BANK OF CANADA
BANQUE DU CANADA

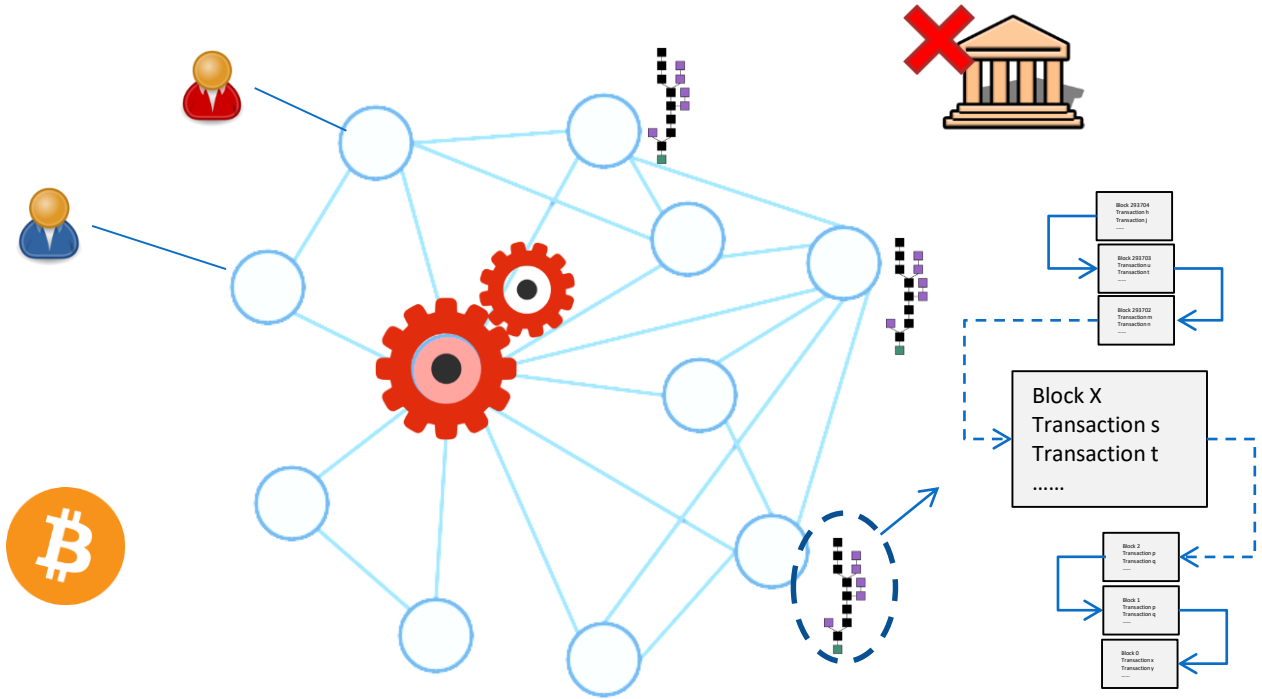
The Mechanics of DLT

Workshop On Fintech, Payments, and Financial Inclusion

Dinesh Shah
Program Manager, E-money and Fintech Research
Bank of Canada

The views expressed here are the author's, not those of the Bank of Canada

Blockchain, Bitcoin's Key Invention

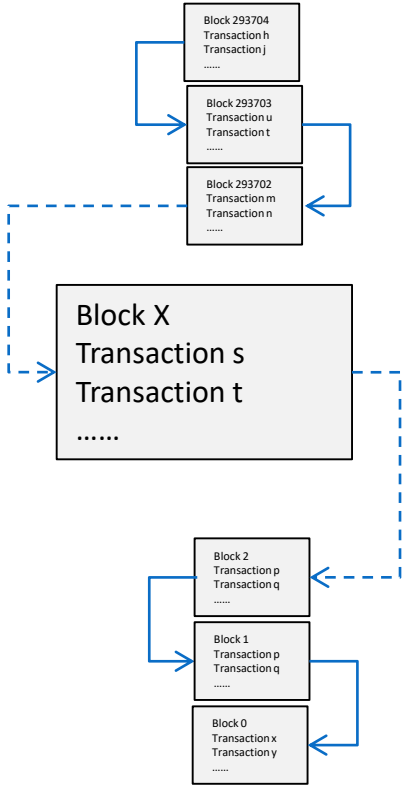


Bitcoin's Security – the Easy Stuff

1. Are you authorised to make a payment?
    1. Use public key cryptography; as long as I know private key (just a sequence of characters) I can digitally sign authorisation.
    2. This is 40 years old and underpins e-commerce, cyber security
