CSAMN cloud security alliance® Minnesota Chapter

GRC as a Service LLC

Solving the Data at Rest Problem

Blockchain Confidentiality and Privacy for Cloud Infrastructure

Michael Solomon, PhD, Principal Consultant

ms@grc-as-a-service.com

Cell: 770-403-6005

Thank you to our sponsor!

Microsoft

Speaker Bio

- **Michael Solomon, PhD**
- GRC as a Service, LLC Principal Consultant / Solomon Consulting Inc, President and Principal consultant
- CISSP®, CISM®, PMP®, PenTest+®
- Professor of CyberSecurity and Global Business with Blockchain Technology graduate programs, University of the Cumberlands, Williamsburg, KY
- Specializes in GRC Consulting for Complex Multi-Reg Environments with “Sensitive” Data
- Book Author (textbooks and cert prep), Cybersecurity and Project Management training video architect
- Private pilot and Star Wars miniatures games enthusiast

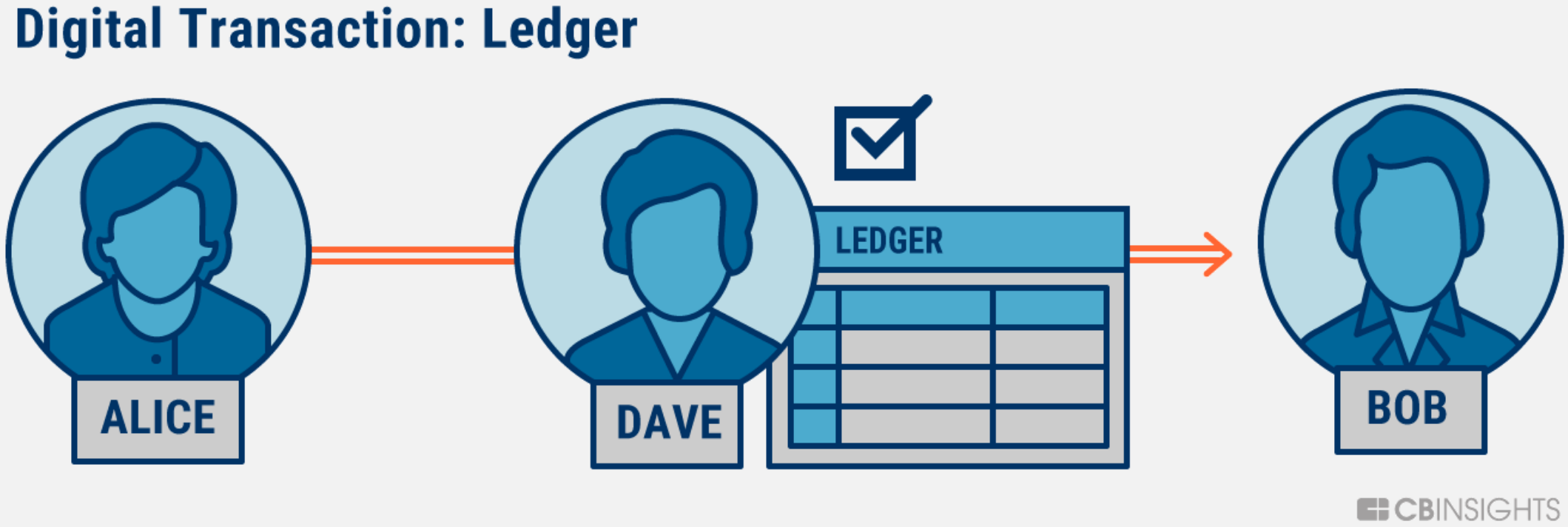
Agenda

- What is blockchain?
- Blockchain and disruption?
- Confidentiality versus privacy
- Can blockchain solve the confidentiality and privacy problem?
- How do you implement it?
- Where to start?

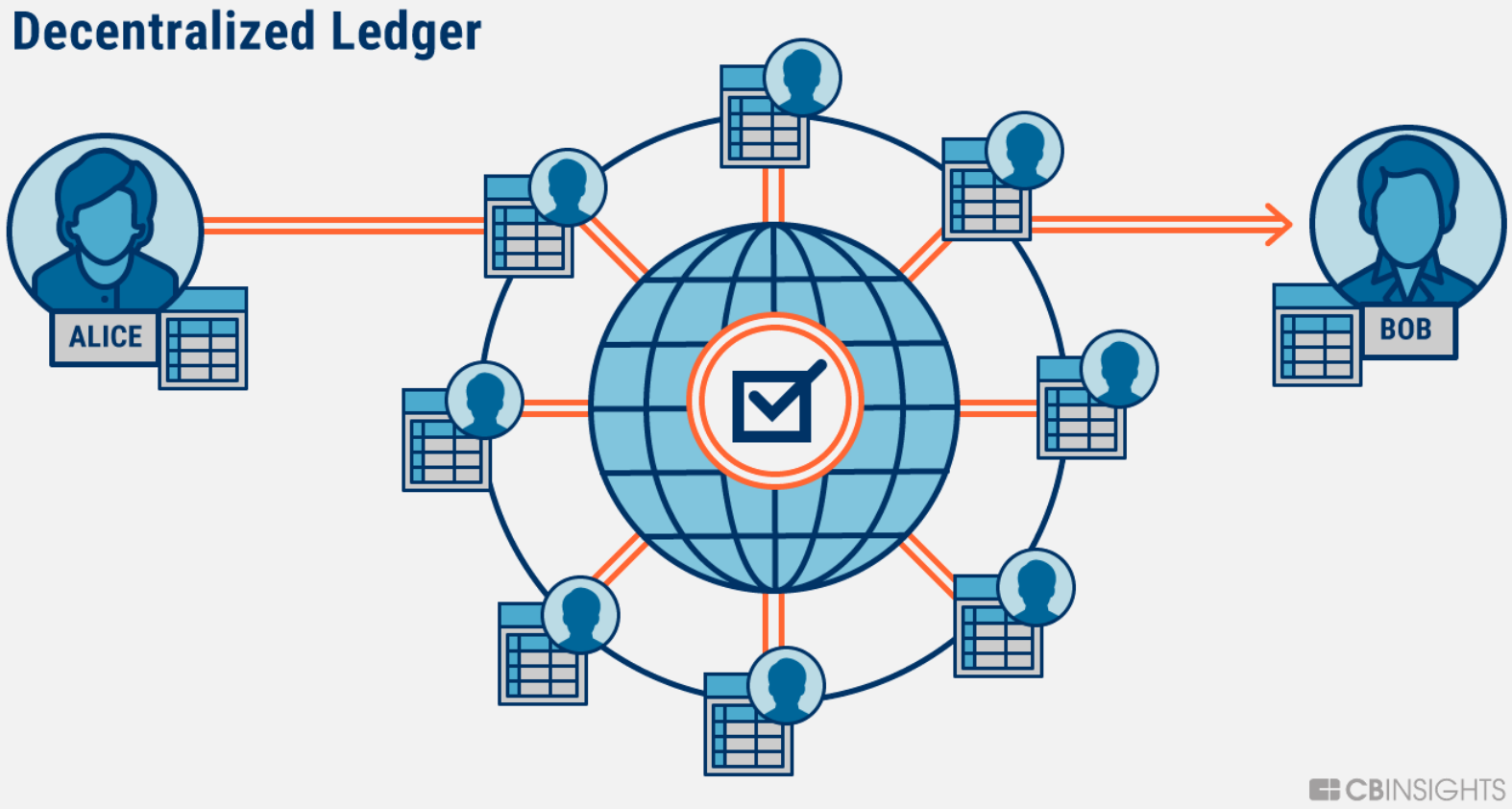
What is blockchain?

