Imperial College London

Governed Blockchains: Trading off Cost, Security, Availability, and Resiliency

Michael Huth

To Prove or Not to Prove Work?

honeybadgerofmoney.com

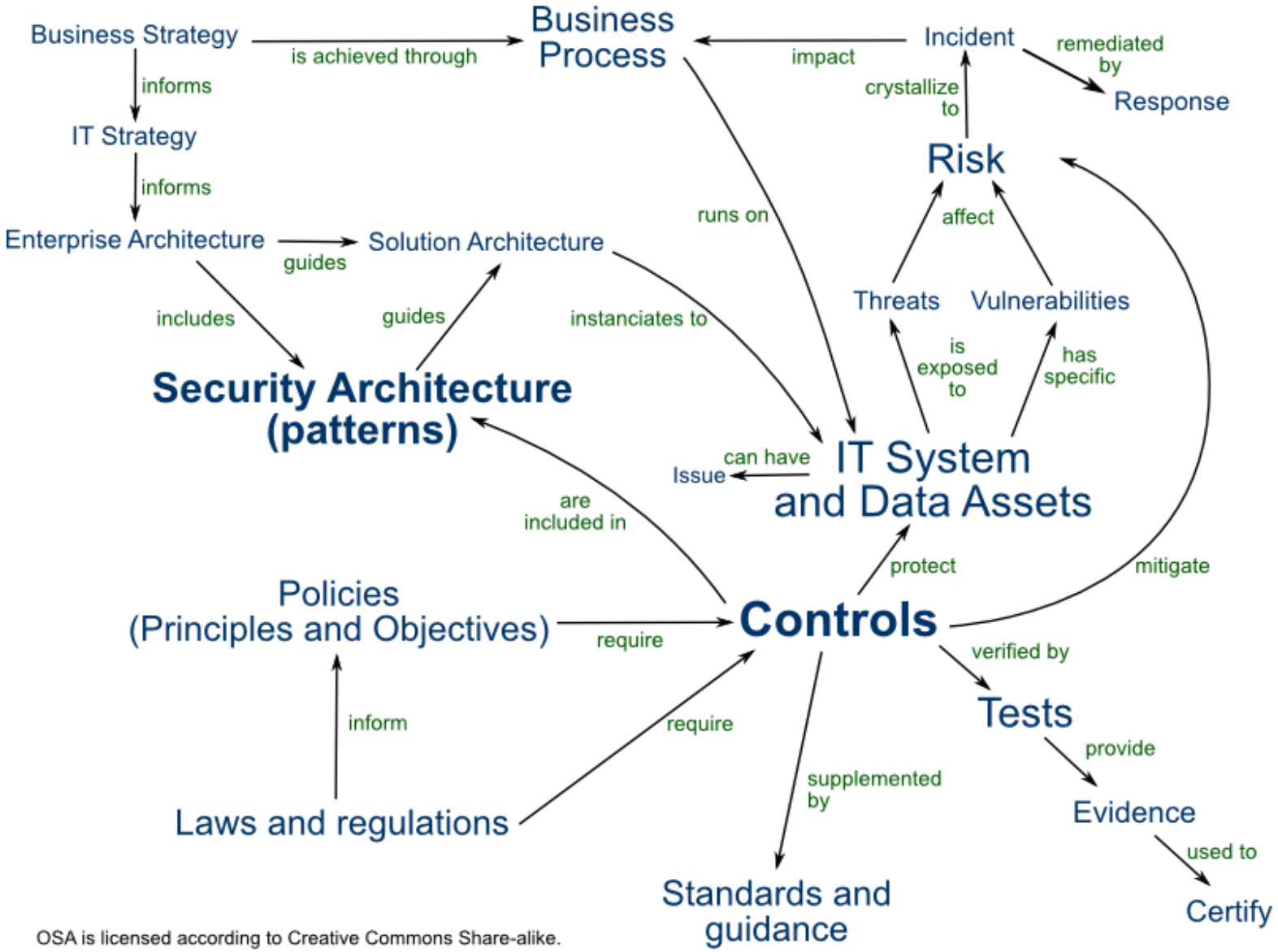
Blockchain: Revolution or Reformation? Governance Issues

