

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: BAC-T07

Blockchainification of Cyber Supply Chain Risk: Hype vs. Hope

Celia Paulsen

Cybersecurity Researcher
National Institute of Standards and
Technology



#RSAC

Disclaimer

The identification of any commercial product or trade name is included solely for the purpose of providing examples of publicly-disclosed events, and does not imply any particular position by the National Institute of Standards and Technology.

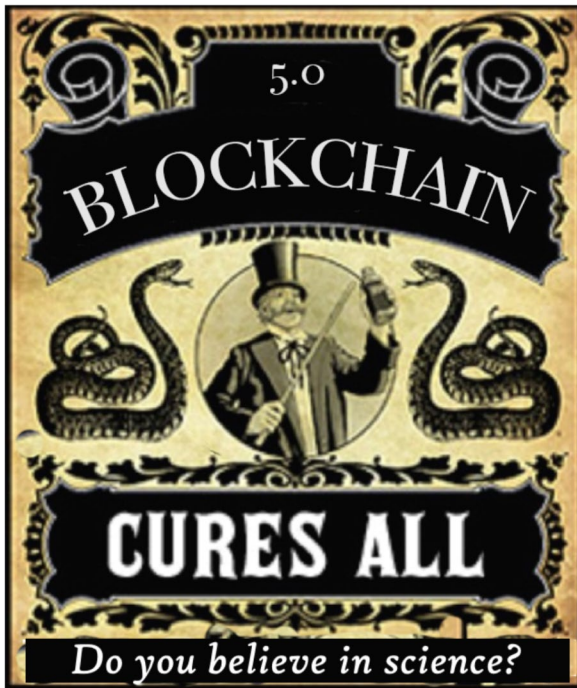


Blockchain all the Things!

Iced tea company rebrands as “Long Blockchain” and stock price triples

Bitcoin madness: Small-cap Longfin soars 2,000% after acquiring blockchain company

Why Big Business Is Racing to Build Blockchains



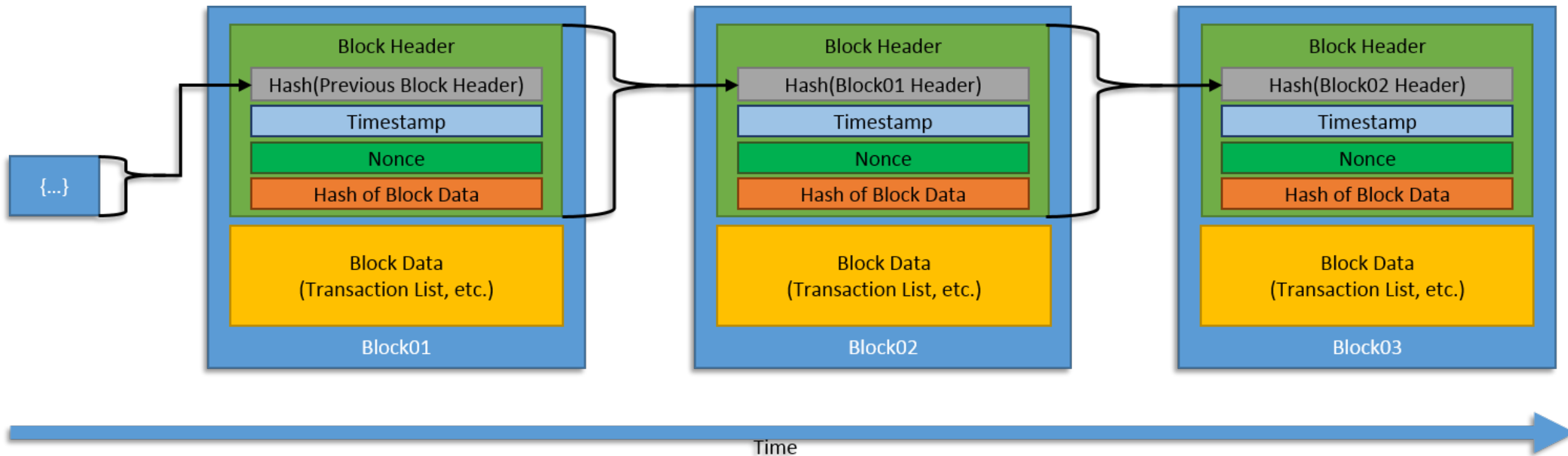
Australian stock exchange to move to blockchain

Blockchain: A Better Way to Track Pork Chops, Bonds, Bad Peanut Butter?