- Data ledgers
  - Traditional
  - Distributed
- How blockchain works
- What does blockchain mean?
- How can we enforce rules?
  - Or is this the wild west?

Traditional ledger – what we do today



Decentralized ledger – where we're headed



Quick Survey Questionnaire

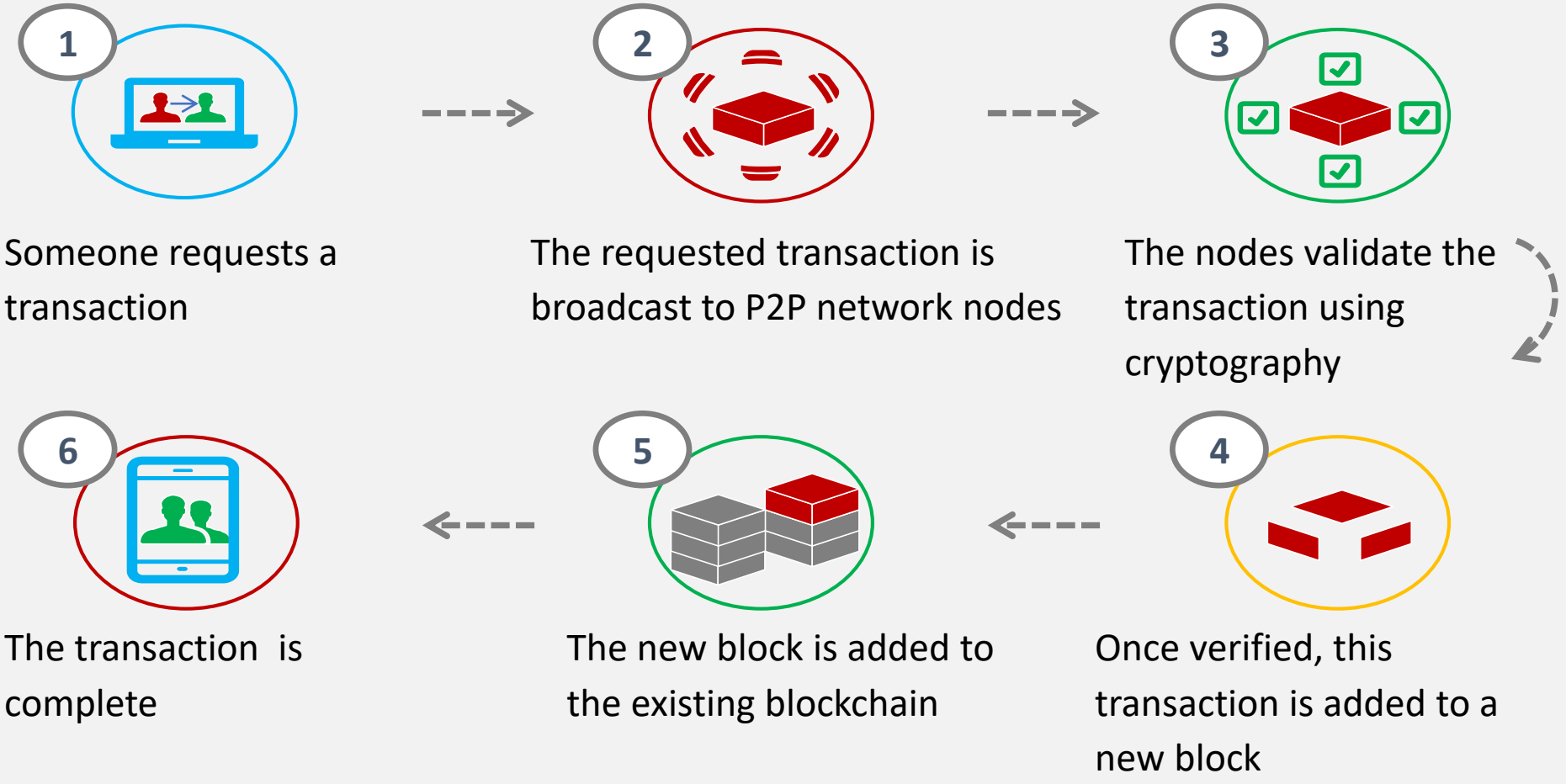
Q1: Are you currently using blockchain?

Q2: Are you using: Private, Public, Hybrid?

Q3: What problems do you see with distributing your data?

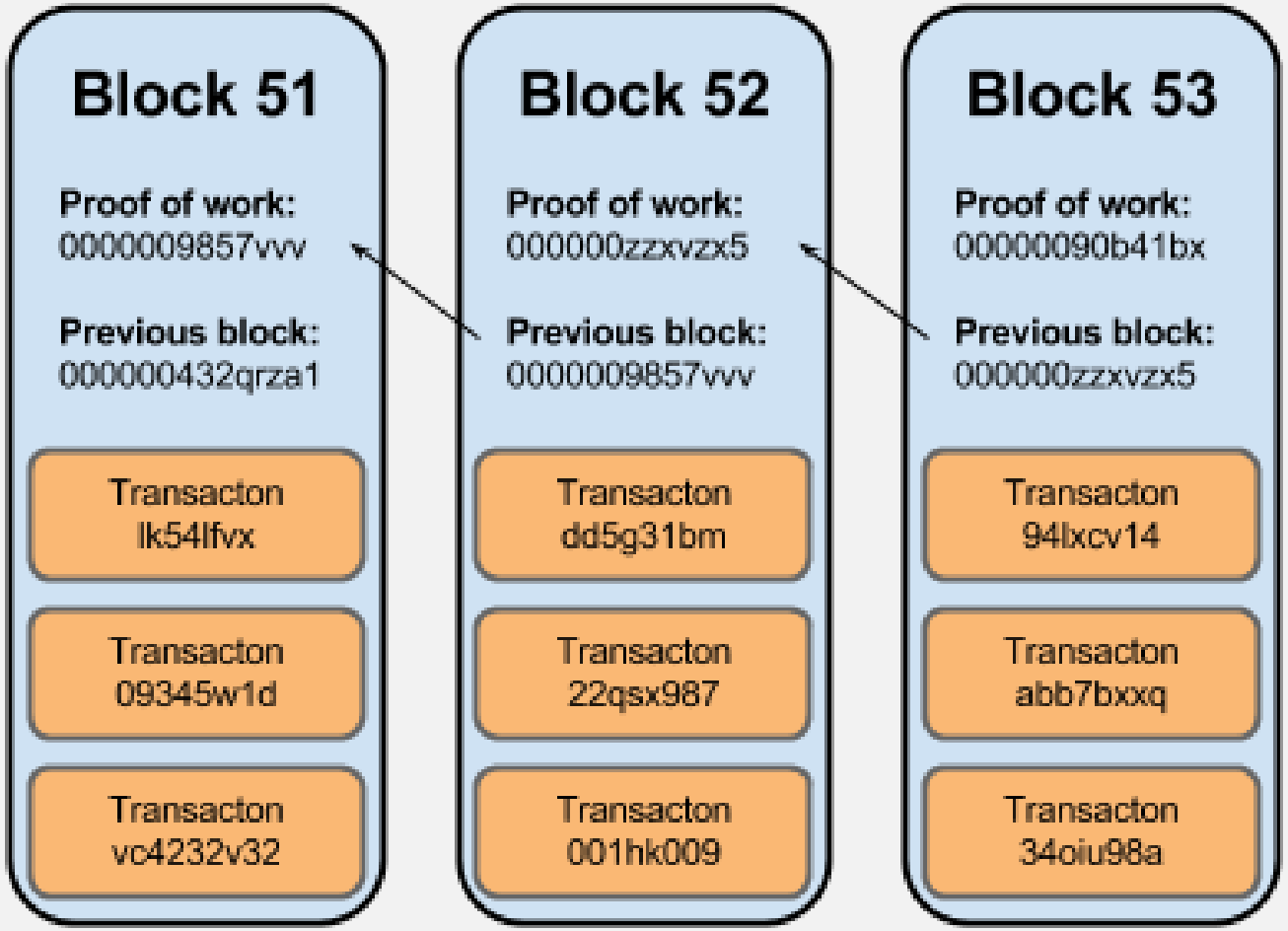
Q4: What business drivers led you to blockchain?

How blockchain works



What does blockchain mean?

A chain of blocks



Another Quick Survey Questionnaire

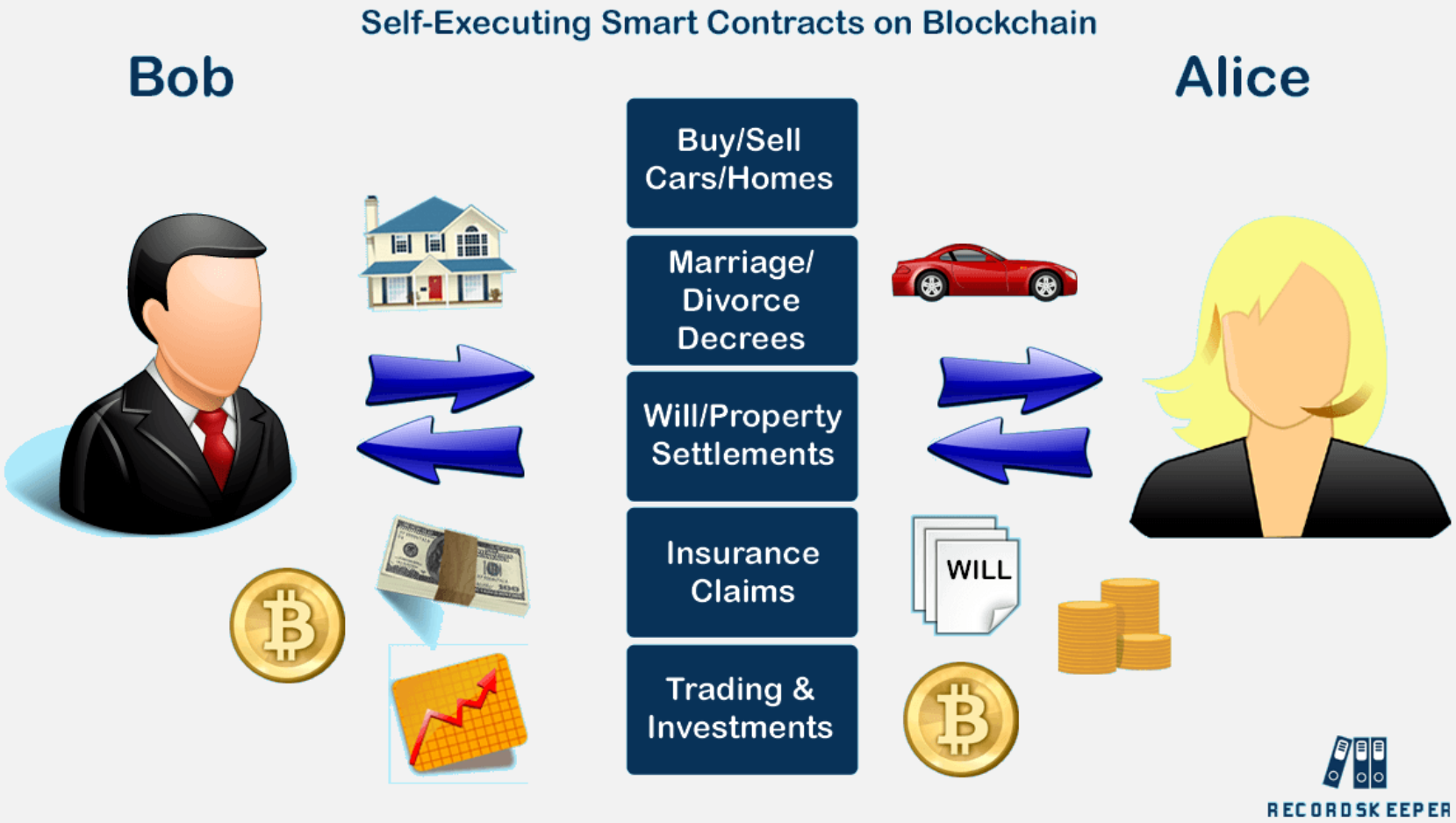
Q1: What rules should govern P2P sales? (i.e. cars)

Q2: Can you think of any middlemen that blockchain can eliminate?

