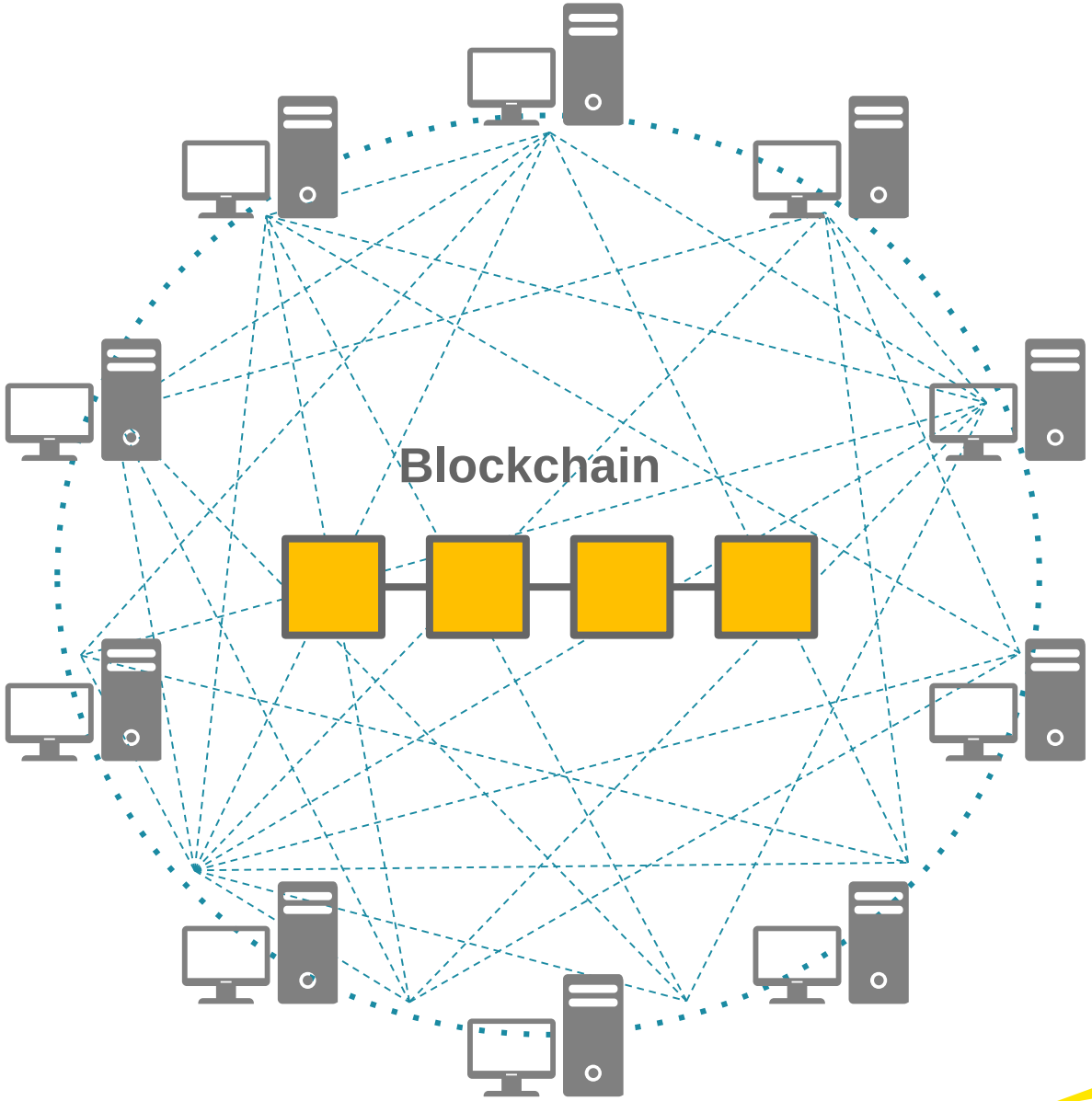
Weighing the Risks and Benefits of Blockchains: Managing Expectations With New Technologies

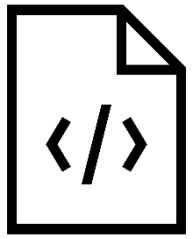
What is distributed ledger technology?

A technology that records activity in ledgers distributed across a network, so that participants can check each other's work and agree on historical activity

Blockchain technology is one example

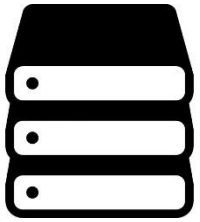


What are smart contracts?



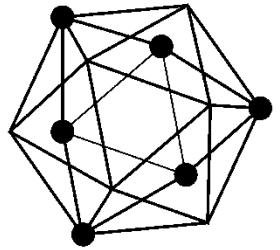
Pre-written business logic

that is

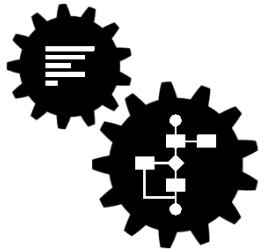


stored and replicated

on a



distributed ledger platform



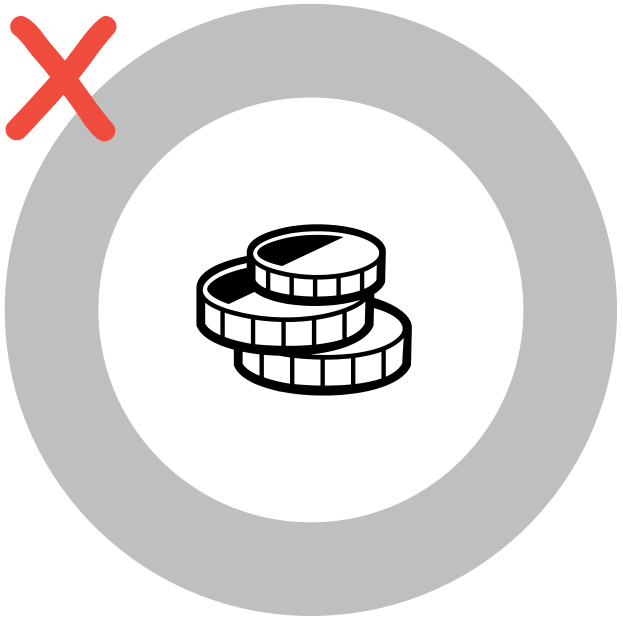
and is

executed by a network of computers

resulting in

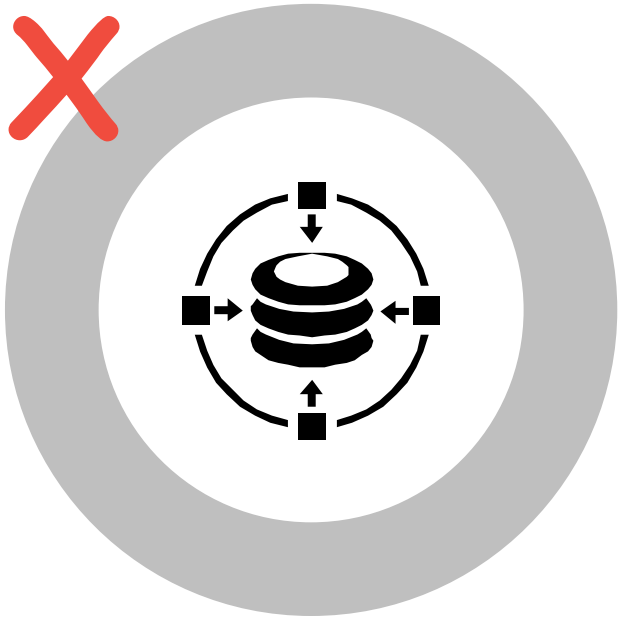
updates to the ledger

By itself, blockchain and distributed ledger technology is not…



Faster / cheaper payments

Fraud reduction technology

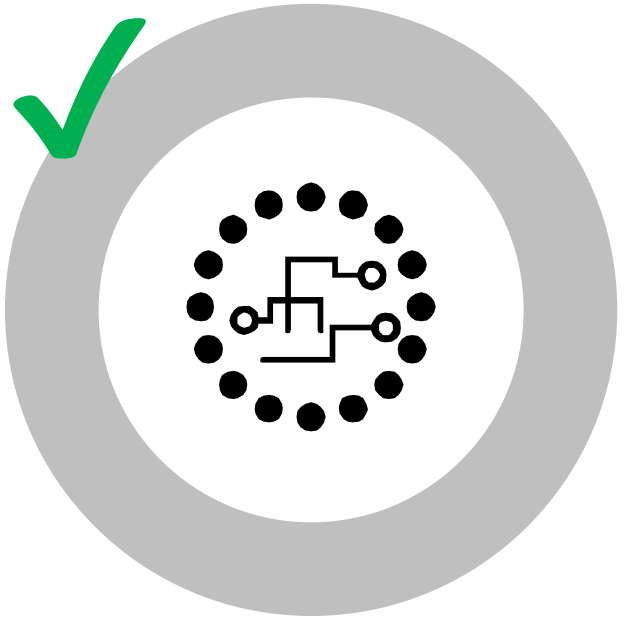


Back-office infrastructure replacement

What it can be

Enabler for more convenient payments

Global data anchor

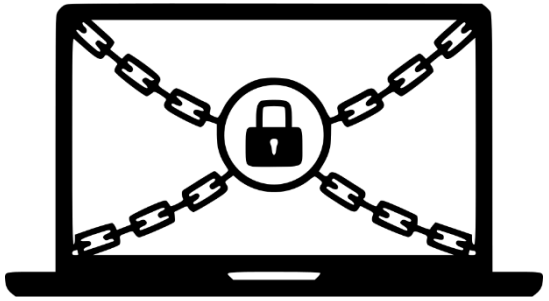


Enabler for new financial products

DLT security issues are like database security issues: it's implementation dependent

