broadcast to each participant.
- Relevant parties approve.
- The block becomes part of the permanent ledger
  - Can be audited and verified

Challenge #1: High degree of cyber-vulnerability

- A process-based model: risk-based strategy
- Risk = threat + vulnerability + consequences .
- Cyber-vulnerability: susceptibility to harm from cyber-attacks.
- Most blockchain networks run the same code
- In case of a faulty code: the entire system could be at risk.

Challenge #2: Ensuring accuracy when data is entered

Blockchain-based property registries may help lift poor people out of poverty

June 28, 2018 6:38am EDT

Many rural farmers in India lack clear ownership of the land they work and live on. AP Photo/Anupam Nath

Email
Twitter 35
Facebook 94
LinkedIn

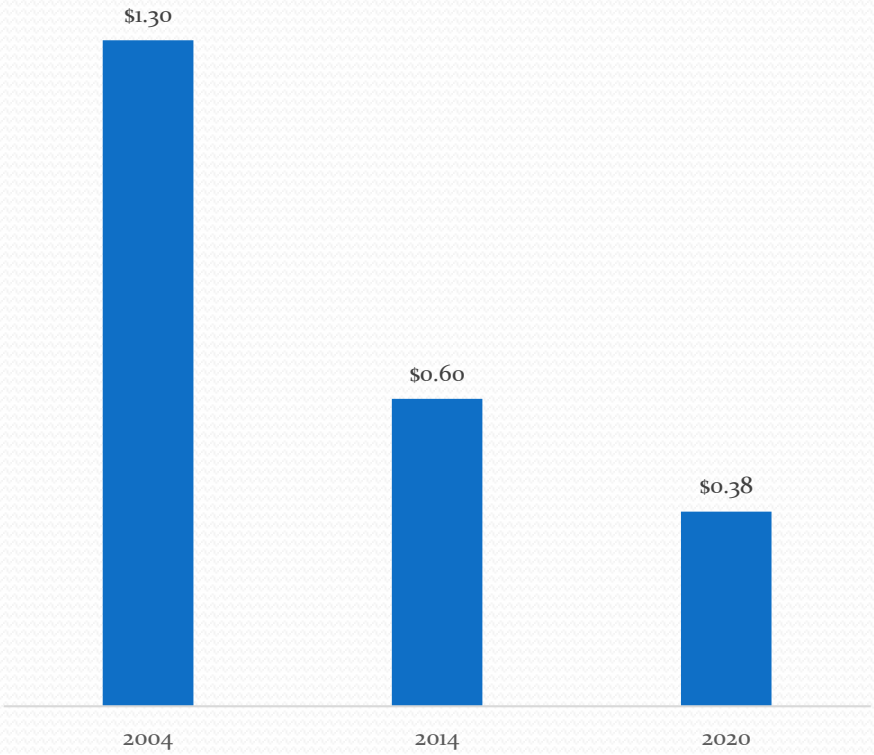
Many developing countries don't have a working system of tracking property rights, and what they do have can be fragile and incomplete. In Haiti, for instance, a large earthquake in 2010 destroyed all the municipal buildings that stored documents confirming many small farmers' ownership of the land they worked. Even years later, many farmers didn't have

Author

Nir Kshetri
Professor of Management, University of North Carolina – Greensboro

- Especially problematic in land registries in developing countries
- Difficult to determine the legitimate owner.

Challenge #3: Low incentive to incorporate blockchain

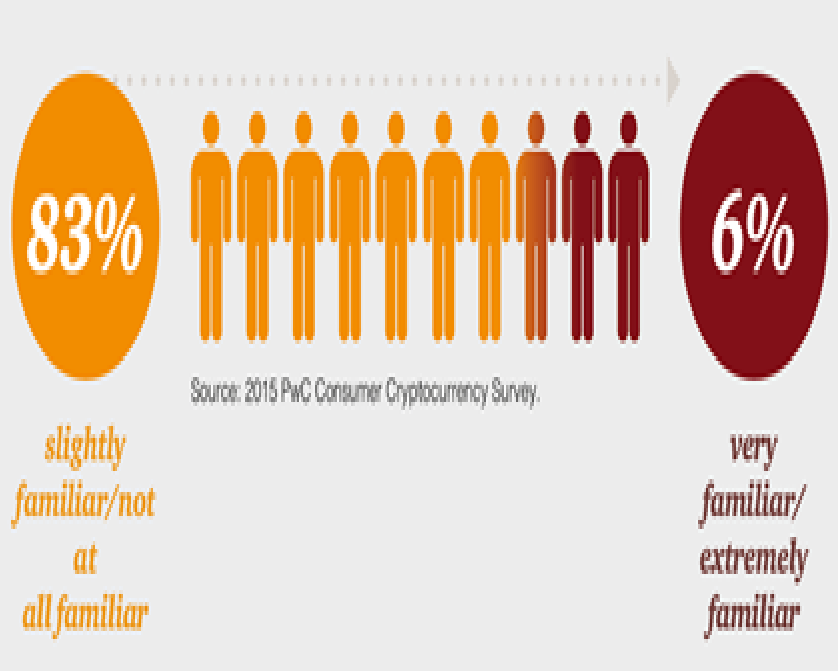


Average cost of a sensor

Source: Goldman Sachs, BI Intelligence Estimates

- Companies that make cheap IoT devices: operate on small profit margins.
- IoT devices: low memory and processing power
- Even lightweight validation models require more than most IoT devices can handle.

Challenge #4: Awareness and understanding among key decision makers



- WFA and dataxu's study, Dec. 2017: only 3% of advertisers understood blockchain's potential to reduce ad fraud

Who should do what

- Innovators' research efforts: feasible to connect billions of IoT devices
- Technology companies: user-friendly security applications.
- Pressure from external stakeholder.
  - Regulators
  - Insurance industry
  - Consumers
    - Make clear products won't sell unless they're more secure.
- Land titles/assets: governments or other implementers need to be fair and impartial
  - Process: transparent and participatory.

Who should do what (contd.)

- Key decision makers: clearer understanding of the benefits of blockchain in cybersecurity
  - Communicate them to consumers and organizations.
- Development of rich blockchain ecosystem
  - Verified national online ID
- Collective efforts
  - Measures at the industry and trade association levels

Thank you!

Email: nbkshetr@uncg.edu