wikipedia.org

Eventual Consensus and Smart Contracts

coinreserve.com

Blockchains as a Service



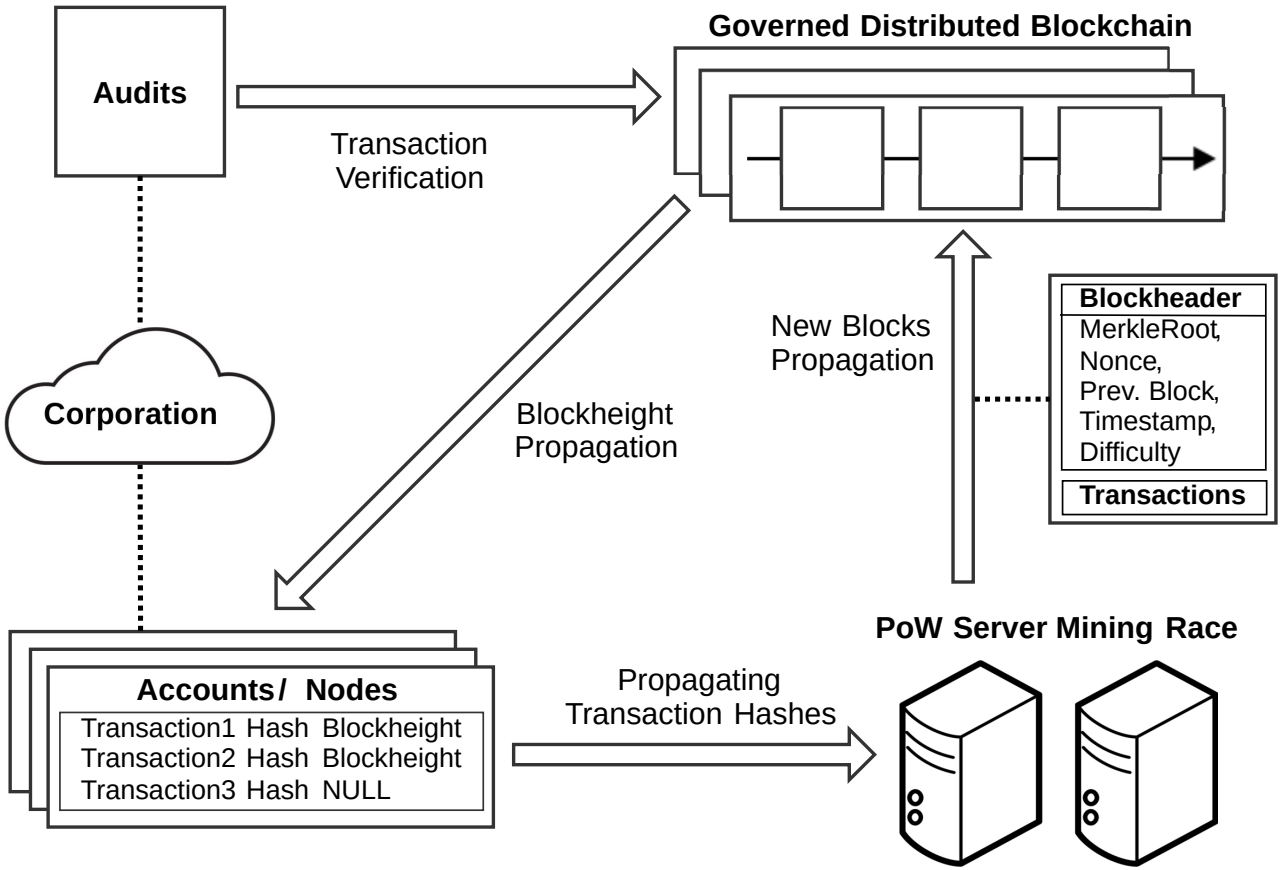
Research Paper on Governed Proof of Work

Optimizing Governed Blockchains for Financial Process Authentications

Leif-Nissen Lundbaek,
Andrea Callia D'Iddio,
Michael Huth

https://arxiv.org/abs/1612.00407

Governed Domain-Specific Blockchains: a Use Case



https://arxiv.org/abs/1612.00407

Proof of Work: Optimize cost, security, availability, resiliency

$$
\begin{aligned}
s_l &\leq s \leq s_u \qquad d_l \leq d \leq d_u \qquad r_l \leq r \leq r_u \qquad \lambda = \lfloor 2^r/s \rfloor \\
y &= (1-2^{-d})^s \qquad z = (1-2^{-d})^{\lfloor \mu/T \rfloor} \qquad 0 \leq \lfloor \mu/T \rfloor \\
\epsilon &\geq y^{\lambda+1} \qquad \lceil (th/T) - 1 \rceil < \lambda \qquad 0 < \lfloor (th'/T) - 1 \rfloor \\
E^s(noR) &= \frac{1 - y^{\lambda+1} - (\lambda+1) \cdot (1-y) \cdot y^{\lambda+1}}{1-y} \\
\tau_u &\geq T \cdot E^s(noR) \geq \tau_l \qquad \delta_1 \geq 1 - y^{\lfloor (th'/T)-1 \rfloor + 1} \\
\delta &\geq y^{\lceil (th/T)-1 \rceil + 1} - y^{\lambda+1} \\
\delta_2 &\geq 1 - (1 - 2^{-d} \cdot [1-z])^{s-1} \cdot \left[1 + (s-1) \cdot 2^{-d} \cdot [1-z] \right]
\end{aligned}
$$

https://arxiv.org/abs/1612.00407

Conclusion

- Seek *Optimal Tradeoffs of Cost, Security, Availability, and Resiliency* for Governed Blockchains
- Use *Mathematical Modelling and Optimization* to compute such optimal tradeoffs
- Study use cases: *domain-specific block chains* in Finance, Internet of Things, and other domains
- ***Welcome international collaboration on this topic!***

Contact: m.huth@imperial.ac.uk