This is applied cryptography: to understand risks, you should understand cryptography

Implementations are not DLT risks

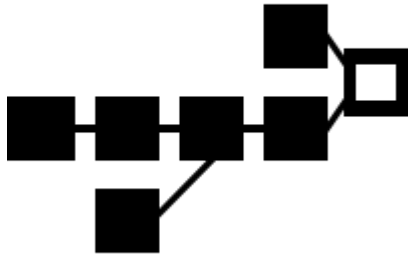


Ransomware

Bitcoin exchange hacks

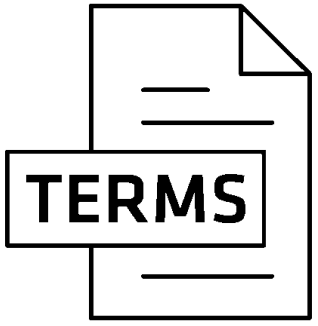
Application design considerations

1 On / off chain



2 Error management

3 Smart contracts



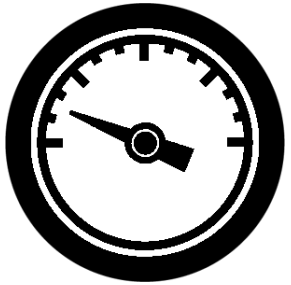
4 Security / privacy assumptions

Interface considerations

1 **Key management**

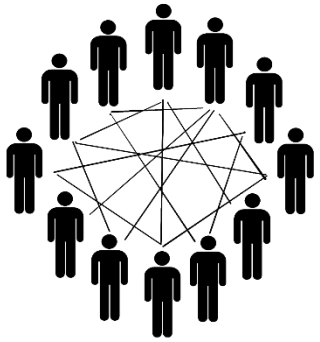
2 **Oracles**

3 **Latency**

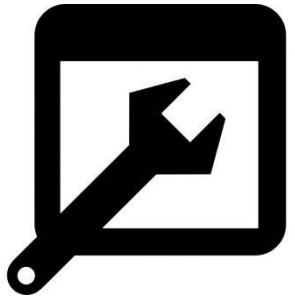


Infrastructure considerations

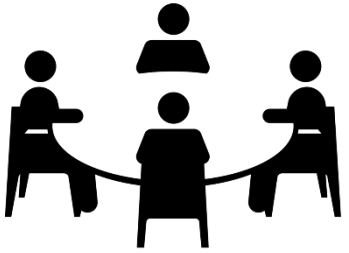
1 **Consensus error tolerance**



2 **Impacts of optimizations**



3 **Technology governance**



4 **Network failure impacts**

Key takeaways

1. To understand risks, you should understand cryptography – or trust someone who does!
2. Differentiate between application, interface, and infrastructure risks
3. What will you do when things go wrong?