

A REASONABLE ASSURANCE FRAMEWORK FOR DISTRIBUTED LEDGER TECHNOLOGY SYSTEMS: A RISK ASSESSMENT APPROACH

DENIZ APPELBAUM, PHD

MONTCLAIR STATE UNIVERSITY

ROBERT NEHMER, PHD

OAKLAND UNIVERSITY

47TH WCARS, NOVEMBER 8 – 9, 2019

AUDIT CONTEXT: “TRUST BUT VERIFY”

“With all these exciting innovations, it is important to remind ourselves that the advent of emerging technologies does not change the fundamental financial reporting framework. If an emerging technology is being used to meet financial reporting of internal control requirements established by the federal securities laws, then auditors need to understand the design and implementation of that technology.” — PCAOB Board Member, Kathleen Hamm

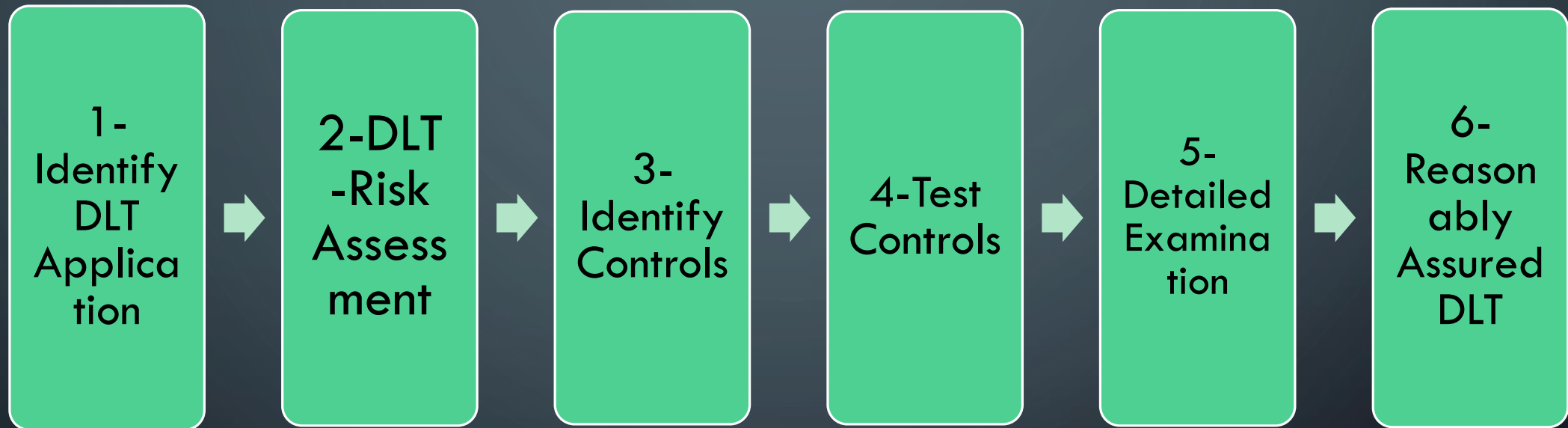
Remarks made during a key presentation at the 43rd World Continuous Auditing & Reporting Symposium, November 2018,