2. Are you trying to double spend?
    1. The bitcoin history is public, we can check for attempts to double spend
    2. This is simple, once we have a reliable record

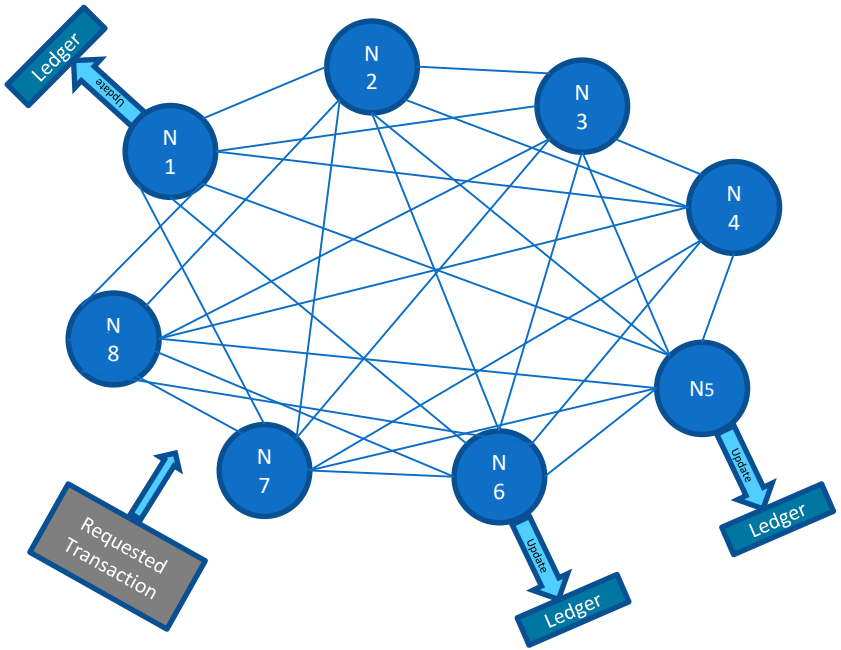
Bitcoin's Security – the Key Tech Innovation

3. How to get a decentralised system to securely conduct steps 1 and 2?
   - create incentives for **anonymous** peers to participate and…
   - reach a majority consensus amongst peers that the requested transaction is valid and…
   - record the transaction in a tamper proof way



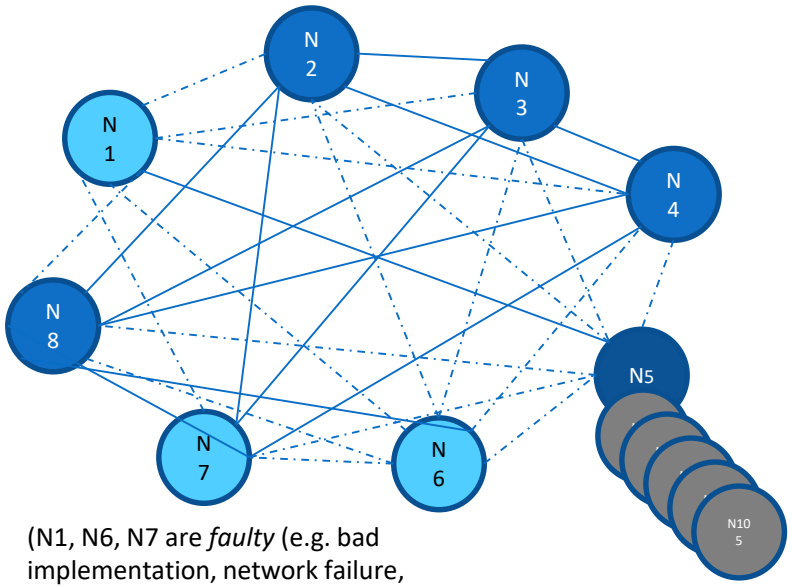
Securely Achieving Consensus – Not So easy

What is the simplest way of achieving consensus?



1. Everyone gets a vote
2. Until a majority is reached
3. Everyone then updates their ledger

Securely Achieving Consensus – Not So easy



(N1, N6, N7 are *faulty* (e.g. bad implementation, network failure, malicious)

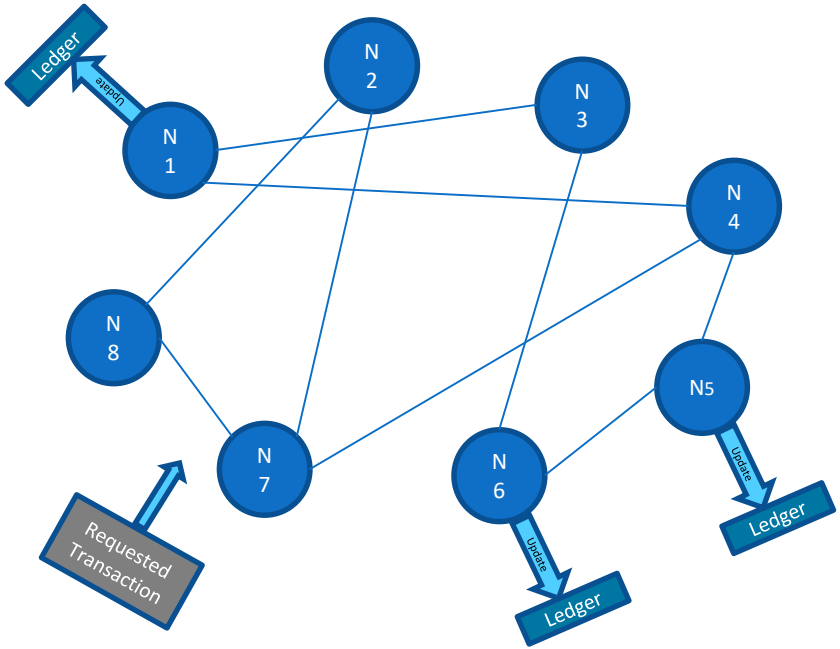
(*Sybil* attack, someone creates many false independent nodes)

This model won't work:

- If open and anonymous – we don't total node count to calculate majority
- Unreachable nodes (internet not 100% reliable)
- A subset of nodes could collude
- Easy to make a Sybil attack (a form of ballot stuffing)
- What is the incentive to be honest?

Consensus In a **Permissioned** System

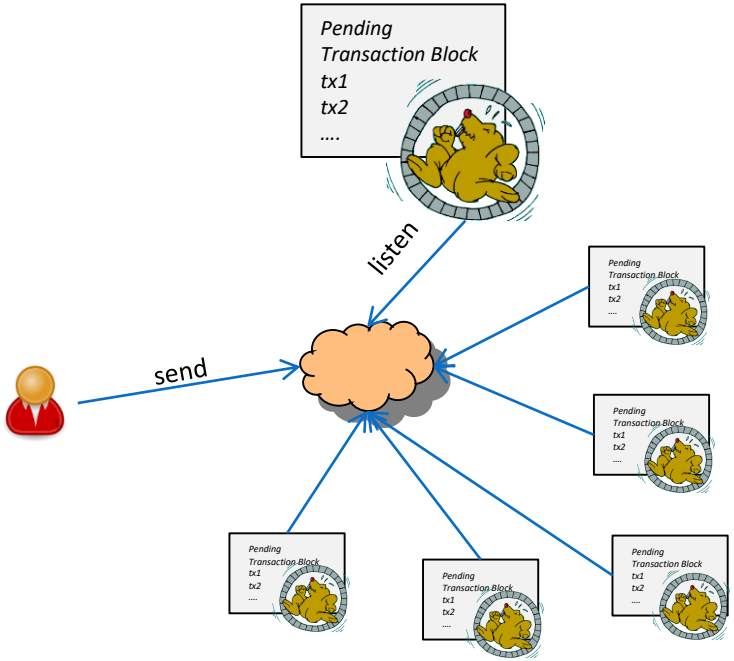
Things are easier if openness and / or anonymity is dropped

