Designing and Auditing Cloud Based Accounting Systems with Blockchain and Distributed Ledger Principles

Deniz A. Appelbaum, PhD Montclair State University
Robert A. Nehmer, PhD Oakland University

40th WCARS, November 3-4 2017, Rutgers University, Newark NJ

Designing and Auditing Cloud Based Accounting Systems with Blockchain and Distributed Ledger Principles

- Introduction
- Discussion of Blockchain (BC) and Distributed Ledger Technology (DLT)
- Issues that Challenge Auditing
- Discussion of BC Accounting and Auditing
- Demo of Cloud Application
- Areas of Future Research and Development
- Conclusion

Introduction

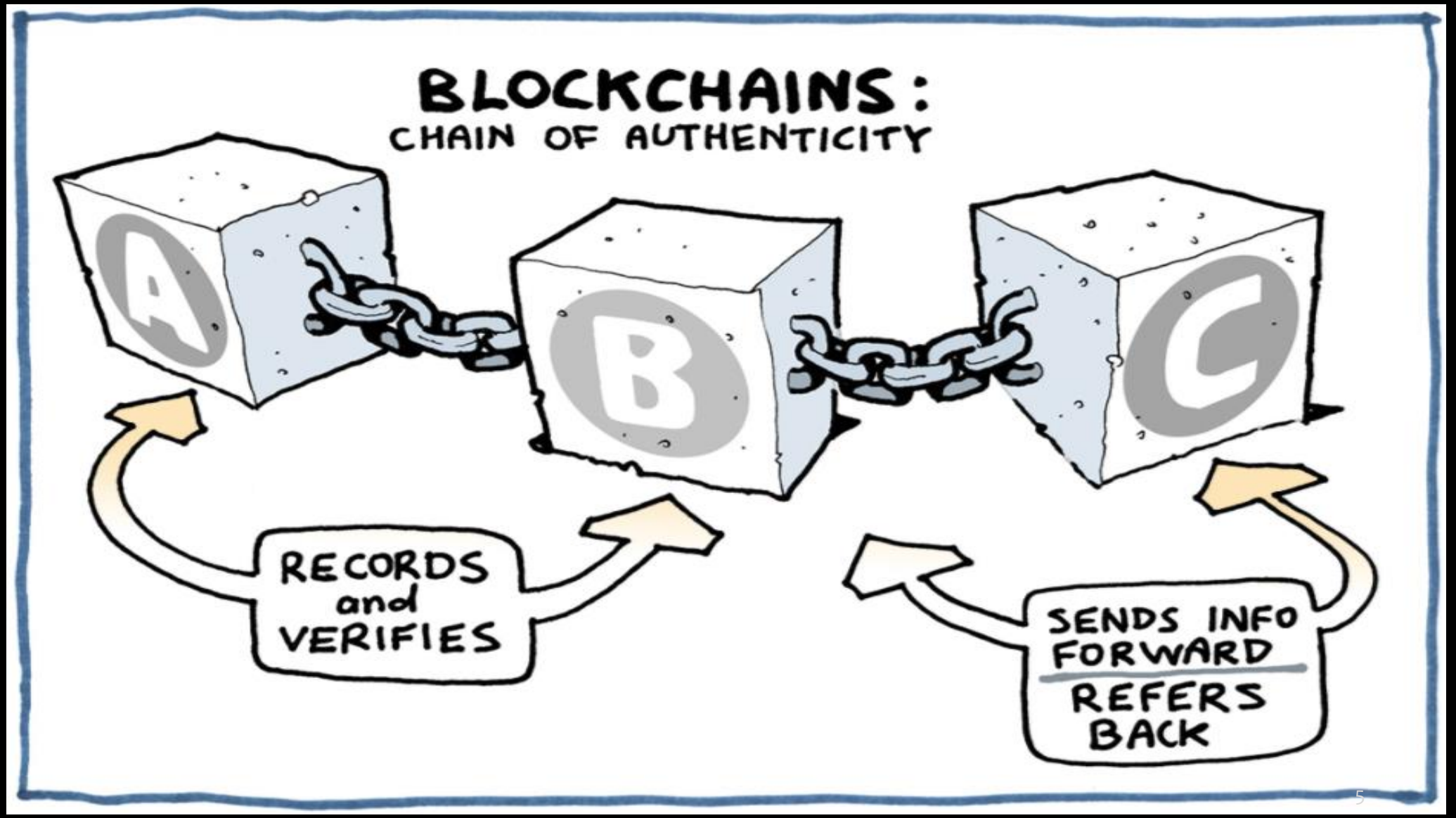
- Would Blockchain in the cloud look like this:

- Or this?

