data amplified™

PARIS 2017

THE FUTURE OF BUSINESS REPORTING

XBRL Cybersecurity Practice

speaker:

Herm Fischer

Developer, Mark V Systems

Cybersecurity practices with XBRL

- XBRL Current Practice
  - Submission requirements on filers
- Arelle features
  - Secure server support
- Data content security, blockchain
- Human Practices
  - 😎

First, pay attention to news articles

- Know the published exploits
  - Credit bureaus, government agencies, firms
  - Awareness of features exploited elsewhere
- Keep up to date
  - Servers, components, OSes, infrastructures
- Plan for contingencies
  - Emergency upgrades, hack & ransom recovery

What should XBRL do?

- Safe practices at authorities
- Safe practices on private servers
- Use XBRL features (CEN, EIOPA, etc)
- Available technology (OIM, blockchain, DB)

Legacy XBRL Practices

- HTML feature restrictions (inline & text block)
  - No active content (*script, applets, links)
  - Restricted HTML tags, style
    - .gif/.jpg in filing locally or authority archive
- Only linkbases: -pre, -cal, -def, -lab, -ref
  - No table or formula linkbases

Legacy Servers

- These are not XBRL-specific
  - Awareness of news and exploits
  - Hackers are smart and motivated
  - Respond promptly

Arelle Practice

- Pre-filing security when web serving
  - Submission by posted zip stream
  - Returns results in zip stream on same socket
  - Only-in-memory processing
  - Nothing ever stored on any file system
- Storing something on file system?
  - 😟?😃

XBRL Features

- Semantic securing XBRL data
  - Detect tampered instance data
    - EIOPA T4U md5 summed instance semantics
      - Adapt blockchain to XBRL semantics
- CEN security of Eurofiling work group
  - Physical security of contents
    - Physical or blockchain?
  - Migrate to XBRL instance packages (OIM)

Hackers are smart and well motivated

- Any OS may be compromised
    - May be listeners on sockets
    - May be scanners on file systems
        - Any virus checker can be compromised
- Any client browser may be compromised
    - Client virus checkers

Virus checker vulnerability

- Smart pattern detection in file system
  - Really, it does sniff for patterns in files
- Hackability of virus checking process
  - May be compromised remote from vendor

Information security

- Assurance that data is intact and as-reported
  - Detect tinkering with content
- Dealing with large collections and databases
  - Ensure values from instances where queried across large sets of data

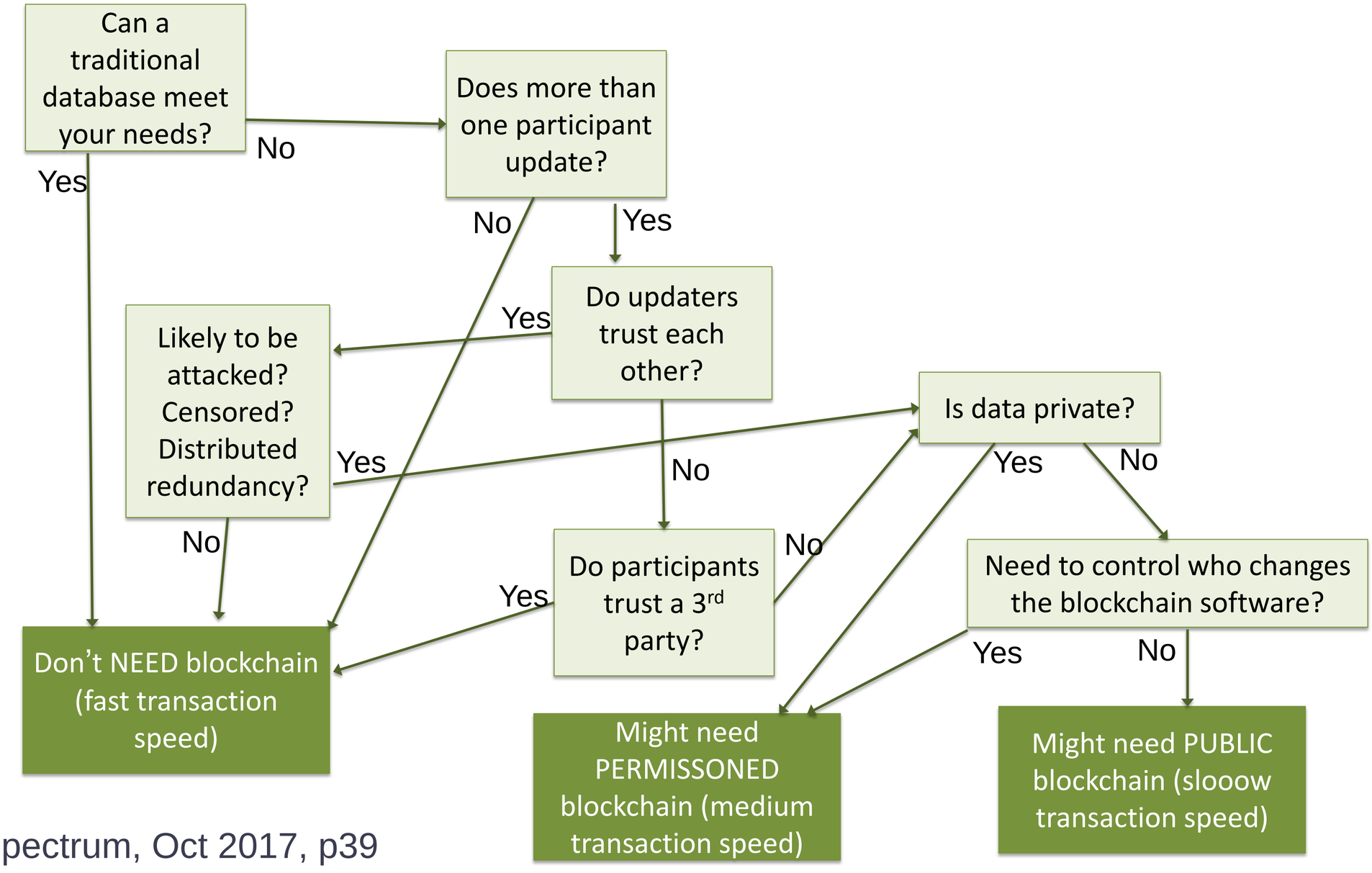
Detect instance tampering

- Assure semantic contents valid
  - Media and stream independent (Traditional XBRL, OIM XBRL, Database)
  - Allow ID changes, DB shredding, instance merging
- Arelle md5 sum of fact & aspect values
  - Where do you put that?

Blockchain for XBRL

- What it is
  - Log with data, who produced, who modified
  - Allows validation, re-filing, amending…
- Not your ‘bitcoin blockchain’
  - Bitcoin is *anonymous*, XBRL is *permissioned*
  - Bitcoin payload is 40b, XBRL is 50M-10G
    - Can protect XBRL’s metadata and checksums
- *Do YOU need blockchain?*

XBRL blockchain criteria



IEEE Spectrum, Oct 2017, p39

Blockchain security for XBRL

- Permissioned (not anonymous)
- Authoritatively validated
- Logged
- Metadata vs. facts and aspects
    - Large collections
    - Databases
    - Re-filing and amending data

Human practices