Red Hot Blockchain Tech

Blockchain study finds 0.00% success rate and vendors don't call back when asked for evidence

Blockchain?

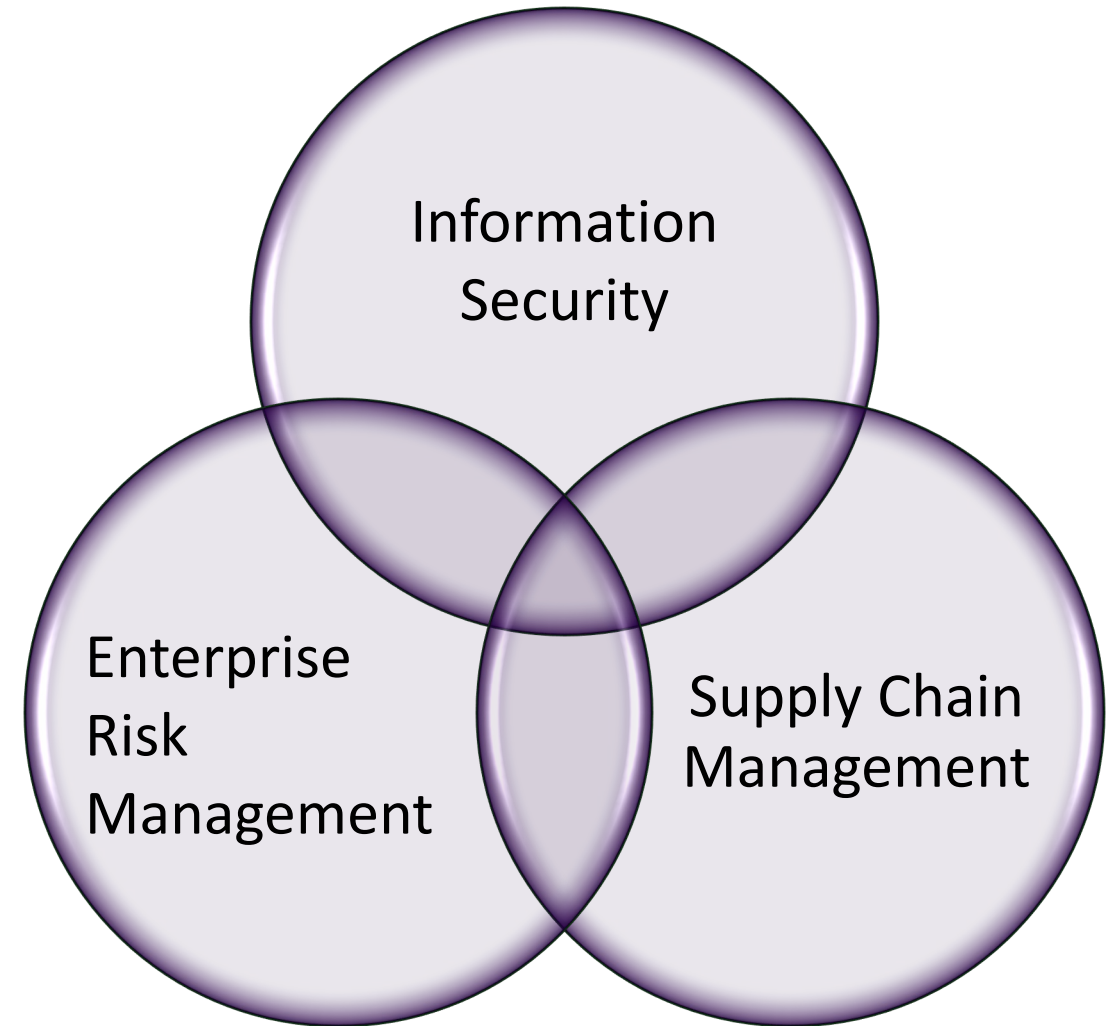


“...distributed ... ledgers of ... transactions ... cryptographically linked ... after validation and a consensus decision....”
- NISTIR 8202: Blockchain Technology Overview