Introduction: The Advent of Blockchain

- Satoshi Nakamoto (2008)
- Provides a means for many participants of different locations to jointly record their transactions in a commonly shared master file.
- BC should be able to reduce assurance tests conducted by auditors

Blockchains



Introduction: Methodology

Design Science Approach:

- 1. Problem Identification and Motivation
- 2. Define the Objectives of the Solution
- 3. Design and Development of an Artifact which meets some of the Objectives
- 4. Demonstration of the solution
- 5. Evaluation of the solution
- 6. Communication of the problem and the solution (usually an article)

Discussion on Blockchain and Distributed Ledger Technology

- Nakomoto's 2008 original paper on Bitcoin
- Core components of DLTs:
  - There is no trusted 3rd party required, network is peer-to-peer
  - New transactions are time-stamped and hashed onto an ongoing chain of transactions
  - The hashed record cannot be changed without redoing the proof-of-work
  - Proof-of-work is accomplished by a pool of CPUs from the peer-to-peer network through computation
  - The longest chain (block of transactions) includes the latest transaction and requires the most CPU work to create the hash, therefore it takes the most times, to date, to compute the hash
  - The system works as long as the majority of peer-to-peer nodes are not colluding to subvert the chain since they could collectively represent the majority of the computing power and could compute the hash faster than any other group/participant

Discussion on Blockchain and Distributed Ledger Technology: We will work through each of these components in turn

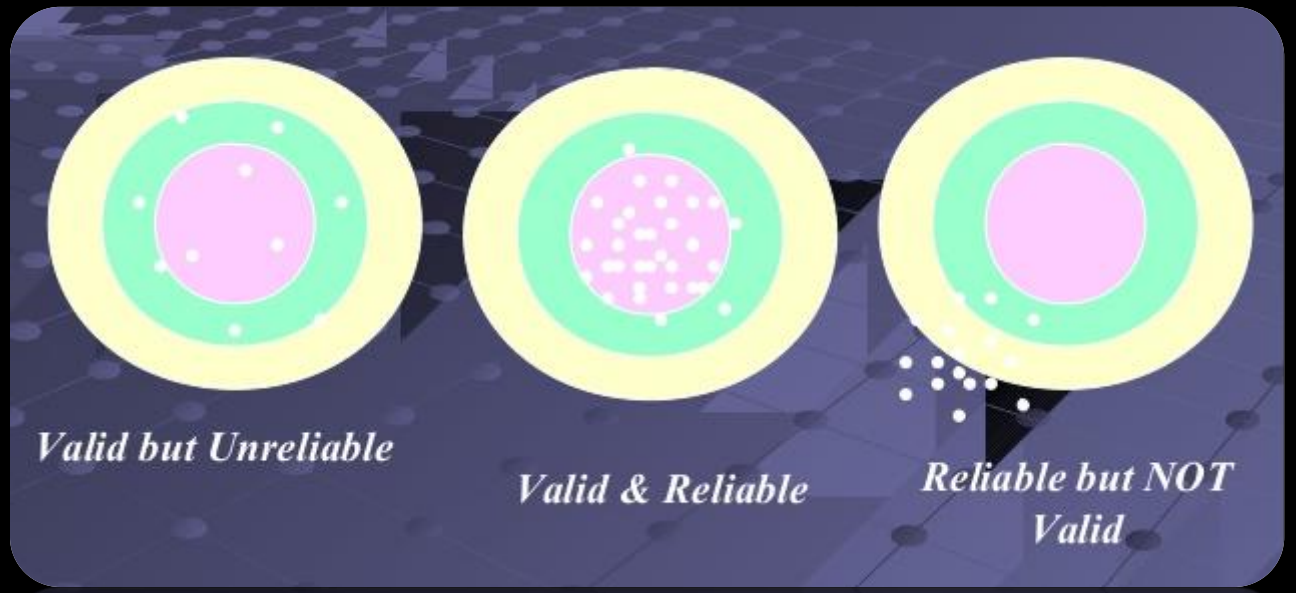
- **First,** as a design requirement, avoid the use of a third-party countersigner or oracle
  - Peer-to-peer level of trust:
    - Timestamping individual transactions
    - Hashing the transaction sequence of block using an algorithm with special properties
  - Publicly auditable cost function (hash) of Nakomoto
    - Takes longer to compute the hash value as the length of the block increases
    - Efficiently verifiable by anyone without any special information
    - Computationally expensive to alter a transaction in the hash
      - Hash for the transaction itself and all subsequent hashes will need to be re-computed
      - If valid transactions are subsequently added, perpetrator's work is increased
      - Not impossible, but infeasible and time consuming
      - But perhaps with quantum computers….