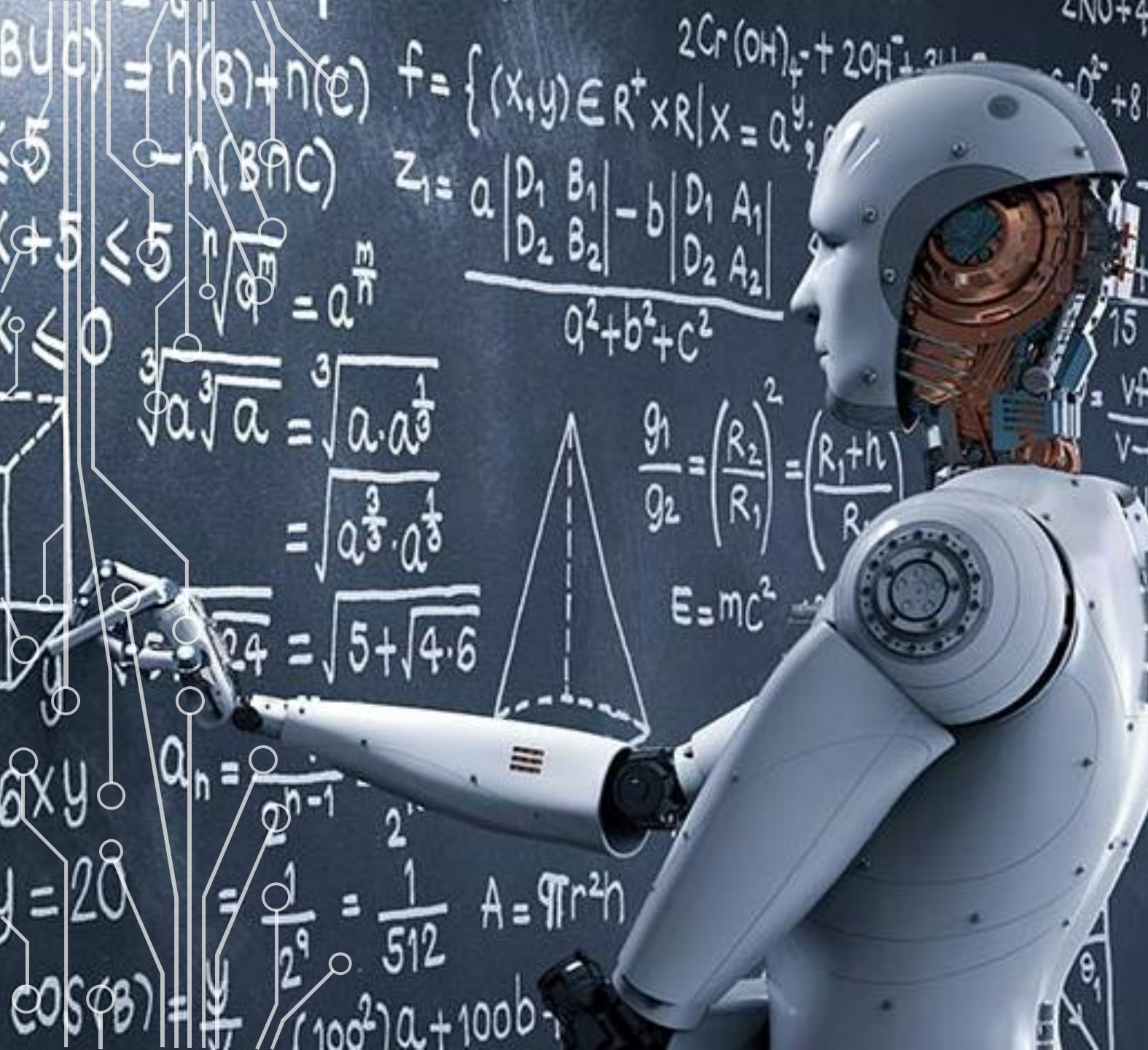
Newark, NJ., USA.

THE DESIGN AND DEVELOPMENT OF AUDIT PROCEDURES IN THE AUDIT OF BLOCKCHAIN

- Standards on evidence collection:
 - “all the information used by the auditor in arriving at the conclusions on which the audit opinion is based.” (SAS No. 106, AICPA 2006; AS No. 15, PCAOB 2010)
 - “The reliability of audit evidence is influenced by its source and by its nature and is dependent on the individual circumstances under which it was obtained.” (SAS No. 106.08, AICPA 2006)
 - Generally, audit evidence is more reliable if it is obtained from sources external to the entity, if it is in documentary form, or if obtained directly from the auditor.” (SAS No. 106.20, AICPA 2006)
 - Continuous evidence gathering