Cyber Supply Chain Risk?

“risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.”

- OMB A-130



What does it all mean?

- How is / could blockchain be used... really?
 - Visibility
 - Traceability
 - Automation
 - Security
 - Usability & Cost-Savings
- For each:
 - p What problem do blockchain solutions hope to solve
 - + How the blockchain could potentially help
 - What the blockchain does *not* do
 - ? Possible solutions or opportunities

RSA®Conference2019

One Tool to Rule Them All!



1/5: Visibility

- p No visibility = no control
- + Shared ledger
- Scalability
- Privacy
- Completeness
- ? Required Participation
- ? Automation

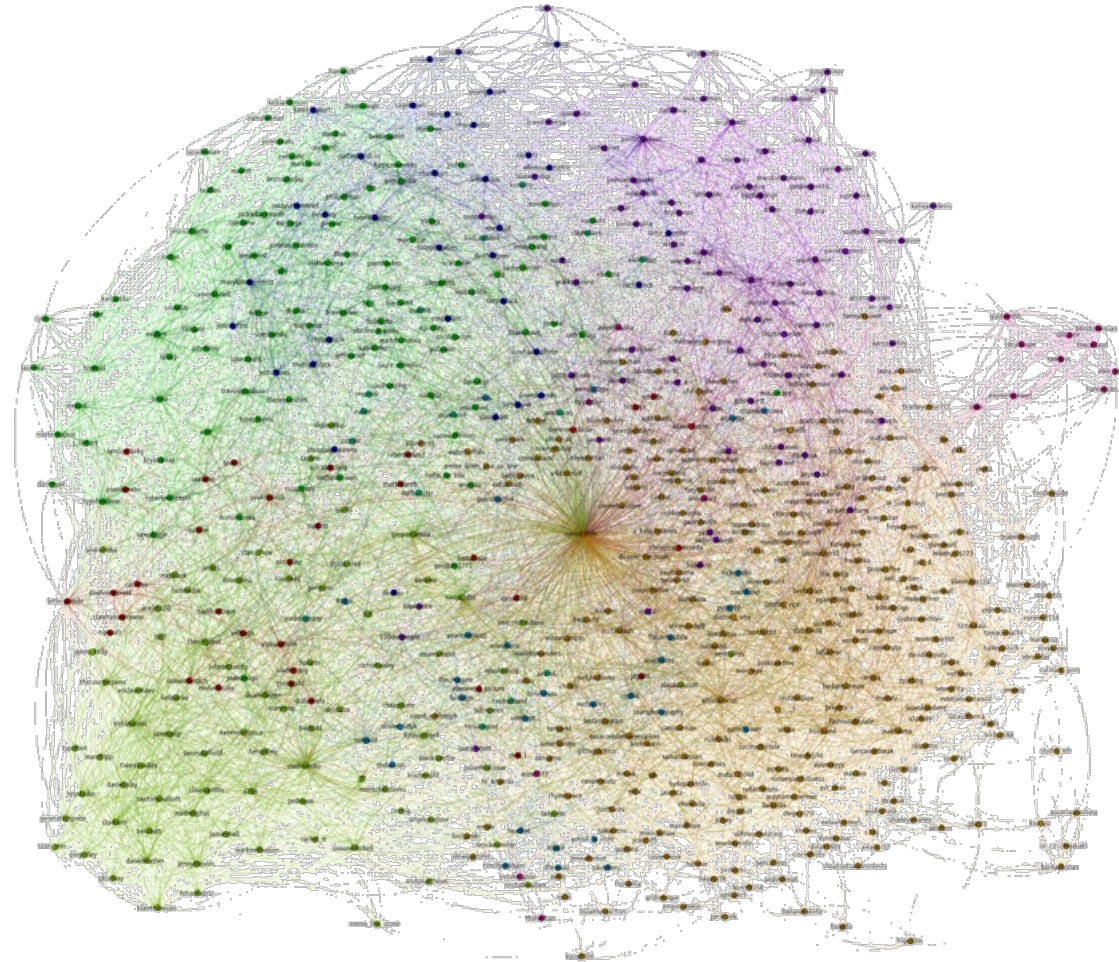


Image by Andy Lamb: <https://www.flickr.com/photos/speedoflife/6924482682>

2/5: Traceability

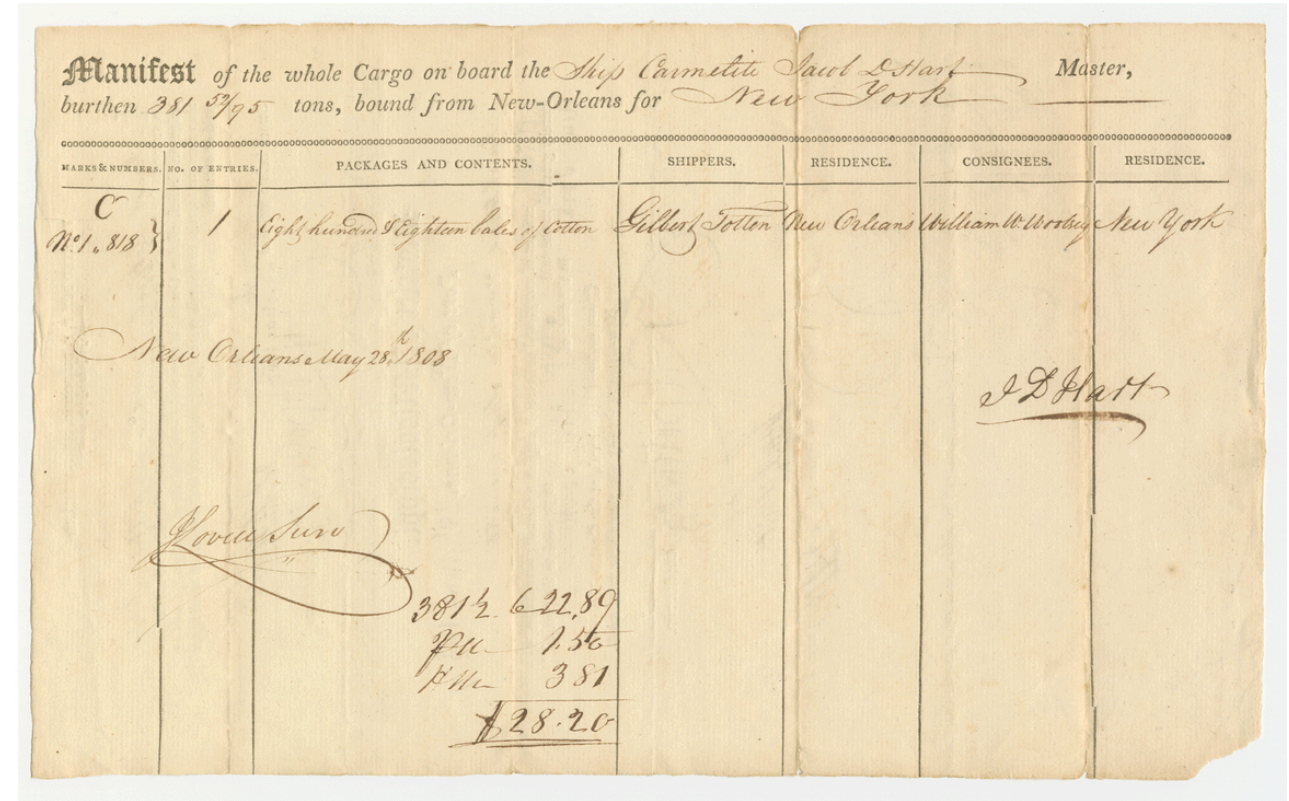
- p Who made this?
- + Tamper-evident
- + Semi-permanent
- + Detailed & precise
- Assimilation
- Interoperability
- ? Standardized interplay