Discussion on Blockchain and Distributed Ledger Technology: We will work through each of these components in turn

- Next design requirement: Hash as proof-of-work
- Third Component: The block cannot be changed without re-computing a new hash for every step and configuration!
- Fourth: Some cooperation amongst peers is required for operational efficiency.
- Fifth: The latest un-hashed block contains all of the transaction history of previous transactions and hashes.
- Sixth: as long as the majority of peer nodes are not actively trying to subvert the network, they can complete the future hashes faster than fraudulent peers

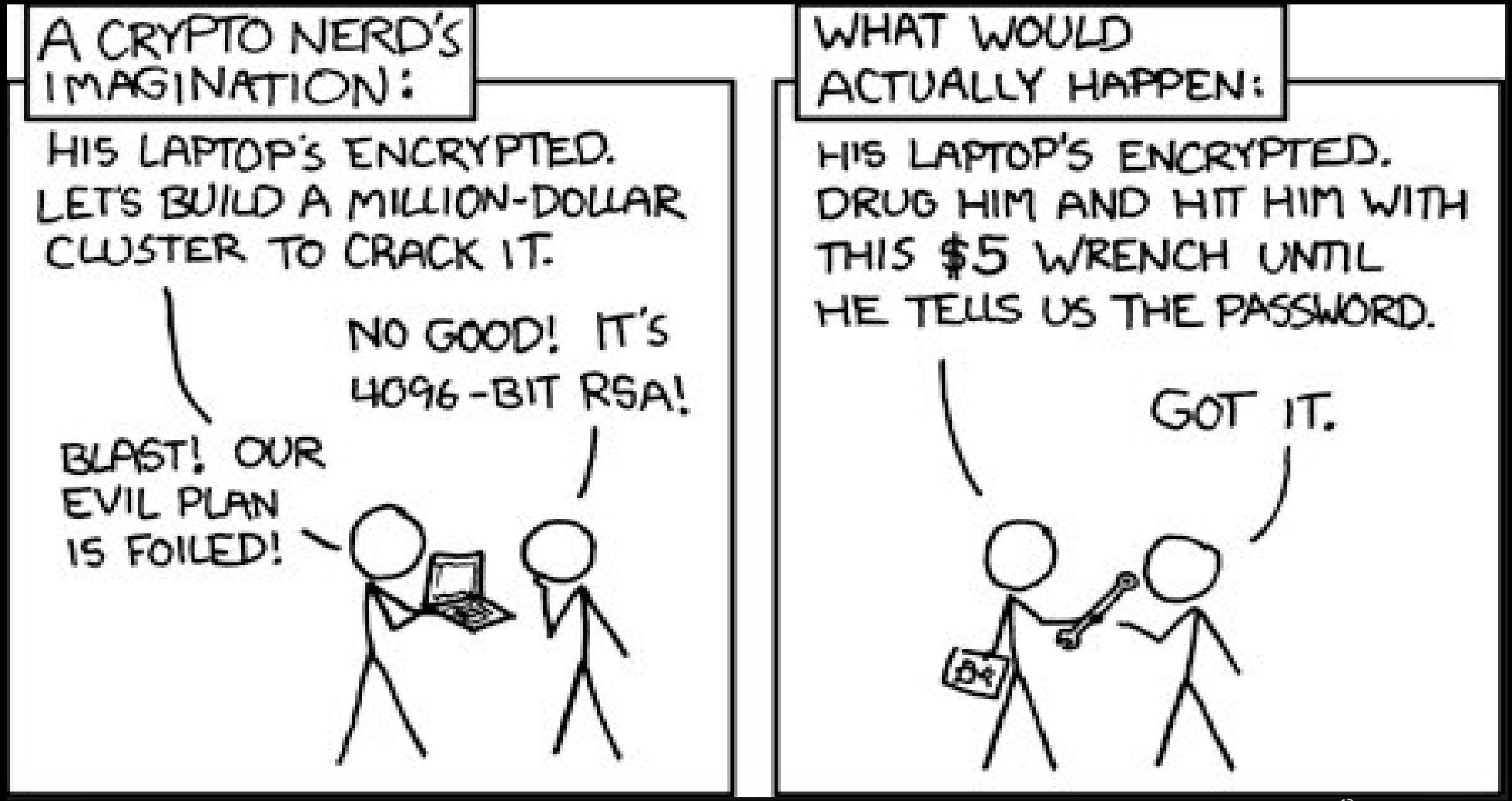
Issues that Challenge Auditing: Data Reliability

- Reliable and valid evidence is that which can be trusted, verified, and "seen" by the auditor
- Data sources external to the client are considered to be more reliable
- Are these two ideas the same for private or semi-private blockchains?



