chrobis

Fundamentals of Blockchain

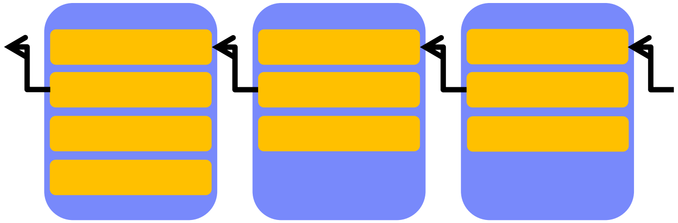
Noel Moriarty

July 2018

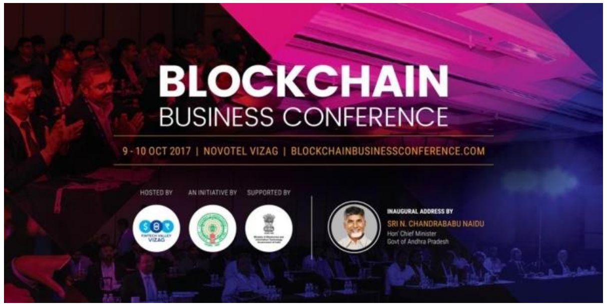
A Shared, Distributed Ledger

- Origins

- How it Works



- Applying it in Business



BLOCKCHAIN
BUSINESS CONFERENCE

9 - 10 OCT 2017 | NOVOTEL VIZAG | BLOCKCHAINBUSINESSCONFERENCE.COM

HOSTED BY AN INITIATIVE BY SUPPORTED BY

FINTECH VALLEY VIZAG

INAUGURAL ADDRESS BY
SRI N. CHANDRABABU NAIDU
Hon' Chief Minister
Govt of Andhra Pradesh

- Use Cases

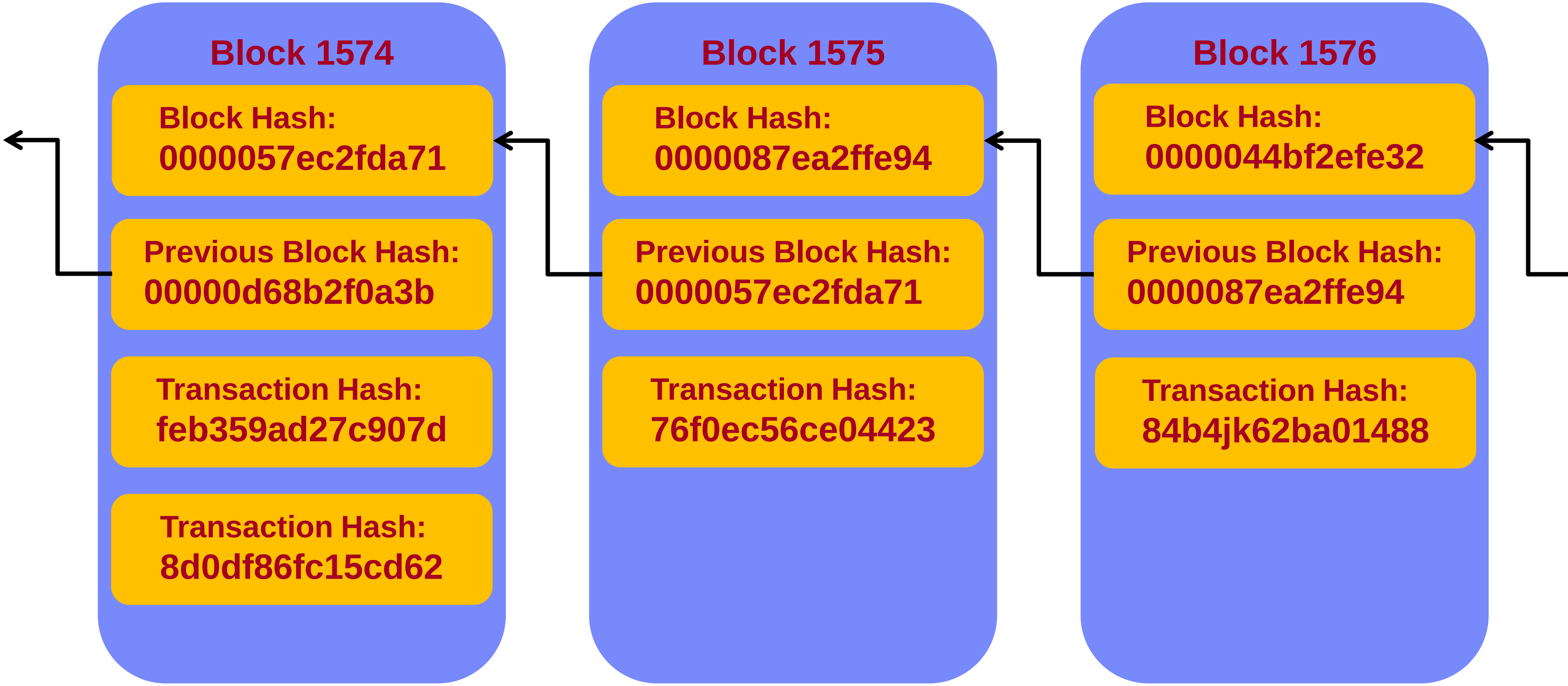
Money is all about trust

- Paper money, coins, letters of credit, cheques, bank accounts used throughout history to facilitate exchange of value
- Technology has improved things, but restrictions remain:
  - Cash not suited to large transactions
  - Duplication of effort and need for validation (banks)
  - Fraud and human error
  - High costs to use, e.g. paperwork and vetting / credit checks
- 50% of the world doesn’t have a bank account

The Emergence of Bitcoin

- Digital currency that addresses the weaknesses of current transaction systems:
  - b 2009, emanating from the financial crash of 2008,of unknown parentage (Satoshi Nakamoto)
  - ‘Coins’ are ‘mined’ by solving mathematical puzzles on computers. Limited volume of 21,000,000,000 coins
  - Users’ computers linked together (similar to Skype) and share a replicated ledger copied across their computers
  - Cost effective, efficient, safe and secure
  - No intermediaries, no central Monetary Authority, no-one controls it

Why is it called ‘block chain’?



Block 1574

Block Hash:
0000057ec2fda71

Previous Block Hash:
00000d68b2f0a3b

Transaction Hash:
feb359ad27c907d

Transaction Hash:
8d0df86fc15cd62

Block 1575

Block Hash:
0000087ea2ffe94

Previous Block Hash:
0000057ec2fda71

Transaction Hash:
76f0ec56ce04423

Block 1576

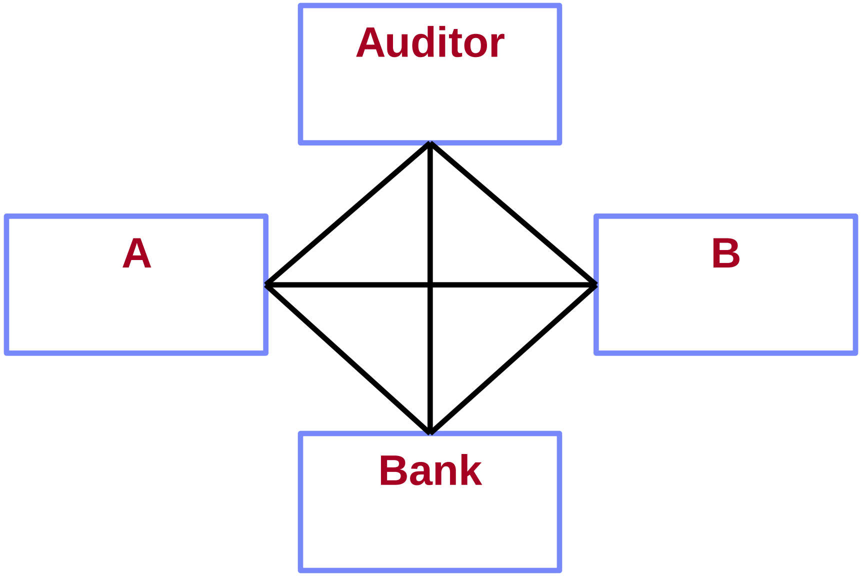
Block Hash:
0000044bf2efe32

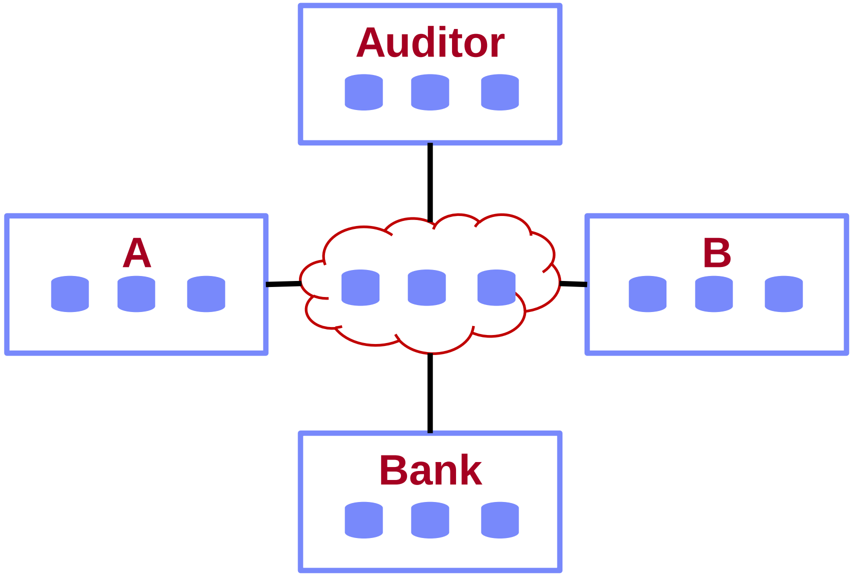
Previous Block Hash:
0000087ea2ffe94

Transaction Hash:
84b4jk62ba01488

Transactions are stored in a series of connected ‘blocks’

Before and After Blockchain





Everyone keeps separate records

- Intermediaries charge fees
- Inefficiences and time delays
- Duplication of effort
- Open to fraud

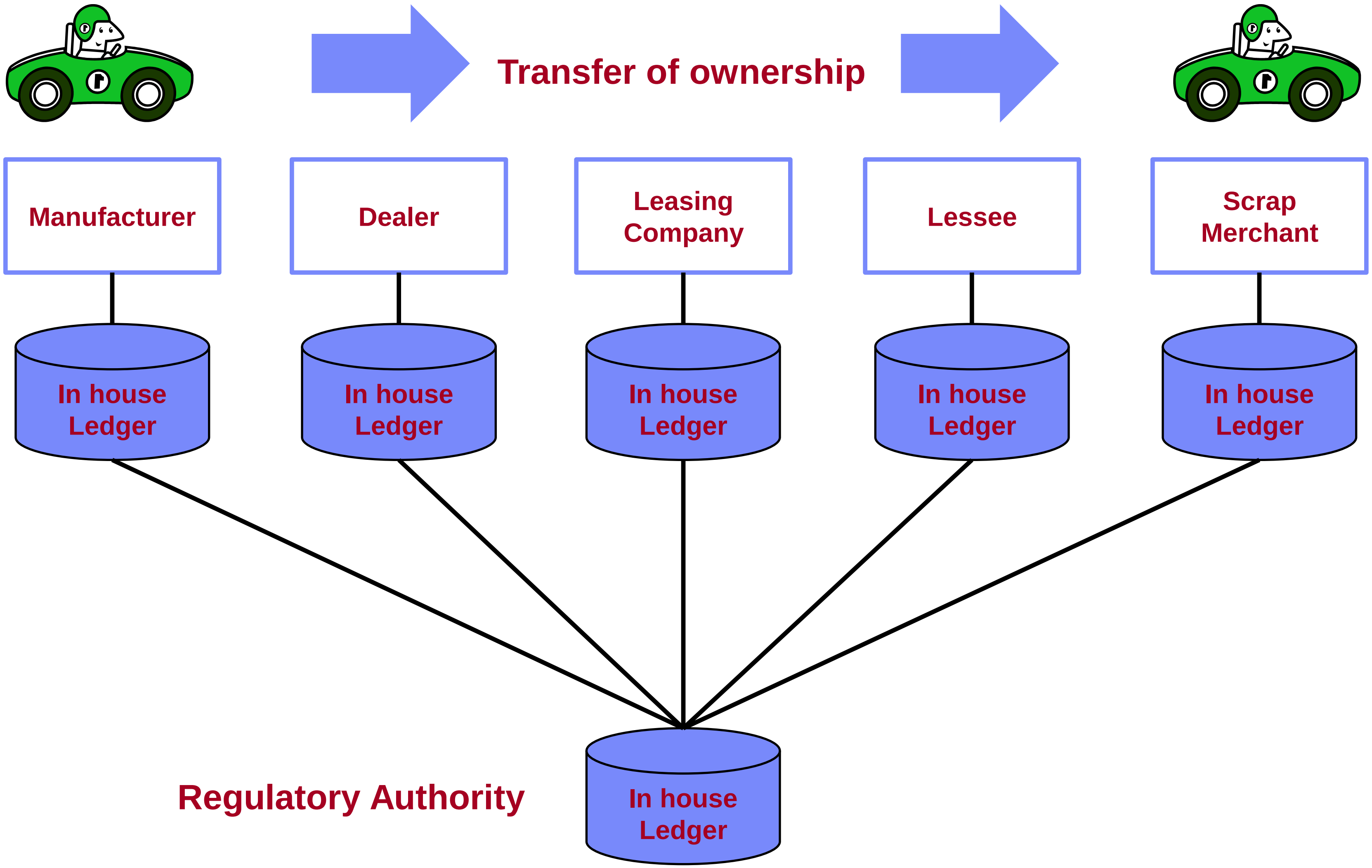
Single ledger replicated to all parties

- Eliminates duplication and reduces need for intermediaries
- Less vulnerable – consensus validation
- Secure, authenticated and verifiable digitally signed transactions

Key characteristics of Blockchain

- Consensus
  - For a transaction to be valid, all participants must agree on its validity
- Provenance
  - Participants know the source and history of the record
- Immutability
  - No participant can change a transaction
- Finality
  - Literally, one version of the truth

Tracking vehicle ownership



Transfer of ownership

Manufacturer

Dealer

Leasing Company

Lessee

Scrap Merchant

In house Ledger

In house Ledger

In house Ledger

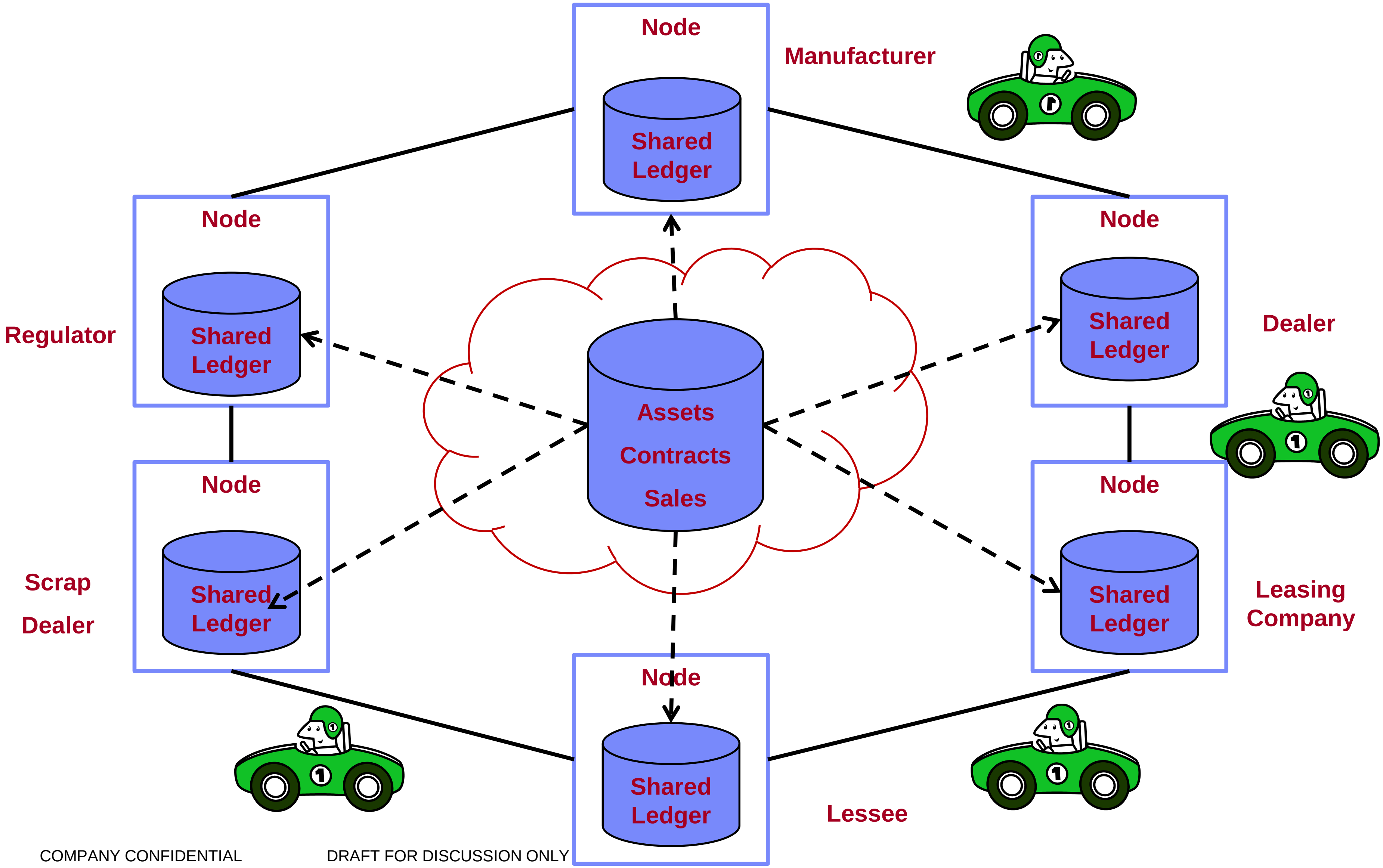
In house Ledger

In house Ledger

Regulatory Authority

In house Ledger

Tracking vehicle ownership



Visibility, time and cost savings build trust

- Complex, multi-party transactions reduced to minutes
  - No oversight, network is self-policed
  - Reduced role for intermediaries
  - Eliminates duplication of effort
- Improved security
  - Secure storage / No tampering
  - Members only networks
- Enhanced privacy
  - IDs and permissions control access rights and capabilities
- Improved auditability
  - Single source of truth, transparent and auditable
- Increased operational efficiency
  - Real-time replication of transactions conducted with speed and accuracy

Why is it suitable for business?

Shared Ledger

- Append-only distributed system of record, shared across business networks

Permissions

- Appropriate visibility for secure, authenticated and verifiable transactions

Smart Contract

- Business terms embedded in transaction database and executed with transactions

Consensus

- All parties agree to network verified transactions

Who can use it?

- **Financial Services**
  - Commercial Finance
  - Trade Finance
  - Cross-Border Transactions
- **Insurance**
  - Claims Processing
  - Fraud Reduction
- **Government**
  - Asset Ownership
  - Identity Verification
  - Welfare Benefits
  - Customs
- **Supply Chain / Manufacturing**
  - Asset tracking / critical parts
  - Traceabiity of High Value Goods
  - Warranty
  - Freight logistics / international shipping
  - Pharmaceuticals
- **Healthcare**
  - Electronic Medical Records
  - Regulation
- **Internet of Things (IoT)**
  - Quality control
  - Maintenance, Repair and Overhaul

Everyone will use it?

- **Payments**
  - Fast secure payment with no need for intermediaries (banks) and fees for their service
- **Contracts**
  - Replaces the need for ‘trust’ in legal affairs
- **Recruitment**
  - You are who you say you are – eliminates reference checks
- **Data Storage**
  - Safe, secure, decentralised storage in the cloud
- **Governance**
  - No authorities setting and monitoring ‘the rules’

https://hackernoon.com/your-company-will-use-blockchain-in-less-than-10-years-heres-how-6d9da452fa8d

How to decide?

- Does my business 'network' use contractual relationships?
- Do we need to track transactions that involve more than two parties?
- Is the way we do it now overly complex, costly, or use intermediaries?
- Can we all benefit from increased trust, transparency and accountability?
- Is the current system prone to errors in manual processes, paperwork or duplication of effort?
- Is the current system prone to fraud or third party attack?

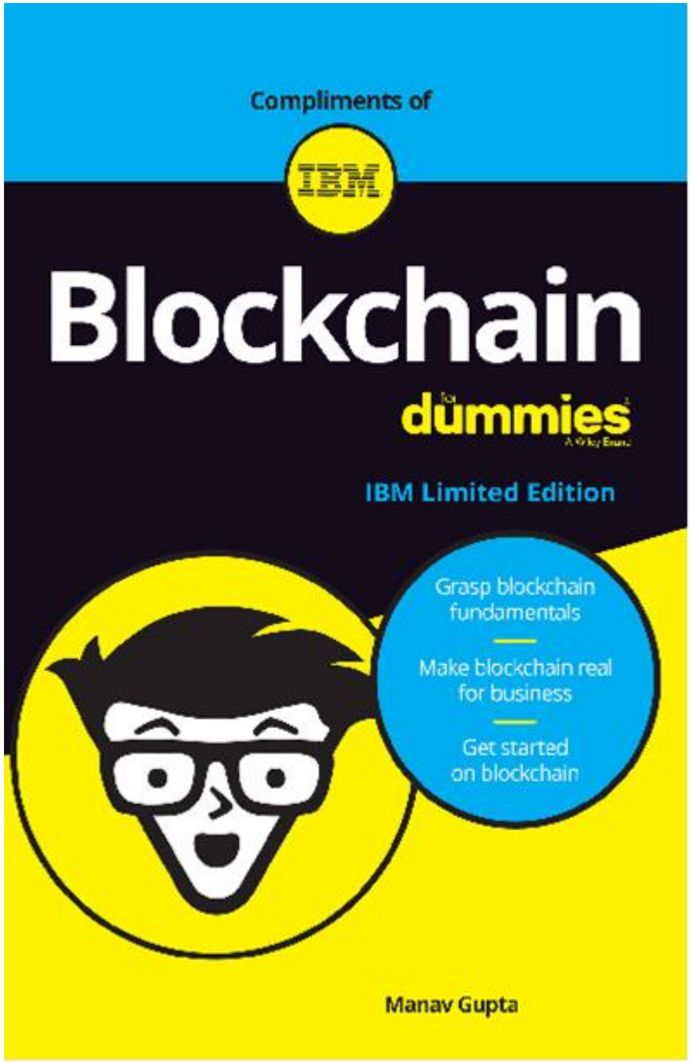
Further reading

- Blockchain for Dummies (IBM Limited Edition)

  https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XIM12354USEN

- Leverage blockchain to transform your business and disrupt your industry

  https://www.ibm.com/blockchain/for-business.html


Compliments of
IBM
Blockchain
for dummies
A Wiley Brand
IBM Limited Edition
Grasp blockchain fundamentals
Make blockchain real for business
Get started on blockchain
Manav Gupta