Q3: What are some of the risks of putting rules on a blockchain?

Q4: What are some advantages of putting rules on a blockchain?

Smart contracts – the “rules”



“You've got to disrupt or be disrupted … [it's about moving] the sources of innovation … from being something you do on the fringe to something you have to do mainline … [and refocusing] on leaders who could work **horizontally** together as opposed to in **silos**” (Chambers, 2016)

- John Chambers, Cisco

Blockchain is disruptive

- Disruptive doesn't mean ***everything*** changes
  - It means ***some*** things change (and maybe a lot)
  - It's all about balance

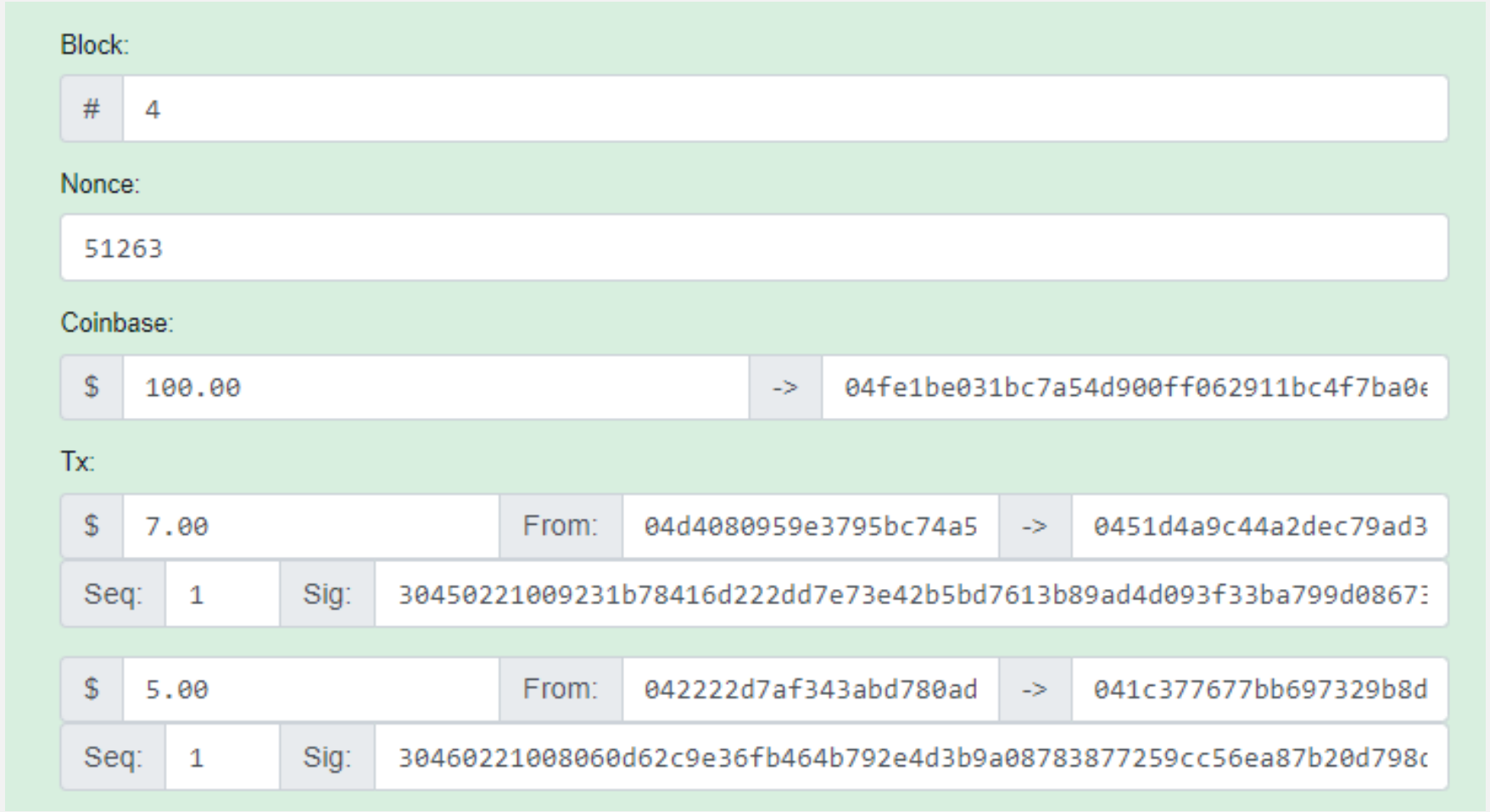
"The basic premise of organizational ambidexterity theory is that to maintain long-term adaptability and viability, organizations must balance the tension between the need to ***innovate*** and the need to ***produce***"

(Duncan, 1976; Tushman and O'Reilly, 1996).

Yet Another Quick Survey Questionnaire

Q1: Is disruption a risk?

Who are Bob and Alice?



Confidentiality and privacy – what's the difference?

- **Confidentiality** is about the data
  - Intention is to keep data secret
  - Allow access only to authorized users

- **Privacy** is about the individual
  - Access to the person (or organization)
  - Appropriate use of information
  - Being free from public attention
  - Ability to be left alone

Compliance Laws That Impact “Privacy”

HIPAA Privacy Rule

EU GDPR Privacy

State Privacy Laws

DFARS CUI Data

COPPA- Kids < 13

FERPA - Students

FACTA – Identity

FISMA – Moderate

Anonymization is not a solution

- In 2000, Latanya Sweeney reported a disturbing finding
- 87 percent of all Americans can be uniquely identified by only THREE pieces of information
  - ZIP code
  - Birthdate
  - Gender

+

+

=

A growing privacy problem

- Individuals
  - Personal info = $$$
  - PHI, PII, behavior ← most concerning
  - Anonymity = Unicorns
  - This isn't 1984
- Organizations
  - Intellectual property
  - Customer behavior
- Big Data
  - Analytics (Data Science) – we used to call that creeping
  - Sanctioned profiling

Can blockchain provide confidentiality?

- Public / Permissionless (i.e. Bitcoin, Ethereum) not so much
  - All data is out there (encryption can help)
  - Some research in this area (Attribute-Based Encryption)

- Private / Permissioned (i.e. Hyperledger Fabric, Ethereum Enterprise) yes
  - Attribute-Based Access Control
  - Encryption (regulator role maintains key)
  - Private channel data (RBAC w/”need to know”)
  - Private transactions
  - Zero-knowledge proof (ZKP)

Can blockchain provide privacy?