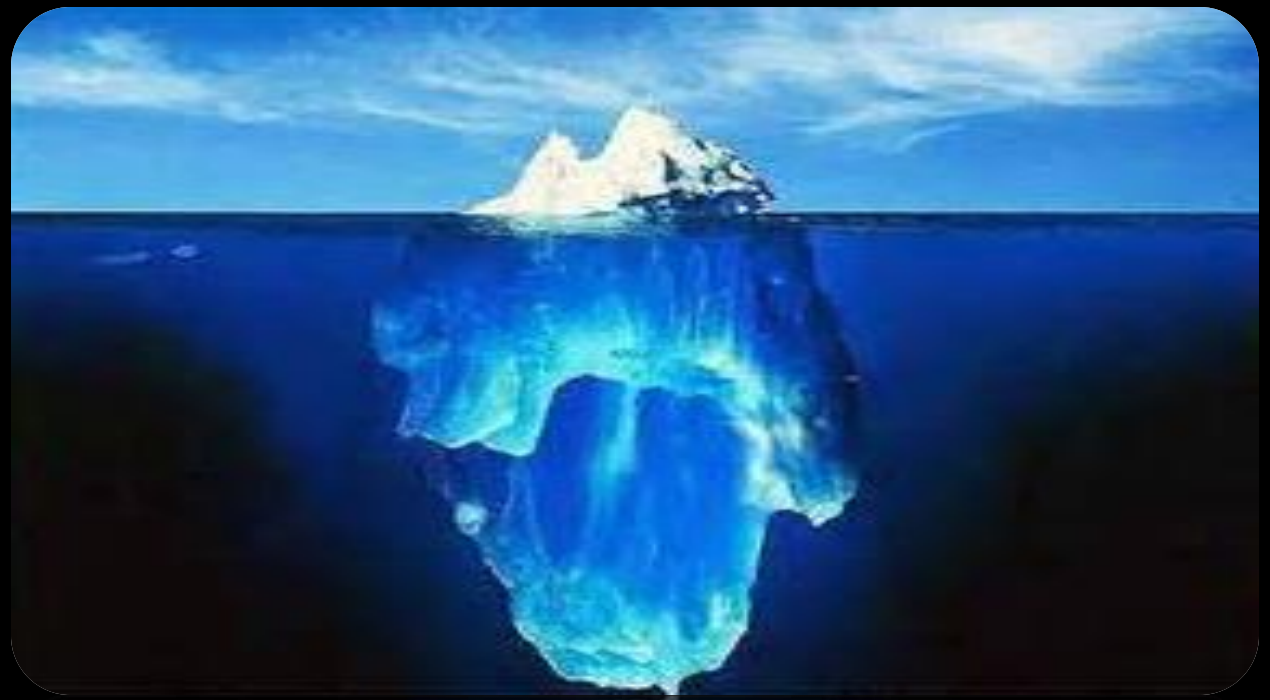
Issues that Challenge Auditing: Data Security

Management Assertion	Control Objectives
Accuracy	Input of each transaction and data is accurate
Completeness	All transactions are entered
Occurrence	Transactions only entered once
Accuracy	Processing of transactions is accurate


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Issues that Challenge Auditing: Transaction Transparency

- Data generation process should be transparent, observable, reliable
- Blockchain for transactions provides a record of the series of blocks (events) and maintains their immutability because of the hashing algorithm



Discussion of BC Accounting and Auditing: Evidence Standards for Auditors

Procedure	"Traditional" Method	Blockchain enabled Continuous Method
Inspection of Records or Documents	Pull samples of records and trace/verify/match	**Evaluate entire transactions that were recorded in a blockchain**
Inspection of Tangible Assets	Physical inventory, walk through, open boxes	**RFID tagging , back end software records sensor reading with BC format in a real-time basis (minimal lag)**
Observation	Stand/sit with worker(s) and observe	**Use blockchains or process mining to verify work flows**
Inquiry	Written or oral interviews	Monitor processes and controls, identify process violators for examination
Confirmation	Verify account balances	**Link data streams using blockchain applications**
Recalculation	Extract and recalculate figures to verify	**Monitor all data and review BC calculations automatically at intervals desired**
Re-performance	Re-perform procedures to verify	**Automatically review all transactions and identify exceptions using BC**
Analytical Procedures	Scanning and statistics	Filter real-time data with continuity equations and statistics

