MILLER THOMSON
AVOCATS | LAWYERS

FORWARD TOGETHER

Blockchain Speak

Aiyaz A. Alibhai
June 21, 2018

Overview

- Institutionalizing Trust
- The Ideal Solution
- Blockchain Definition and Elements
- Blockchain Applications
- Legal Issues
- Financial Transactions and Cryptocurrencies
- Reflections

Institutionalizing Trust

- Trust is a foundational element of business.
- Yet maintaining it—particularly throughout a global economy that is becoming increasingly digital—is expensive, time-consuming, and, in many cases, inefficient.
- Business transactions take place every second of every day — orders, payments, account tracking and much more.
- Each participant has his own, separate ledger — increasing the possibility of human error or fraud.
- Reliance on intermediaries for validation creates inefficiencies, delays and costs.

Vehicle Ownership before Blockchain

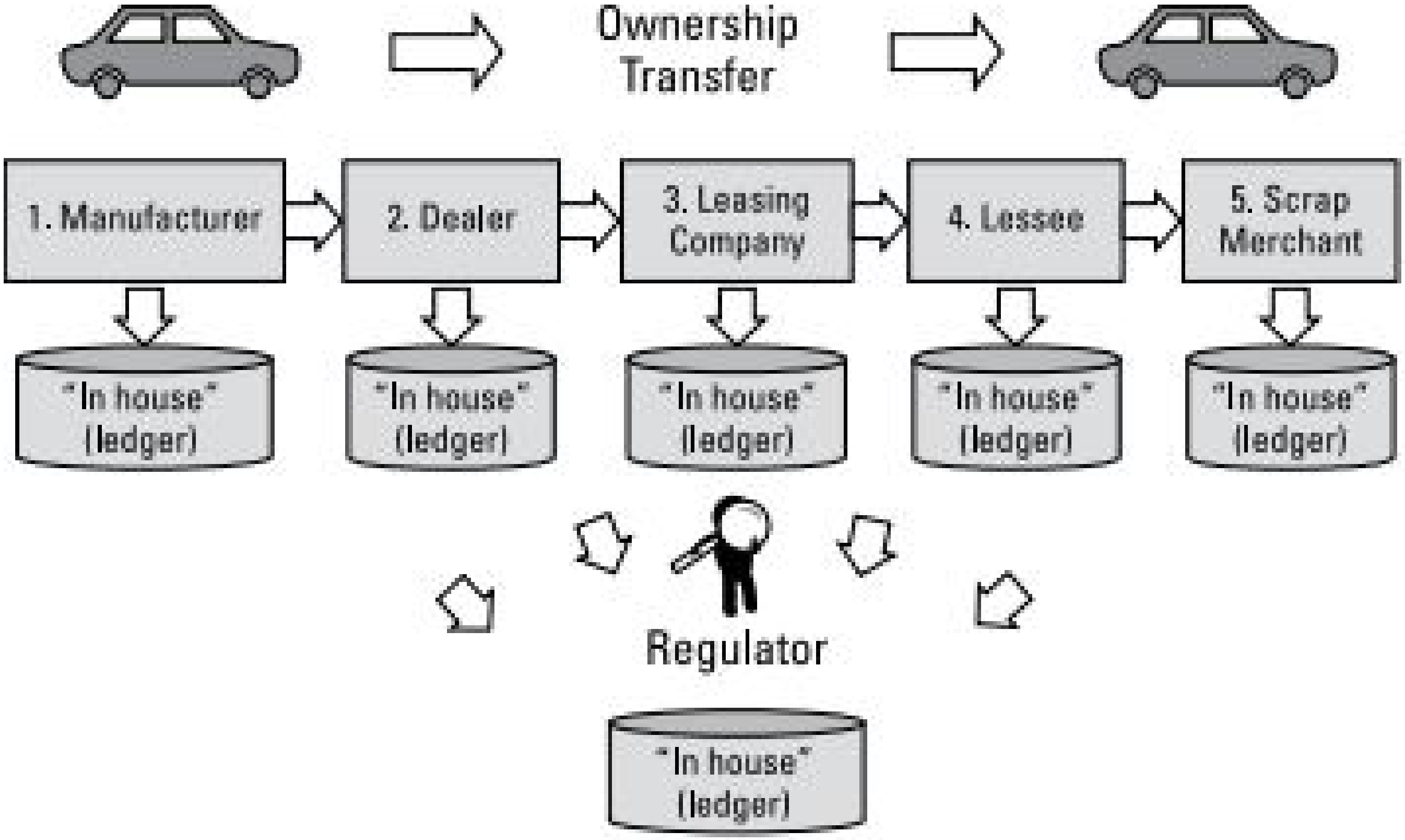


FIGURE 1-2: Tracking vehicle ownership without blockchain.

The Ideal Solution

- Recording information in a way that creates trust in the information recorded
  - Single, shared, tamper-evident record for related transactions
  - Accessible by all members
  - Separate passwords for access to own information
- Transparent chain of data, eliminating the need for intermediaries and other third parties
  - Verification process for trust
  - Consensus by all parties before a new transaction is added to the network
- Reliability and Resilience
  - Backed up across various systems

Vehicle Ownership - Blockchain

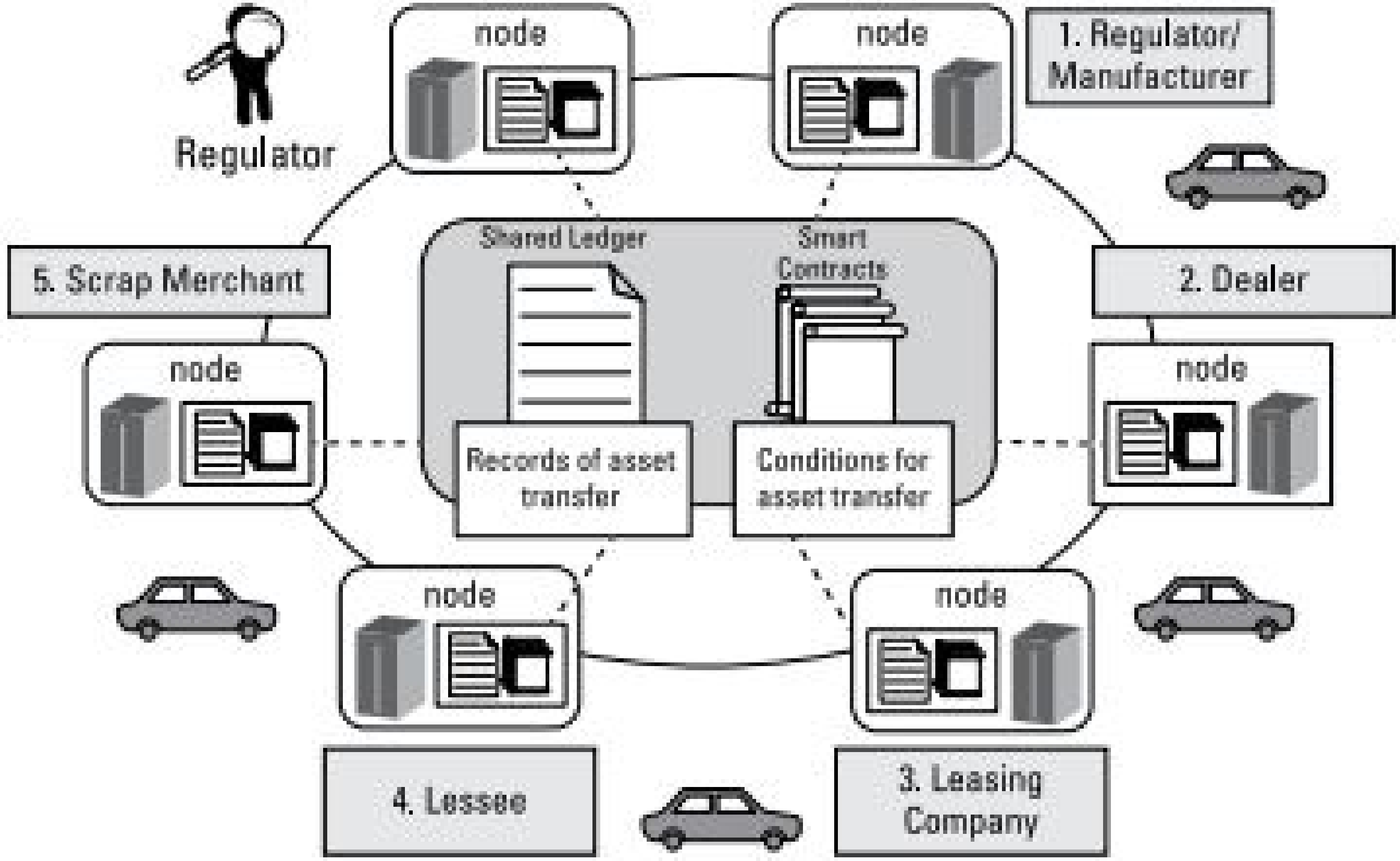
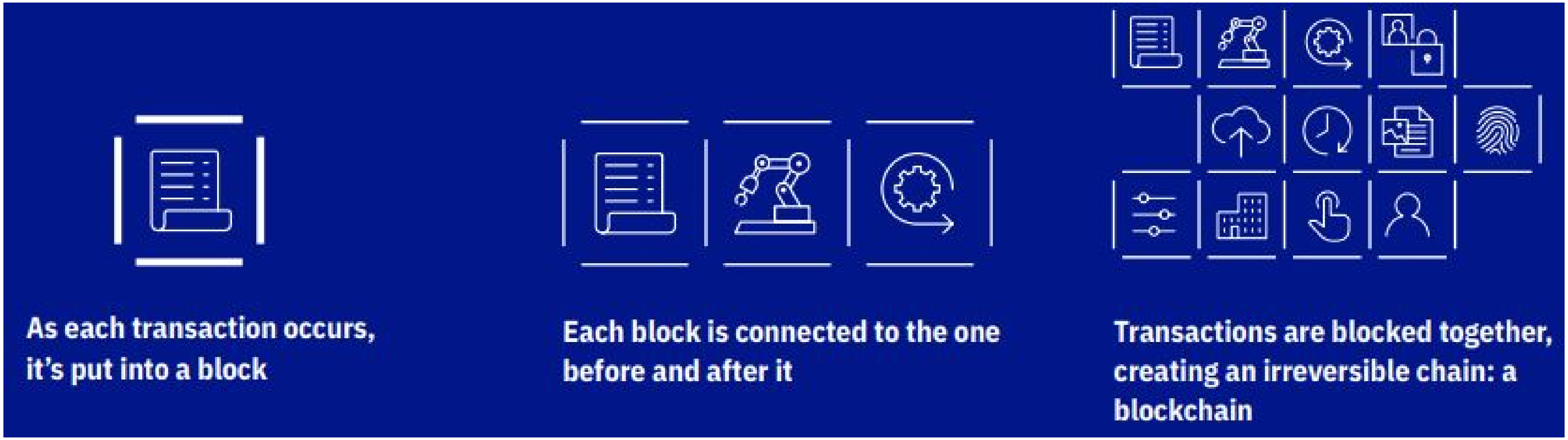


FIGURE 1-3: Tracking vehicle ownership with blockchain.

Building a Blockchain



As each transaction occurs, it's put into a block

Each block is connected to the one before and after it

Transactions are blocked together, creating an irreversible chain: a blockchain

Blockchain Definition

- A blockchain is a shared database that is managed by a global network of computers.
- Information held in the database is distributed and continually reconciled by the computers in the network in an encrypted form.
- The computers are often referred to as *nodes, miners,* or *peers.*
- When data is entered in a blockchain, it can’t be removed.

Summary of Key Elements

- Distributed Network
  - Blockchain works as a shared system of record among participants on a business network, eliminating the need to reconcile disparate ledgers.

- Permissioned
  - Each member of the network has access rights so that confidential information is shared on a need-to-know basis.

- Secured
  - Consensus is required from all network members, and all validated transactions are permanently recorded. No one, not even a system administrator, can delete a transaction.

Consensus Protocol

- Consensus Agreement and terms built into protocol in advance
- **Proof of Stake ("Skin-in-the-Game")**
  - To validate transactions, validators must hold a certain percentage of the network's total value.
  - Proof-of-stake might provide increased protection from malicious attack on the network by reducing incentives for attack and making it very expensive to execute attacks.
- **Multi-Signature**
  - A majority of validators (specified in advance) must agree that a transaction is valid.
- **Computerized and Automated Dispute Resolution for Consensus**
  - An algorithm designed to settle disputes among computing nodes (network participants) when one node in a set of nodes generates different output from the others in the set.

Summary of Blockchain

- A blockchain is a distributed database, meaning that the storage devices for the database are not all connected to a common processor. It maintains a growing list of ordered records, called blocks. Each block has a timestamp and a link to a previous block.

- Blockchain technology offers the intriguing possibility of eliminating this “middle man”. It does this by filling three important roles – recording transactions, establishing identity and establishing contracts – traditionally carried out by the financial services sector.

- Cryptography ensures that users can only edit the parts of the blockchain that they “own” by possessing the private keys necessary to write to the file. It also ensures that everyone’s copy of the distributed blockchain is kept in synch.

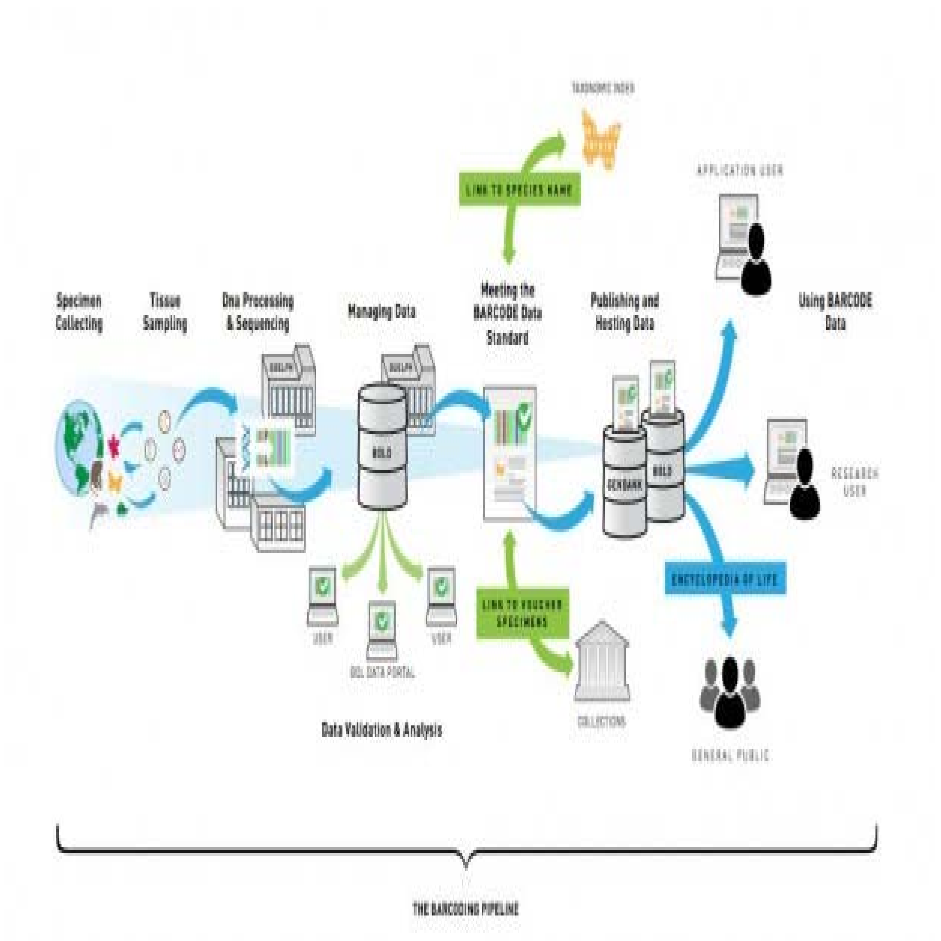
Blockchain Uses and Examples

- Using blockchain in a supply chain allows complete traceability of a product’s origin and final recipient.
- When something goes wrong with a complex “system of systems,” such as an aircraft, it’s important to know the provenance, through supply chain management, of each component, down to the manufacturer, production date, batch, and even the manufacturing machine program.
- Blockchain holds complete provenance details of each component part, accessible by each manufacturer in the production process, the aircraft owners, maintainers, and government regulators.

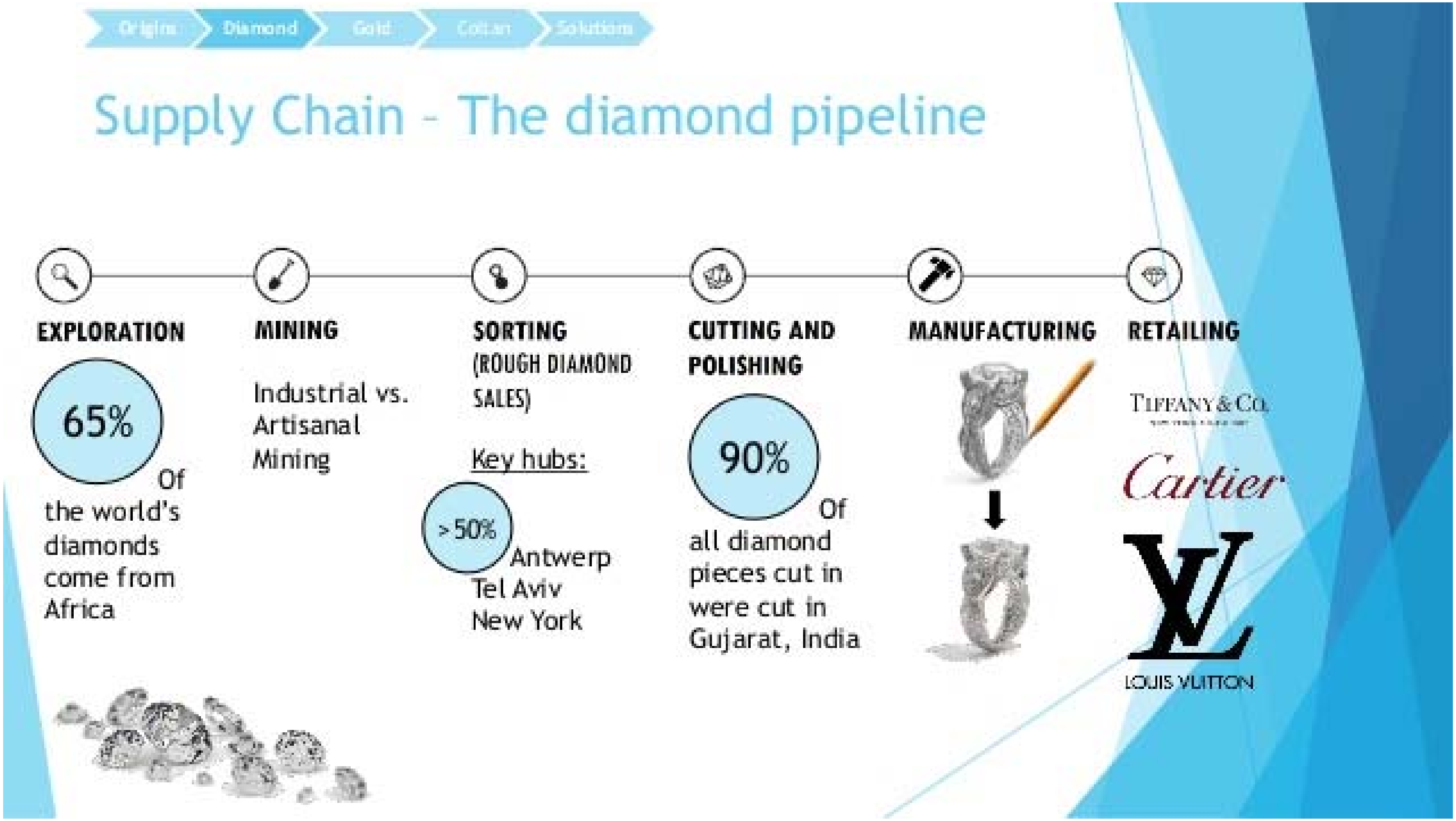
Blockchain Applications

- Food Supply Chain
  - Digital product information such as farm origination details, batch numbers, factory and processing data, expiration dates, storage temperatures and shipping detail are digitally connected to food items and the information is entered into the blockchain along every step of the process. Records are permanent.
- Financial / Commercial Services
  - Businesses need to purchase goods and services on credit with end-to-end visibility to avoid and resolve transaction disputes.
- Trade Finance (Digital Bill-of-Lading)
  - The process of obtaining approvals from multiple legal entities (customs, port authorities, trucking or rail transportation firms, and so on) for the movement of goods across borders.
  - **Internet of Things** (IoT) - As machines interact with one another, any relevant interactions can be reported by the machines and recorded in the blockchain to increase efficiency and accuracy and reduce costs.
- Healthcare
  - Efficient and secure system for managing medical records.

Supply Chain Management



Conflict Diamonds Supply Chain



Origins Diamond Gold Coltan Solutions

Supply Chain - The diamond pipeline

EXPLORATION

65% Of the world's diamonds come from Africa

MINING

Industrial vs. Artisanal Mining

SORTING (ROUGH DIAMOND SALES)

Key hubs:

>50% Antwerp Tel Aviv New York

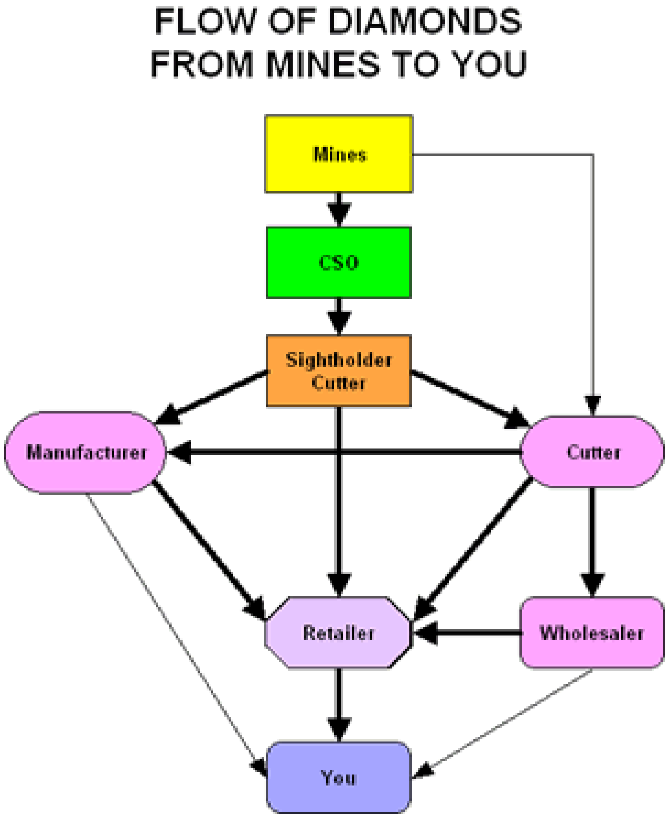
CUTTING AND POLISHING

90% Of all diamond pieces cut in were cut in Gujarat, India

MANUFACTURING

RETAILING

Flow of Diamonds



- Tracking diamonds from mine to final customer is complex. Smuggling, fraud, counterfeit diamonds and unethically-mined stones pose real challenges.
- Blockchain allows:
  1. Keep a record of high resolution photos for each diamond at every touchpoint along its journey.
  2. Track real-time records of every payment transaction.
  3. Hold certificates of authenticity.
  4. Maintain product details like cut, clarity, color, carat and diamond serial numbers.

Legal Issues

- Technical requirements must be established and agreed upon in advance.

- Legal input is essential to understand what requirements must be fulfilled or avoided and any regulatory frameworks must be complied with.

“Smart” Contracts

- Agreements that have been codified inside a blockchain.
- Smart contracts have an internal memory containing their code (**Terms**).
- The code gets executed when predetermined restrictions are met (**Conditions precedent or subsequent**).
  - e.g construction contract with sensor or human input

    “If building height increase by one floor, release $$$ to contractor.”
- These restrictions could be internal or external to the smart contract.
- The smart contracts facilitate, verifies, and enforce the performance of a contract. There is no outside part or legal system that interprets the contract and the intent of the parties.
- The code is self-contained “law”.

“Smart” Contracts - Issues

- No Agreement is truly self-contained.
- Formalities and Compliance
  - What other formalities outside the blockchain required to perfect the transaction
  - Who is responsible for identifying these and ensuring compliance.
- Liability
  - Issue of liability needs to be addressed if the contract has been miscoded such that it doesn’t achieve the intent of the parties, or the oracle makes a mistake or deliberate error.
  - Applicable law, jurisdiction, general principles of proper governance, dispute resolution, privacy and the means of digital identity.
- From a public-law perspective, there are obviously risks that permissionless blockchains are used for illegal purposes such as money-laundering or to take advantage of pseudonymous involvement to get around competition-law issues.

Parties in a Blockchain Transaction

- Blockchain User
- Blockchain Developer / Programmer
- Blockchain Network Operator
- Certificate Authority
    - An individual who issues and manages the different types of certificates required to run a permissioned blockchain. For example, certificates may need to be issued to blockchain users or to individual transactions.
- Regulator?
    - A blockchain user with special permissions to oversee the transactions happening within the network.

Liability of blockchain organization

- What is the legal status of an entirely blockchain-enabled organization (Distributed Autonomous Organization - DAO), which operates through pre-programmed smart contracts, without human involvement?
- Does it have its own legal personality?
- In the absence of certainty about the nature of a DAO, how will ownership and control be determined?
- Who will be responsible for defects in a blockchain system / DAO?

Subject Matter - Is Data “Property”?

- At common law as a general principle there is no property right in information itself, but that while individual items of information do not attract property rights, compilations of data – for example in a database – may be protected by intellectual property rights.
- Where a database of personal information is sold, if a buyer wants to use the personal information for a new purpose, in order to comply with privacy legislation they will have to get consent for this from the individuals concerned.
- *R v. Stewart*, SCC held that confidential information is not property which may be subject matter of theft under s. 322 of the Criminal Code.

Personal Information and Data Protection

- Federal PIPEDA governs the inter-provincial and international collection, use, and disclosure of personal information.
- Provincial Privacy Acts govern use of personal information within a Province.
- “Personal Information” is consistently defined very broadly under Canadian Privacy Statutes as information about an identifiable individual (including IP address).
- Legislation requires an Organization to clearly disclose purpose for collection and use, consent, transparency, proportional use, and limited retention period.
- Legislation grants individuals the rights to access personal data; correct and delete; objection and withdraw consent; and right of redress to authority.

Data Privacy and Compliance

- Once data is stored it cannot be altered; this clearly has implications for data privacy, particularly where the relevant data is personal data or metadata sufficient to reveal someone's personal details.
- Who are the data controllers (those who determine the purposes and manner of processing, and have primary legal responsibility for data protection compliance).
- Who are the data processors (those who process on behalf of the data controllers).
- More than one party to a blockchain network may be responsible for compliance with the relevant privacy requirements.
- Technology-based solutions will need to be found to design privacy-protecting blockchains.
- The transparency of transactions on the blockchain is not easily compatible with the privacy needs of the banking sector - the use of crypto-addresses for identity is problematic as no bank likes providing its competitors with precise information about its transactions, and banking secrecy must be kept by law.

Legal Jurisdiction?

- Blockchain has the ability to cross jurisdictional boundaries as the nodes on a blockchain can be located anywhere in the world.
- This can pose a number of complex jurisdictional issues which require careful consideration in relation to the relevant contractual relationships.
- The principles of contract and title differ across jurisdictions and therefore identifying the appropriate governing law is essential.
- The inclusion of an exclusive governing law and jurisdiction clause is essential for legal certainty as to the law to be applied to determine the rights and obligations of the parties to the agreement and which courts will handle any disputes.

Regulatory Requirements

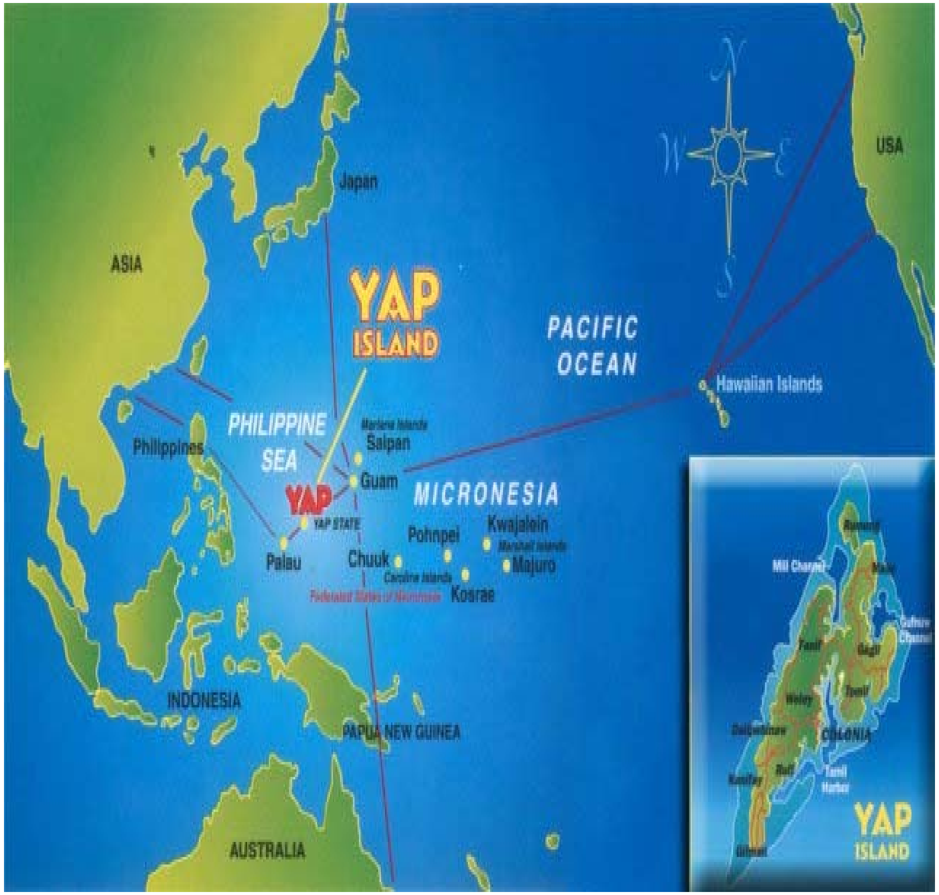
- It may be technically possible to transfer the ownership of a house from one participant in a blockchain to another, but in many jurisdictions it is not legally valid without registering the transaction on the national registry.
- Data protection and anti-money-laundering provisions – must be complied with.
- Where personal data is recorded in a blockchain, who is responsible for protecting that data and complying with national and supra-national regulations.
- In a permissioned blockchain this could be the super-user as data controller, in a permissionless blockchain it would potentially be every member of the network.
- How does a natural person get their data deleted or corrected if they cannot identify the data controller(s) using pseudonyms, and how can their data be removed from an immutable record?

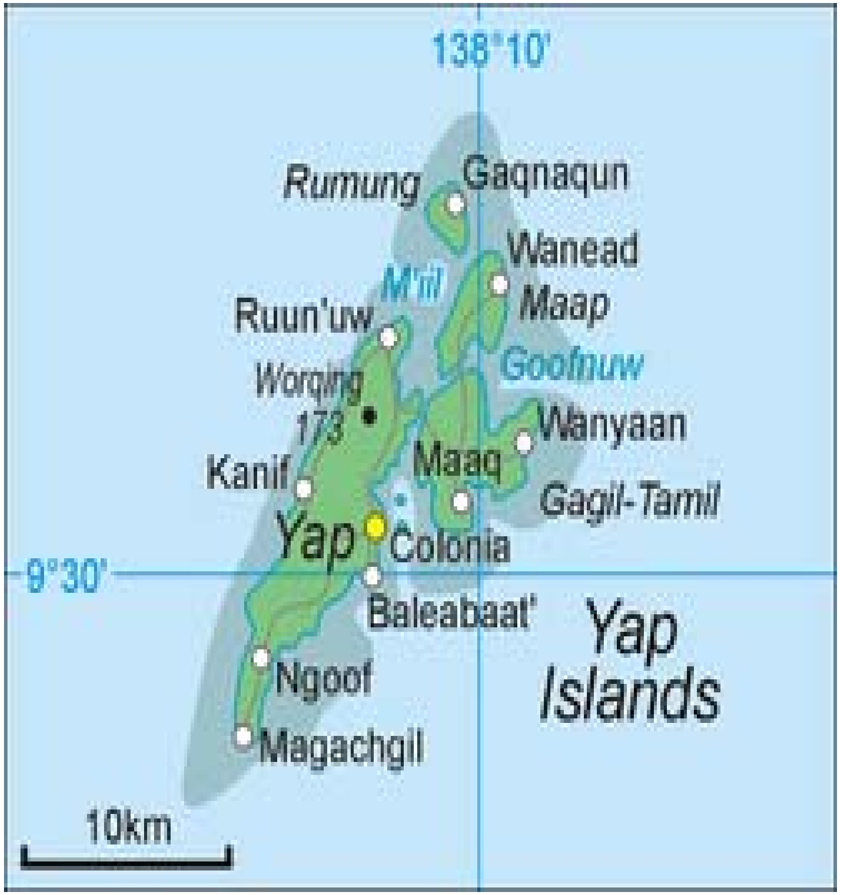
Financial Transactions

Fiat Currencies

- Today, most currencies—the U.S. dollar included—are fiat currencies.
- Fiat currencies are not backed by physical assets; rather, they are backed by the promise of their issuing government.
- Gold worked as a store of value due to its physical characteristics.
- The move away from gold was brought on by the realization that commodity money ties a country's economy to a scarce natural resource, and this can have destabilizing effects.
- Fiat currency's supply— and thus its value—is protected by regulation.
- It is recognized as legal tender, the government is obliged to accept it for tax payment, the central bank has monopoly control over supply, and it is often backed by indirect collateral and insurance.

Yap Islands


ASIA
Japan
USA
YAP ISLAND
PACIFIC OCEAN
Hawaiian Islands
PHILIPPINE SEA
Philippines
Mariana Islands
Saipan
Guam
MICRONESIA
YAP
YAP STATE
Palau
Chuuk
Pohnpei
Kwajalein
Marshall Islands
Majuro
Caroline Islands
Federated States of Micronesia
Kosrae
INDONESIA
PAPUA NEW GUINEA
AUSTRALIA
N
W
E
S
Mill Channel
Tamil
Gagil
Weloy
COLONIA
Rull
Tamil Harbor
YAP ISLAND


138°10'
Rumung
Gaqnaqun
Wanead
M'ril
Maap
Ruun'uw
Goofnuw
Worqing
173
Wanyaan
Kanif
Maaq
Gagil-Tamil
Yap
Colonia
9°30'
Baleabaat'
Yap Islands
Ngoof
Magachgil
10km

Yap Coins

Yap-Coins

- Until the early 20th century the people on Yap, an island in the Pacific Ocean, used large stone disks as money for big expenses, such as a daughter’s dowry.
- Being very heavy, they were rarely moved when spent. Instead, they simply changed owners.
- Every transaction became part of an oral history of ownership, which allowed islanders to know the proprietor of each stone and made it difficult to spend the same stone twice.

Bitcoin

Cryptocurrency

- