Due Diligence of Blockchain-Based TE Solutions

Session: The Power of Blockchain

Richard Shandross
Associate Director
Navigant Consulting
Blockchain’s strong points for TE

- Designed for use by many parties from different organizations
- Transaction-oriented
- Distributed nature provides robustness and resilience
- *Smart contracts* allow automation to be embedded within the ledger
- Tokens can be created and assigned exchangeable value
- Being developed in parallel for many functions relevant to TE (finance, billing, payment…)

*Provisional characteristics:*

- Can eliminate intermediate parties that create expense, inefficiency, or time delays … depending on the type and degree of decentralization
- Strong transaction and information integrity, including data immutability … when combined with appropriate shared-validation methods and governance schemes
Blockchain is rarely a *whole* solution
Four-step due diligence process

1. Benefit fit
2. Compatibility check
3. Blockchain property verification
4. Vulnerability screening
**Benefit fit**

- Break down the application into constituent processes and/or functions
- Enumerate blockchain (BC) intrinsic strengths
- Find components of the application that overlap with strengths of blockchain
- Compare BC to existing technologies and solutions
- Identify where BC can improve on existing technologies

**Compatibility check**

- Check the fit into system architecture
- Investigate the usage in practice
- If decentralization really what you want or need? What type of decentralization?
- Check for side effects
  - Rigid time structure of consensus
  - Data immutability headaches
  - Inadequacy of BC as a database
- Does the underlying BC system have transaction fees?
Property check

• Enumerate the BC properties you are relying on
• Study the solution architecture
  – BC properties are not universal – they are emergent characteristics of the architecture!
• How will the system evolve over time as it gets implemented?
  – NB reduction in Bitcoin decentralization due to mining pools
  – What will be involved in making upgrades or other needed changes to the system over time?

Vulnerability screening

• Identify the attack vectors and modes
  – IT compromise
  – Attacks from within
  – Malware and illegal behavior in the metadata
  – Smart contract issues
  – Infrastructure connections and their unintended vulnerabilities
• Evaluate the strength of the solution under both plausible and currently implausible circumstances