Discussion of BC Accounting and Auditing: Observation/Inquiry

- Supports the assertions of existence, occurrence, and valuation
- Blockchain provides proof of observation/scanning for many instances
  - Auditors can observe time-stamping of transactions that are added to a chain and its hash, as a test of **reasonableness**
  - They can also observe if the length of the hashes is increasing over time
- Inquiry can be used to obtain evidence from the peer network as to their understanding of the governance characteristics of network and blockchain

Discussion of BC Accounting and Auditing: Confirmation

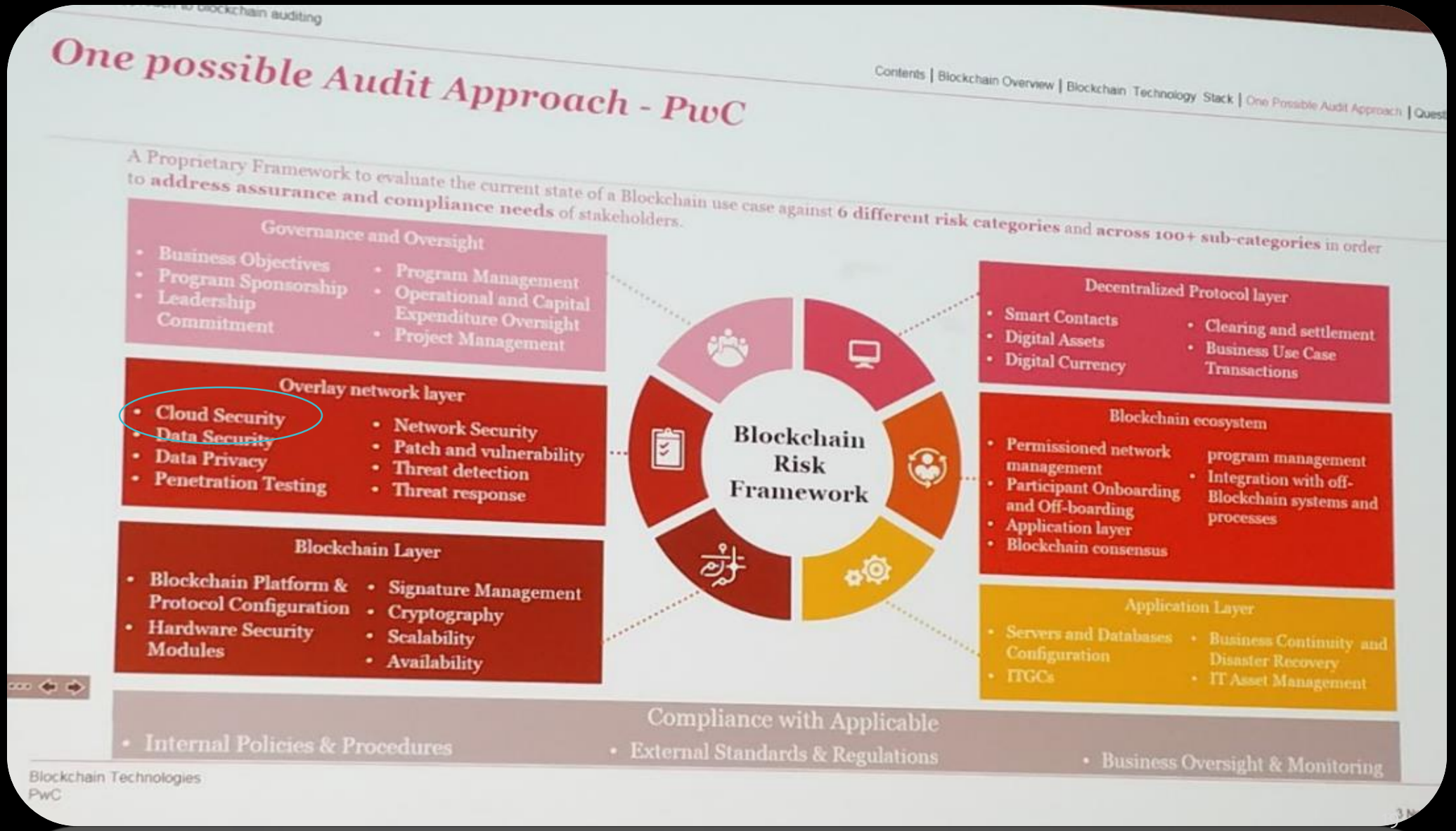
- Existence of transactions with third party/external validation already exist with the blockchain methodology
  - Real time, immediate confirmations provided by banks, clients, attorneys, regulators, and suppliers, and other consensus participants
- Specifically, a confirmation relating to the BC process components would be to confirm with members of the peer network as to the design and function of the hashing algorithm

Discussion of BC Accounting and Auditing: Inspection of Records or Documents/Recalculations

- Auditors or audit software can easily scan or inspect the documents that support the configuration or governance structure of the Blockchain process
- Auditors or audit software can scan the chains for outliers/abnormalities
- Recalculation: The hash can be verified by being calculated back-word and for-word – Accuracy assertion!


PROFITS
SALES
"What if we don't change at all ...
and something magical just happens?"

And…


Contents | Blockchain Overview | Blockchain Technology Stack | One Possible Audit Approach | Quest
One possible Audit Approach - PwC
A Proprietary Framework to evaluate the current state of a Blockchain use case against 6 different risk categories and across 100+ sub-categories in order to address assurance and compliance needs of stakeholders.
Governance and Oversight
Business Objectives
Program Sponsorship
Leadership Commitment
Program Management
Operational and Capital Expenditure Oversight
Project Management
Overlay network layer
Cloud Security
Data Security
Data Privacy
Penetration Testing
Network Security
Patch and vulnerability
Threat detection
Threat response
Blockchain Layer
Blockchain Platform & Protocol Configuration
Hardware Security Modules
Signature Management
Cryptography
Scalability
Availability
Blockchain Risk Framework
Decentralized Protocol layer
Smart Contacts
Digital Assets
Digital Currency
Clearing and settlement
Business Use Case Transactions
Blockchain ecosystem
Permissioned network management
Participant Onboarding and Off-boarding
Application layer
Blockchain consensus
program management
Integration with off-Blockchain systems and processes
Application Layer
Servers and Databases Configuration
ITGCs
Business Continuity and Disaster Recovery
IT Asset Management
Compliance with Applicable
Internal Policies & Procedures
External Standards & Regulations
Business Oversight & Monitoring
Blockchain Technologies
PwC

Demo of Cloud Computing: Cloud Computing Environment

- Clouds are popular pay-as-you-go locations for data storage
- Flexible, scalable based on demand and workload
- Perceived as INSECURE
  - Guarantees of data location and transformations are scant
  - Little client interoperability on data, applications, and service
  - Not designed to record and store log file data, due to cyclic nature of log file creation –
    - Stored separately but linked to the data objects
- Tracking of data in the Cloud persists as an open research question
- Auditors: CSP and data accountability, reliability, compliance, security, verifiability, auditability, and reperformance???
- Cloud and Blockchain? HUGE OPEN RESEARCH ISSUE

Demo of Cloud Computing: Demonstration

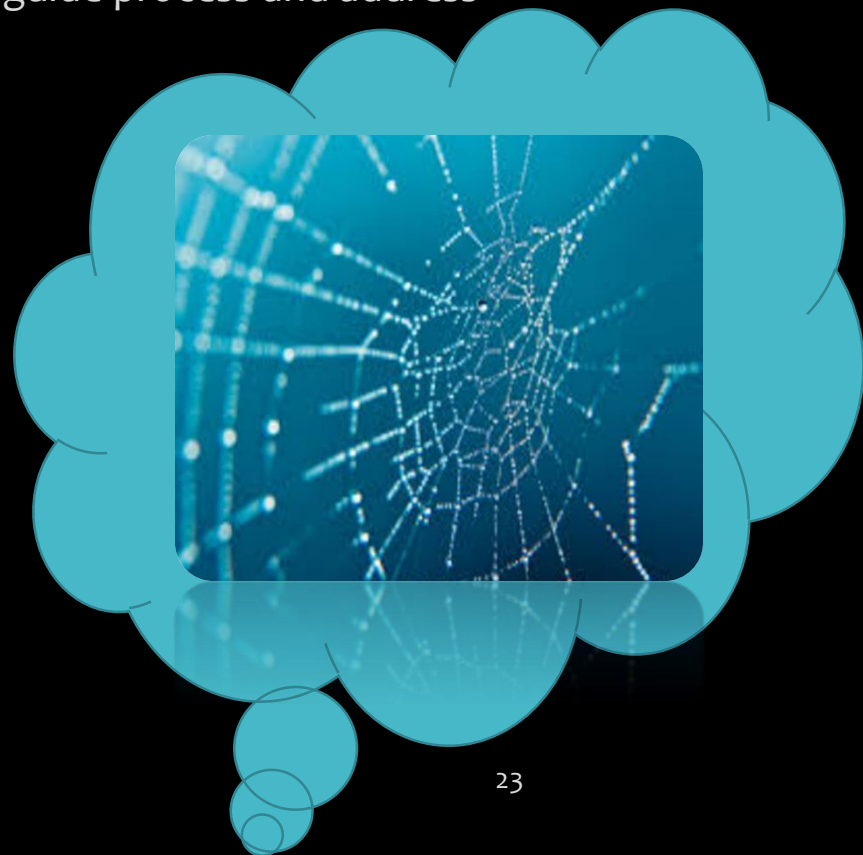
- Proof of Concept:
  - Cloud computing system with a formal governance structure
  - Designs of a blockchain application in the cloud eco-system
  - Auditing the resulting design
- Terminology
  - Cloud ecosystem with a formal governance structure includes (Schmidt et al, 2016):
    - Cloud Service User (CSU)
    - Cloud Service Provider (s) (CSP)
    - Cloud Service Network (CSN)
    - Board of Directors
    - External Auditors
    - Stakeholders: all of the above PLUS investors, regulators, lenders

Demo of Cloud Computing: Demonstration

- Where in the Cloud Ecosystem does the peer-to-peer network fit from an IT architectural standpoint?
  - Considerations:
    - The cloud being used is entirely operated and owned by the CSU
      - Risks are shifted to other peers
      - Two extremes: none are using this cloud or they are all on this same cloud
        - Or many intermittent conditions of overlapping CSPs and network members – a tangled web!
      - What if the CSU is on an external cloud, then the CSU becomes one of the peers
      - Added risk of collusion or subversion of blockchains
- Governance provisions for contracting and service provisioning of the peer-to-peer network on which the DLT operates
  - CSU: risk is affected by governance provisions
  - Auditor: risk is also the provisions themselves and their ability to collect evidence
    - Moderated by level of risk assessment, the nature and level of evidence required

Demo of Cloud Computing: Demonstration

- Potential types of audit evidence:
  - Policies on cloud computing provisioning and if they address DLT
    - Contracting process is key – are there policies and procedures to guide process and address risks?
    - How do companies enter and leave the peer-to-peer network?
    - Required audit provisions for member peers?
    - Technical details for hashing process?
    - Who is responsible for DLT contracts?
    - How will the DLT process interface in the Cloud?
    - What are the Board's role or roles in the monitoring process?
      - What if the Board doesn't understand BC ?



Areas for Future Research and Development

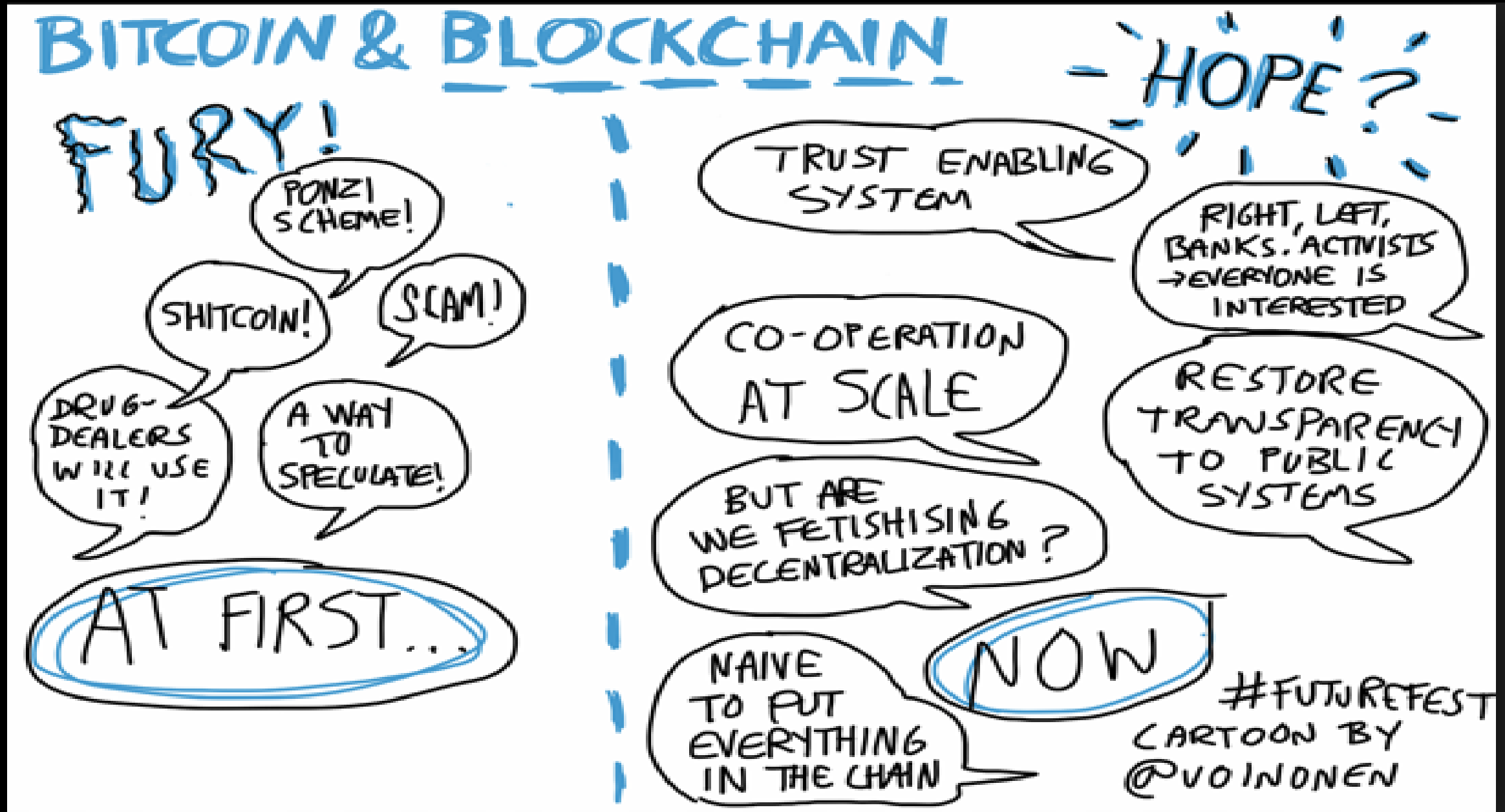
- Blockchain is at the peak of the Gartner Hype Cycle
  - Difficult to alter, credible, complete, obvious, transparent, with evidence of approvals
  - However – the **SIZE** of blockchains may compel companies to use the Cloud!
- Originating Entry still needs validation/corroboration
- Proof of lack of collusion amongst a majority of peer-to-peer nodes
- BC in the Cloud may address basic audit issue of the Cloud: How does the CSU comply with the regulations and trust its critical transaction data to an outsourced cloud with little verifiability?
  - How does BC Cloud computing impact the role of the external auditor?
  - Does BC complexity further hinder the audit of the Cloud?
  - How does the external auditor approach the structure and planning of a BC in the Cloud? (hypothetical approach adopted from KPMG 2013 Cloud audit plan proposal)

Areas for Future Research and Development

- How can the audit standards evolve to provide guidance for auditing BC in the Cloud?
  - Auditors' roles may need to be re-defined
    - Increased emphasis on controls?
    - Standards to enforce audits of smart contracts?
    - What would be the scope of auditing a BC in the Cloud?
  - Does the use of BC in the Cloud change the assessment of the Cloud by the auditor?
    - Will it matter where the BC is located?
  - Does the use of BC mitigate the locational challenge?
  - What would be the differing levels of assurance for *BC Cloud as a Software Service* (BCCSaaS), *BC Cloud Platform as Service* (BCPaaS), and *BC Cloud Infrastructure as Service* (BCIaaS)?
  - What about private cloud versus public cloud and the various forms of BC?
  - What level of assurance would be necessary?

Conclusion

- We examine system requirements for DLT based on Nakomoto's paper
  - Peer-to-peer
  - Transactions publicly announced
  - Single history of the order of the transactions
  - Time stamp server
  - System of proof-of-work
- We map these requirements to the audit issues of data reliability, data security, and transaction transparency
- Steps of integration will need to be considered (Alles et al 2008)
- **Conflict of essential philosophies behind BC and that of auditing: libertarianism of de-centralized system versus extreme regulation from a central authority!!!**


BITCOIN & BLOCKCHAIN
FURY!
PONZI SCHEME!
SHITCOIN!
SCAM!
DRUG-DEALERS WILL USE IT!
A WAY TO SPECULATE!
AT FIRST...
HOPE?
TRUST ENABLING SYSTEM
RIGHT, LEFT, BANKS. ACTIVISTS →EVERYONE IS INTERESTED
CO-OPERATION AT SCALE
RESTORE TRANSPARENCY TO PUBLIC SYSTEMS
BUT ARE WE FETISHISING DECENTRALIZATION?
NOW
NAIVE TO PUT EVERYTHING IN THE CHAIN
#FUTUREFEST
CARTOON BY @VOINONEN