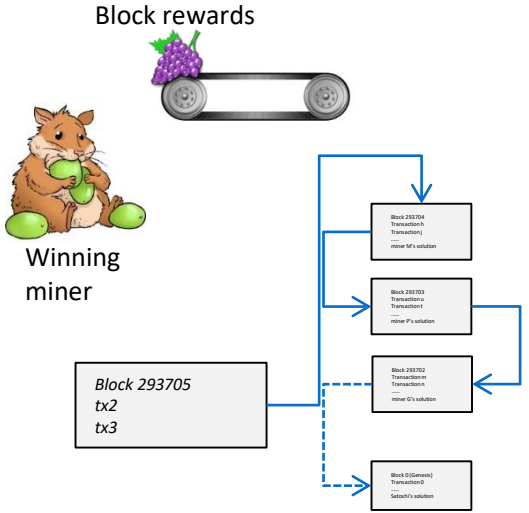


Features:

- Each node maintains a list of a subset of nodes it *collectively* trusts. i.e. your vote only counts if yours peers recognise you
- Multi-round ballots gets around network reliability issues; unreliably nodes dropped from future rounds

Consensus In a **Unpermissioned** System (Proof-of-Work)

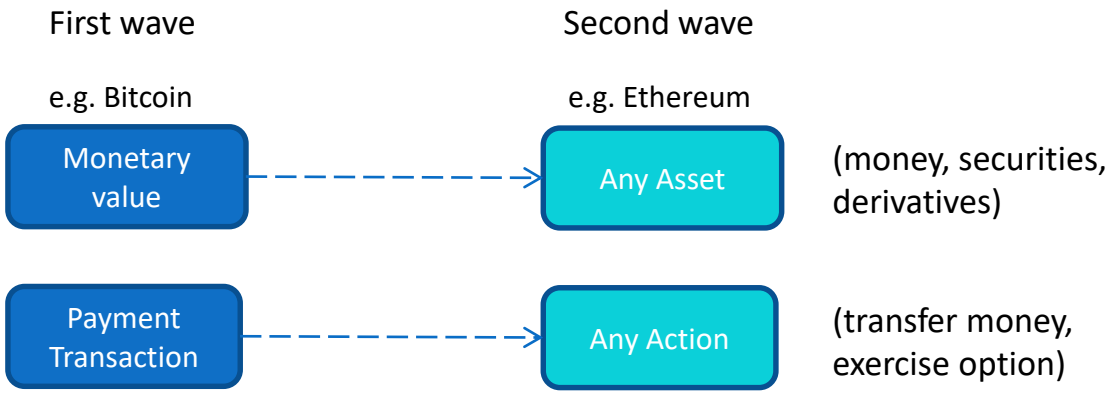




In a permission-less system:

- Money creation central to incentive
- Proof-of-work creates consensus and the tamper-resistant blockchain