THE ARTIFACT





PHASE ONE – DLT IDENTIFICATION

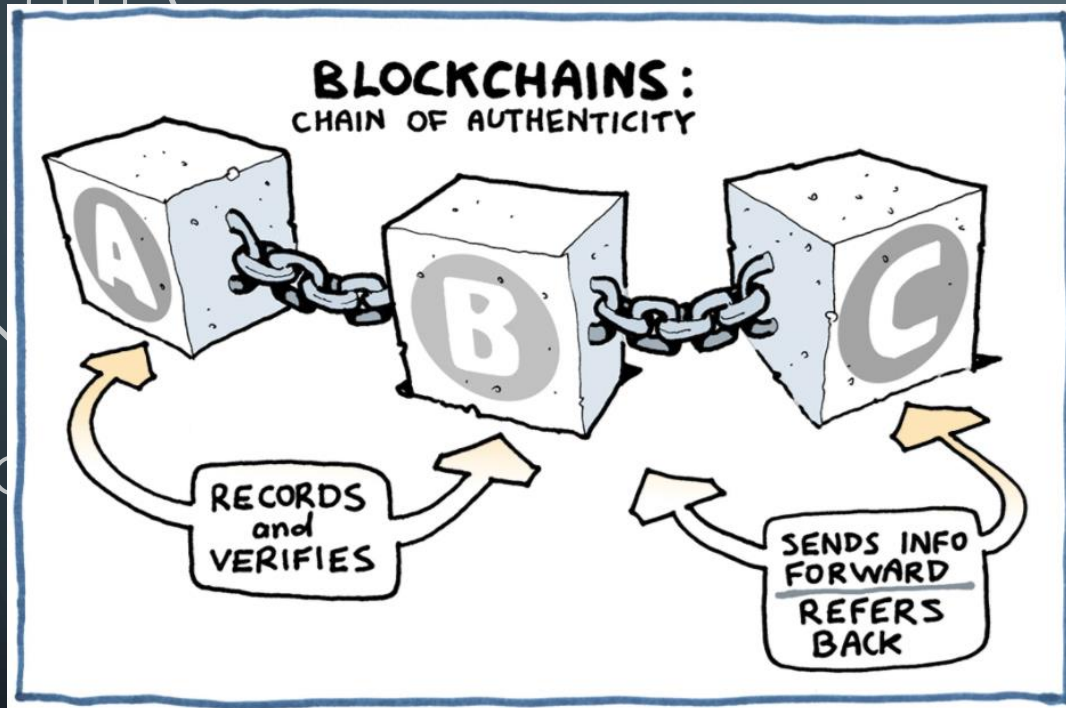
- Identify DLT
- Identify the objective(s)
- Understand the context
 - Who
 - What
 - Where
 - When
 - Why?



COMPONENTS OF DLT RISK



PHASE TWO - DLT RISK ASSESSMENT PROCESS



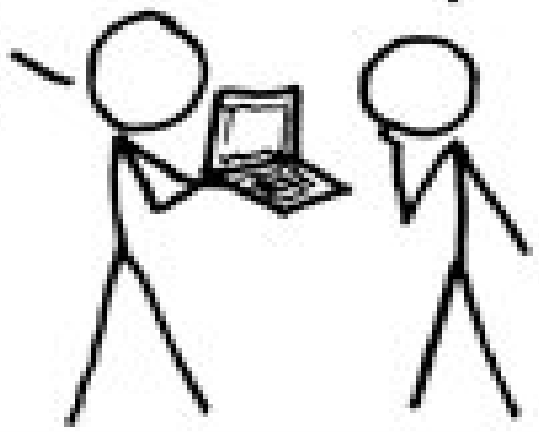
- Information Risk
- Ethics Risk
- Reputation Risk
- Financial Risk
- Decision Risk
- Execution Risk
- Regulatory risk
- Legal Risk
- Complexity Risk* - new risk

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!

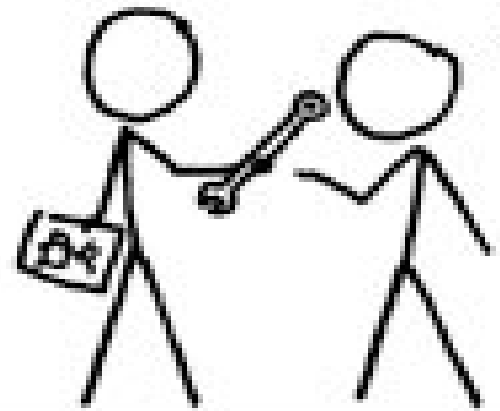
BLAST! OUR
EVIL PLAN
IS FOILED!




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.