Image from: sourcemap.org, created by "Leo" in 2012

3/5: Automation

- p Paperwork
- + Smart Contracts
- + Near real-time
- Self-contained ecosystem
- Validation
- ? IoT?



1808 cargo manifest:

<https://research.mysticseaport.org/item/I006405/I006405-c026/>

4/5: Security

- p Tampering, theft, etc.
- + Cryptographic foundation
- + No single point of failure
- + Means to trust the untrusted
- Trust
- Contract code validity
- ? Validate participants

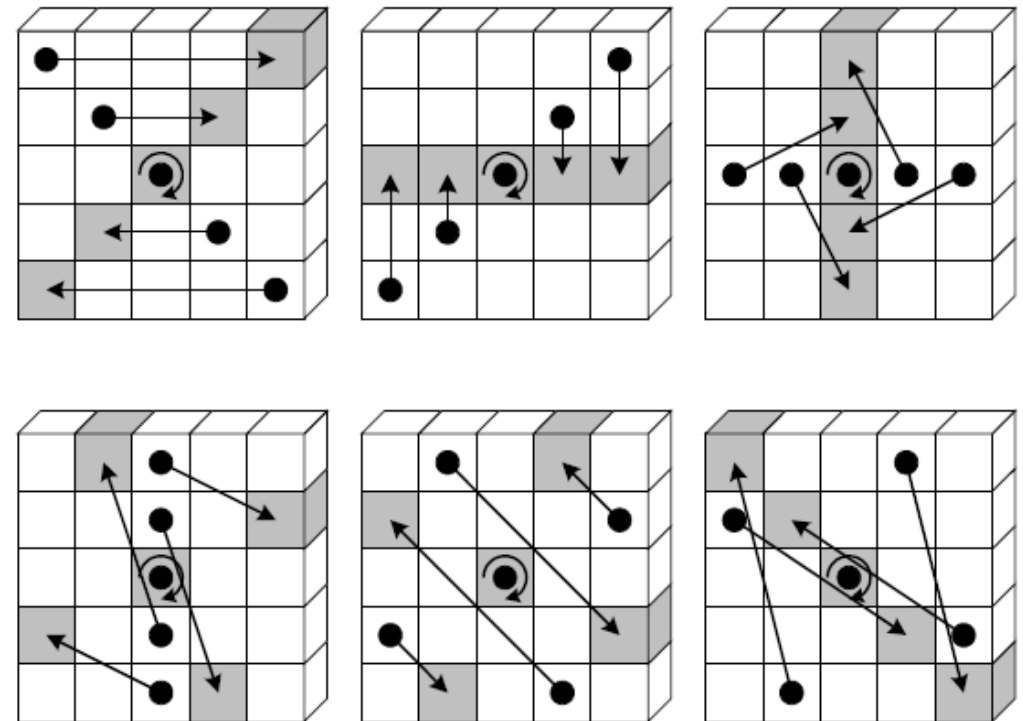


Image from FIPS PUB 202: SHA 3 Standard

5/5: Usability & Cost-savings

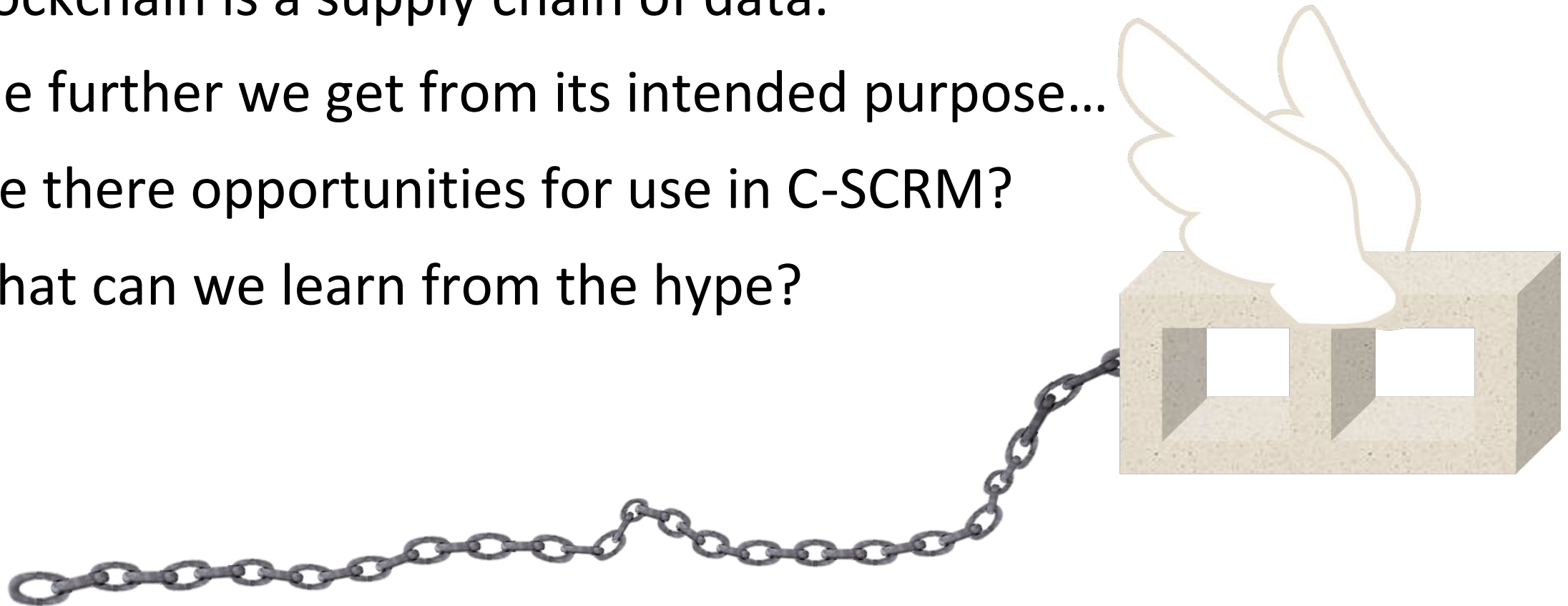
- p Existing solutions cumbersome
- + Relatively simplistic
- + Additional hardware
- Infrastructure
- Integrated with existing tools
- ? Tools



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Summary

- Blockchain is a supply chain of data.
- The further we get from its intended purpose...
- Are there opportunities for use in C-SCRM?
- What can we learn from the hype?



Homework: Apply What You Have Learned

- Next week:
 - Are you drinking snake oil?
- Next three months:
 - Do you have a use-case?
 - What are you looking to achieve?
- Within six months:
 - Plan your blockchain strategy
 - Plan your research & development strategy



Resources

- **NISTIR 8202: Blockchain Technology Overview**
<https://csrc.nist.gov/publications/detail/nistir/8202/final>
- **ISO TC 307: Blockchain and distributed ledger technologies**
<https://www.iso.org/committee/6266604.html>
- **IEEE:**
 - **P2418.1: Framework of Blockchain Use in Internet of Things**
 - **P2418.2: Standard Data Format for Blockchain Systems**
 - **P2418.3: Framework of Distributed Ledger Technology in Agriculture**
 - **P2418.4: Framework of Distributed Ledger Technology in Connected and Autonomous Vehicles**
 - **P825: Interoperability of Transactive Energy Systems with Electric Power Infrastructure**

Questions?

Celia Paulsen

celia.paulsen@nist.gov