Second Wave of Distributed Ledgers



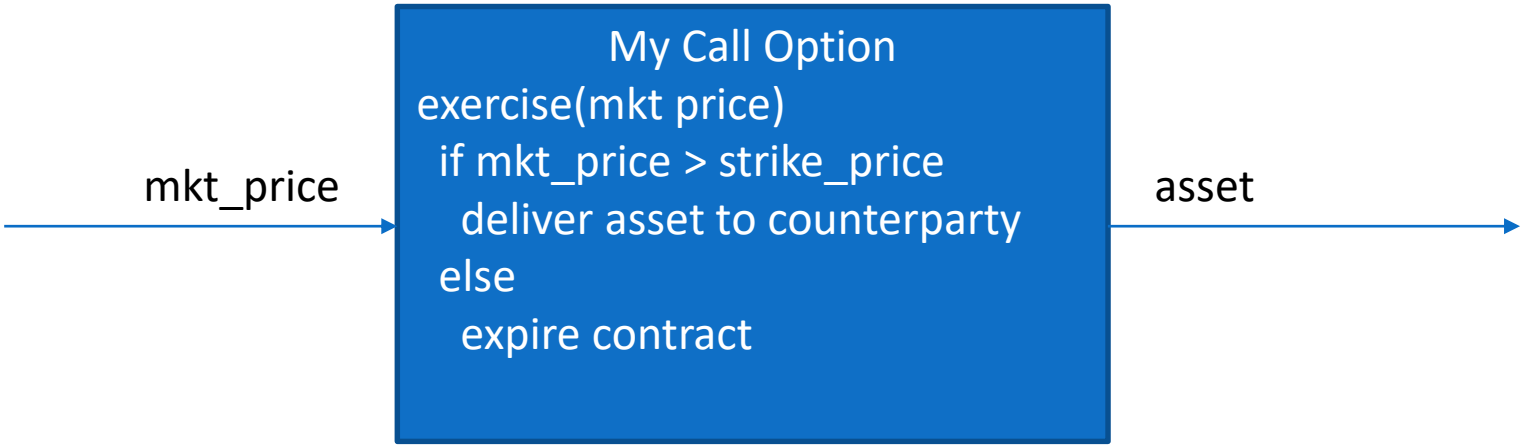
The second wave:

- the ledger is still the single source of truth for all participants
- introduces closed and permissioned ledgers
- Introduces ‘smart contracts’

Smart Contracts

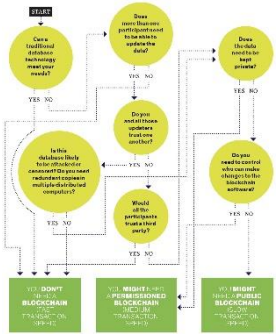
Not smart, not contracts – but useful:

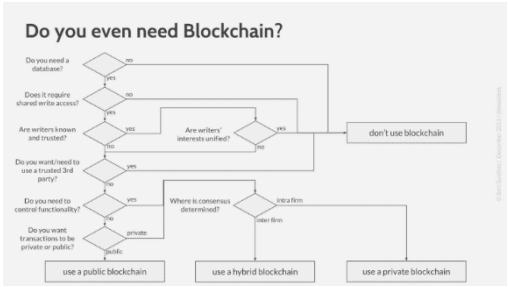
- programmable, computationally binding actions triggered by an event
- Can *express* the intent of a legal contract and *automate* actions

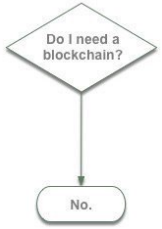


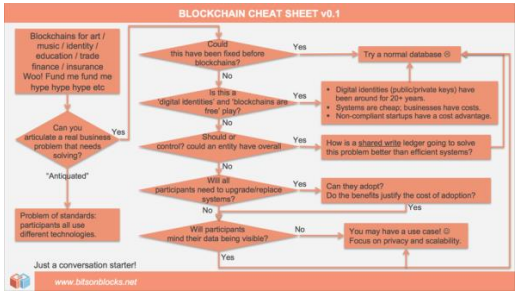
To DLT, or not to DLT?

Many decision heuristics…









…but 2 simple questions will get us a long way:

1. Is there a single widely trusted party in the ecosystem?
2. Is good governance feasible (accountability, change)?

BANK OF CANADA
BANQUE DU CANADA

Thank you