PHASE THREE - DLT INTERNAL CONTROLS GUIDELINE

The purpose of an DLT inherent controls guideline is to identify:

- Inherent risks from utilizing DLT in business
 - Threats to organizations arising from DLT
 - Vulnerabilities (internal and external to organizations)
 - The harm or adverse consequence to the firm from DLT
 - The likelihood that harm will occur from DLT
 - Identify the internal controls that have been designed and that are being enforced to mitigate these issues
- 

EVALUATE CONTROLS – EXAMPLE FOR DLT DESIGN

Asset or Process	Inherent DLT Risks	DLT Risks and Vulnerabilities	Likelihood and Impact	IR Risk Score, where 0 is low risk and 1 is high	DLT Internal Controls	CR Risk Score (0 is high risk and 1 is low)
DLT Design & Components	1-not explainable 2-not understandable 3-design encourages fraud 4-error in design 5-not correctable 6-rely on 3 rd party algorithms 7-hacking 8-access controls	1,2-too complex to explain 1,2-design execution is opaque 3-design enforces error or fraud 3-design creates error or fraud 4-design magnifies errors 4-design creates errors 5-design is uncorrectable 5-do not know where corrections should be made 6) lack of design provenance 7) lack of security 8) lack of access controls enforcement	These ratings are DLT application specific		1,2,3,4,5-IT staff receives updated training with emphasis on error correction/fraud detection 1,2,3,4,5-continual efforts are made to convert the DLT to explainable DLT 1,2,3,4,5-reperform the DLT process 6,7-audit the open source/3 rd party platforms (SOC2 type report) 7-business-wide internet security training 8-access permissions embedded in the DLT platform 8-access permissions enforced 100% of the time	



PHASE FOUR: TESTING FOR EXPECTED CONTROLS

Controls to mitigate the following inherent risks specific to blockchains across all applications:

1. Complexity
2. Transparency
3. IT Security Practices
4. Collusion (over 50%)
5. Oracle Paradox
6. Privacy Concerns
7. Hacks/Malware
8. Lack of Authorization
9. 3rd Party Platform Reliance

Persons Control Issue #1: Poor DLT familiarity /IT Staff Expertise

1. Has the IT staff received training in blockchain and smart contracts?
2. Where did this training occur?
3. How did this training occur?
4. Is there a formal measure of competency?
5. When did this training occur?
6. Is this training documented?
7. Has the IT staff received training in blockchain and smart contract coding?
8. Where did this training occur?
9. How did this training occur?
10. Is there a formal measure of competency?
11. When did this training occur?
12. Is this training documented?
13. Has the IT staff received training updates in these areas?
14. Where did this training occur?
15. How did this training occur?
16. Is there a formal measure of competency?
17. Who does the IT staff consult with regarding issues beyond his/her expertise?
18. Has the IT staff hired outside consultants for assistance in resolving issues?
19. How were these experts vetted?
20. Are any individuals that access the blockchain code lacking in training (what are the access controls)?

AUDIT OF BLOCKCHAIN: DETERMINE THEIR EFFECT ON NATURE, TIMING, PROCEDURES

- **PHASE FIVE: Detailed Examination:**

- Sample or Exceptional Exceptions (Issa et al 2018)

- **PHASE SIX: Reasonably Assure the DLT system**

- Timing: continuous or batch?

- Procedures:

- Continuous monitoring?
- Batch?
- Ad hoc? Sampling?

- Depth?

- Physical Verifications? (smart contracts)

DEMONSTRATION OF THE SOLUTION

- Asset or Process: Persons
- Inherent DLT Risk (IR): Lack of DLT Expertise
- Threat/Vulnerability: Poor Understanding of DLT
- Likelihood and Impact: Moderate to high likelihood & moderate to high impact
- Internal Controls DLT Risk (CR): IT Staff Expertise
- The auditor will evaluate the IR based on the Threat/Vulnerability and Likelihood/Impact scores, which should be closer to 1 if there is a high likelihood if a material misstatement can occur due to the use of DLT, and closer to 0 if there is a lesser likelihood that a material misstatement can occur. The auditor could use the questionnaire presented earlier to evaluate the CR score, where the lower number indicates a likelihood that the controls will not detect a material misstatement due to the use of DLT and the higher number indicates the opposite condition. For Control Risk, after labeling each CR question with a decimal between 0 and 1, the auditor will compute the average score. For Inherent Risk, the auditor will score Threat, Vulnerability, Likelihood, and Impact with a score between 0 and 1 and compute the average.