- Public / Permissionless (i.e. Bitcoin, Ethereum) not so much
  - All data is out there
  - Encryption doesn't help

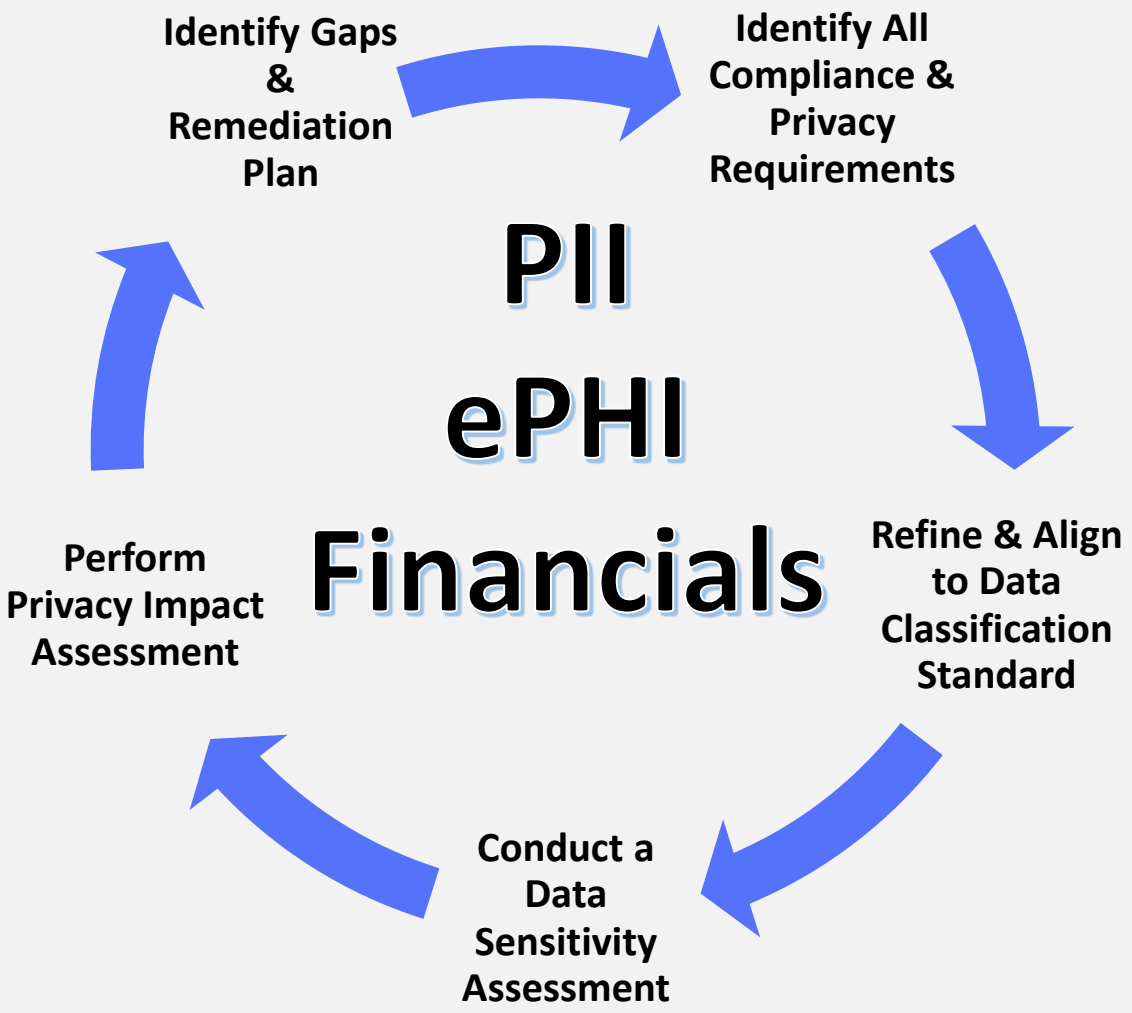
- Private / Permissioned (i.e. Hyperledger Fabric, Ethereum Enterprise) yes
  - Central control of smart contracts
  - Can enforce privacy filters (for statistical queries)
    - Differential privacy
    - K-anonymity / l-diversity / t-closeness

Privacy Impact Assessment - Scope

Image From: Copyright © EasyCloud Consultants Pvt. Ltd.

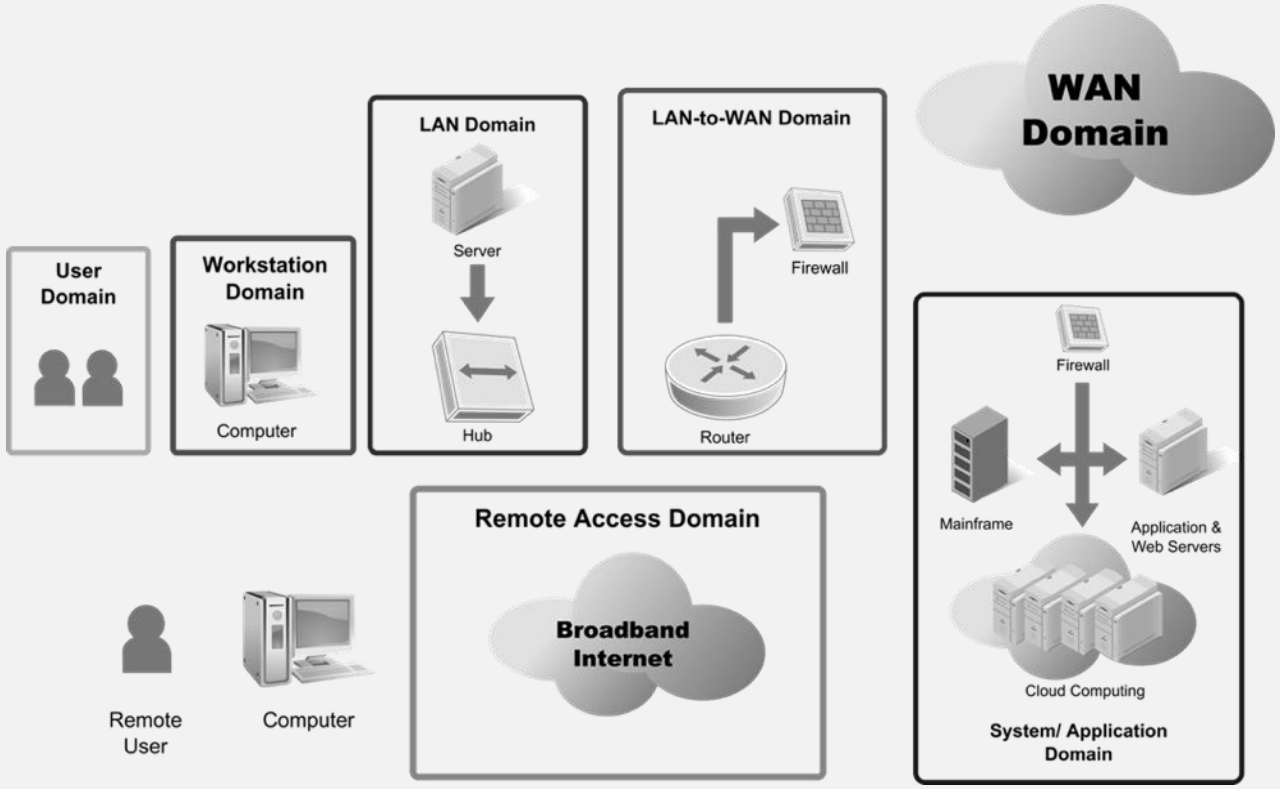
- Identify WHO is Accountable for Privacy
- Confirm a Data Classification Policy, Standard, & Procedure Definition Exists
- Verify who has access to “Sensitive” data (HR Roster), enable audit trails & logs
- Assess organizational use of access, storage, & transmission of “Sensitive” data
- Confirm use of encryption as rest and in transit for all “Sensitive” data use, storage, and transmission
- Document “Sensitive” data work-flows and traffic flows throughout
- Is your CSP – ISO27001, ***ISO27018*** “Certified”?

Privacy Impact Assessment - Approach

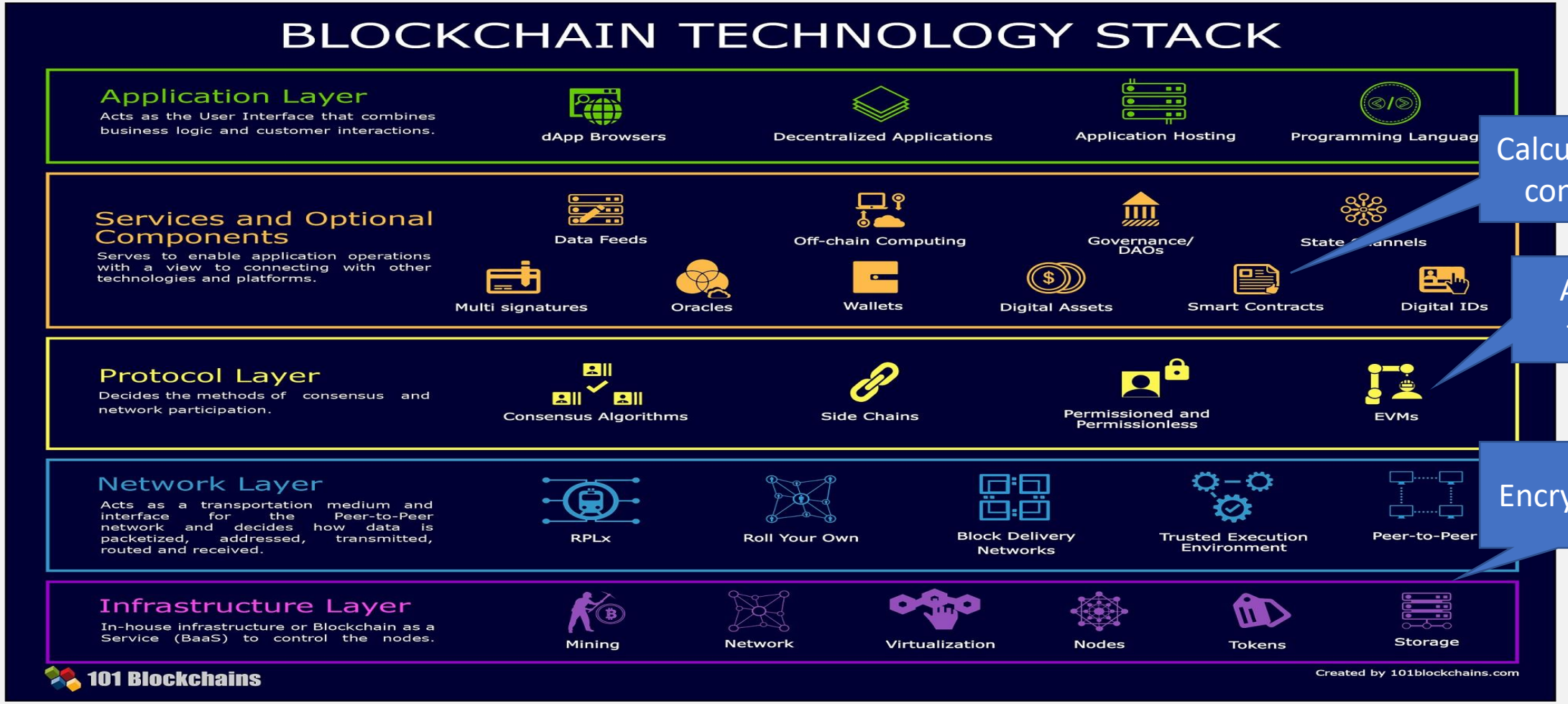


Blockchain innovation - Approach

- Align your BIA and IRP with innovation targets
  - Start with non-critical data and processes
- Perform a ”Sensitive” data treasure hunt
- Ensure data is encrypted or protected appropriately
- Migrate incrementally
  - Test
  - Test
  - Test



A new technology stack

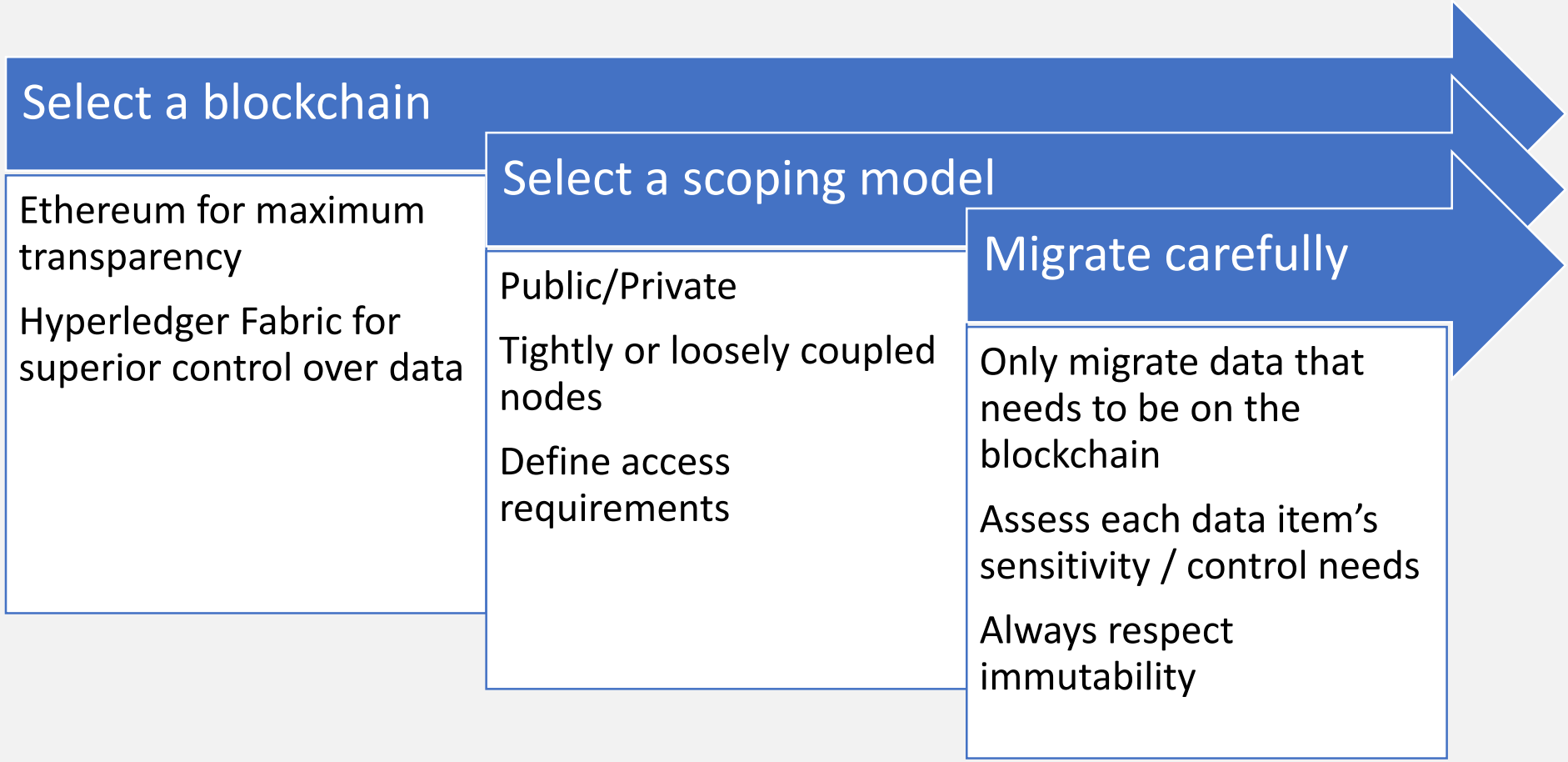


Calculation control

Access filters

Encryption

How do you implement this?



Where do we start?

- Learn about blockchain application (do this first)
  - Explore existing projects
  - Examine implementations
    - Public / general - Ethereum
    - Industry / private – Hyperledger Fabric
- Conduct a Business Impact Analysis (BIA)
- Identify innovation opportunities (don’t force it!)
  - Align PoCs blockchain strengths and innovation opportunities
  - Stay away from business critical processes (at least at first)

Menu ORACLE Ricerca Registrati Paese/Regione Contatta

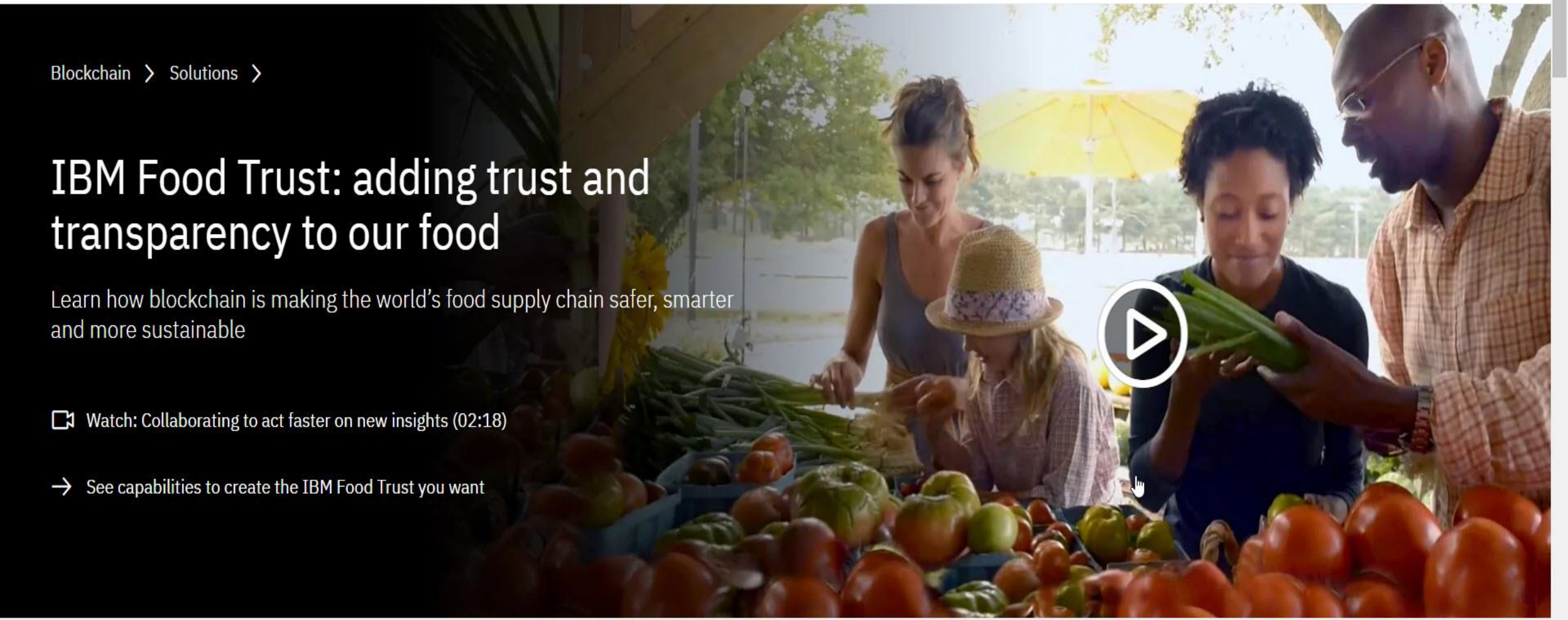
Oracle Italia / Corporate / Customer Stories /

Oracle Customer Success — Certified Origins Italia Srl

Certified Origins Italia Enhances Supply Chain Traceability and Trust with Oracle Blockchain

Share

> We believe that buyers and growers deserve a world in which authenticity and quality are not only valued but verified. Managing traceability with blockchain technology is the logical progression of the whole traceability process for our Bellucci Premium Extra Virgin Olive Oil. We are using Oracle Blockchain to track shipments of our EVOO from our bottling facility in Italy to the port of arrival in the



IBM Food Trust: adding trust and transparency to our food

Learn how blockchain is making the world's food supply chain safer, smarter and more sustainable

Watch: Collaborating to act faster on new insights (02:18)

→ See capabilities to create the IBM Food Trust you want

How we can improve food for all

IBM Food Trust™ uses blockchain technology to create unprecedented visibility and accountability in the food supply. It's the only network of its kind to connect growers, processors, distributors, and retailers through a permissioned, permanent and shared record of food system data.

Let's talk

Webjet uses blockchain to simplify transaction disputes in the travel industry

March 30, 2018

Print

The hotel booking ecosystem is complex, decentralized, and high volume, with millions of transactions per day. To streamline processes and reduce industry-wide costs, Webjet uses blockchain to power Rezchain, a data reconciliation service for the travel industry. With Rezchain, the company has seen a 90 percent reduction in losses associated with transaction disputes across its internal brands. And as more external partners join the Rezchain network, Webjet can extend those efficiencies throughout the industry.

Customer

Webjet

Learn More

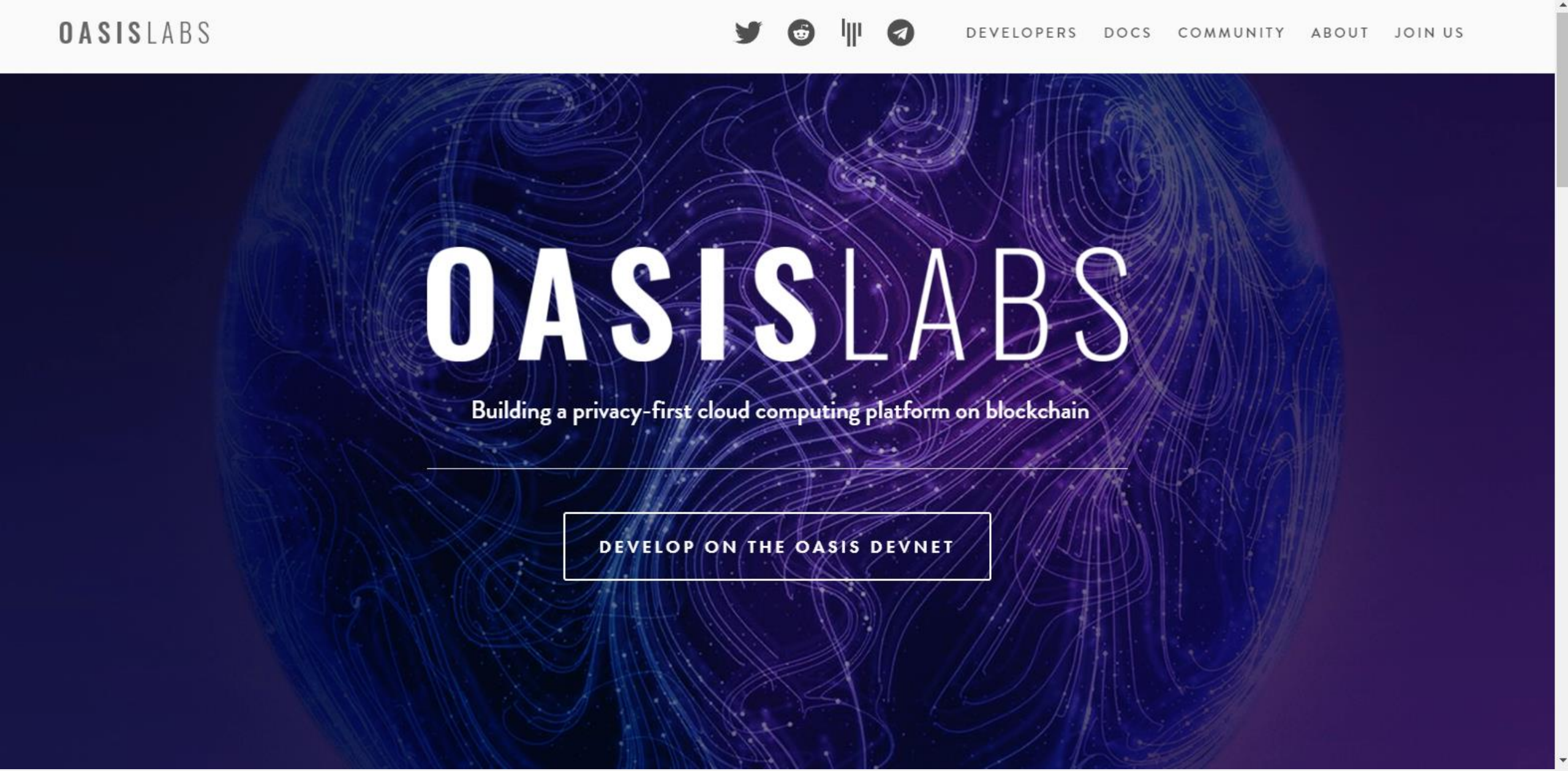
- Blockchain on Microsoft Azure
- Azure Table Storage
- Azure Container Service
- Power BI

Oracle Customer Success — Alpha Acid Brewing Company, LLC

Alpha Acid Brewing Merges Blockchain and Beer with Oracle

Share

> With Oracle Blockchain solutions, we can track materials and ingredients from our suppliers and analyze sensor data from the production process. Oracle Blockchain Platform tracks where we are getting the highest quality hops, malt, and yeast, and enables us to create a strong narrative around our products.


OASISLABS
DEVELOPERS
DOCS
COMMUNITY
ABOUT
JOIN US
OASISLABS
Building a privacy-first cloud computing platform on blockchain
DEVELOP ON THE OASIS DEVNET


QUESTIONS
poll
asking
query
ask
reply
questions
q&a
challenge
investigation
confusion
problem
answers
interrogation
who
what
how
when
puzzle

Thank You for Participating in Today's Event!

Heads Up! Next Month's Event is on…

How to Secure Access Controls to Your Cloud Applications & Sensitive Data

References

- Chambers (2016). http://www.mckinsey.com/industries/high-tech/our-insights/ciscosjohn-chambers-on-the-digital-era.
- Duncan, R. (1976). The ambidextrous organization: Designing dual structures for innovation. In R. H. Killman, L. R. Pondy, & D. Sleven (Eds.). The management of organization (pp. 167–188). New York: North Holland.
- Solomon, M. (2019). *Ethereum for dummies*. John Wiley & Sons.
- Tushman, M. L., & O'Reilly, C. A., III (1996). Ambidextrous organizations: Managing evolutionary and revolutionary change. California Management Review, 38(4), 8–30.