DEMONSTRATION OF THE SOLUTION

- Asset or Process: People
 - Inherent Risk: Lack of DLT Expertise
 - Threat: .5
 - Vulnerability: .4
 - Likelihood: .7
 - Impact: .8
 - Average IR score: 0.6
- (where 0 is low, 1 is high)

Control Risk: IT Staff Expertise (where 1 is highly unlikely that a material misstatement will occur)

1. Has the IT staff received training in blockchain and smart contracts? .9
2. Where did this training occur? .9
3. How did this training occur? .9
4. Is there a formal measure of competency? .5
5. When did this training occur? .3
6. Is this training documented? .9
7. Has the IT staff received training in blockchain and smart contract coding? .4
8. Where did this training occur? .4
9. How did this training occur? .8
10. Is there a formal measure of competency? .9
11. When did this training occur? .3
12. Is this training documented? 1.0
13. Has the IT staff received training updates in these areas? .4
14. Where did this training occur? .4
15. How did this training occur? .4
16. Is there a formal measure of competency? .9
17. Who does the IT staff consult with regarding issues beyond his/her expertise? .8
18. Has the IT staff hired outside consultants for assistance in resolving issues? .8
19. How were these experts vetted? .5
20. Are any individuals that access the blockchain code lacking in training (what are the access controls)? .1

AVERAGE CR SCORE: 0.63

DEMONSTRATION OF THE SOLUTION

Risk score for this DLT application regarding Persons and their training:

$$\begin{aligned} \text{AR} &= \text{IR} \times \text{CR} \times \text{DR} \\ 0.05 &= 0.6 \times 0.63 \times 0.132 \end{aligned}$$

Where $[\text{DR} = \text{AR} / (\text{IR} \times \text{CR})]$.

EVALUATION OF THE SOLUTION

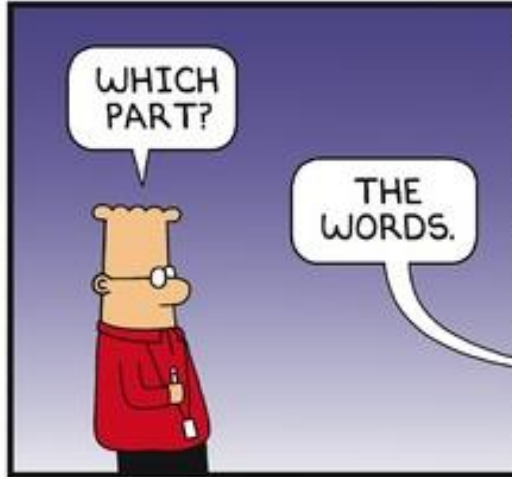
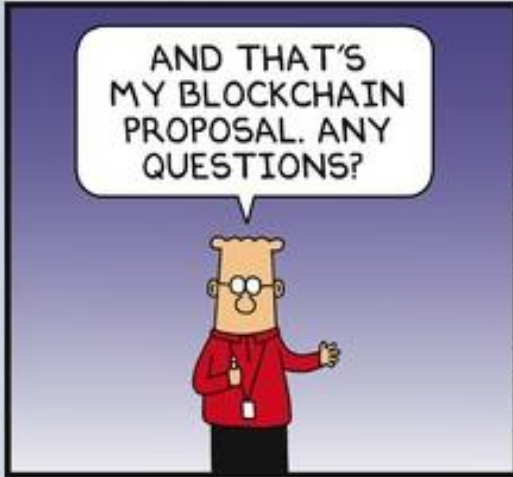
- Grounded in prevalent audit methodology
- Demonstration of artifact is hypothetical
- Biggest factor may be the risk of the accounts or disclosures which are affected by disclosures from DLT systems
- Auditing “around” DLT systems?
- Will DLT have an impact on financial reporting systems?

COMMUNICATION OF THE PROBLEM

- The audit profession needs to adjust itself to these emerging technologies
- Wide-scale adoption of DLTs may take some time (Alles et al 2008)

CONCLUDING THOUGHTS

- Generalizable Framework based on NIST & audit procedures
- Complex technologies need to be audited if they impact numbers reported in the financial statements of public companies
- This paper contributes to the research in the DLT domain



Twitter: @scottadamssays

© 2019 Scott Adams, Inc./Dist. by Andrews McMeel

dilbert.com

11-3-19



THANK YOU!

CONTACT DETAILS

appelbaumd@montclair.edu

nehmer@oakland.edu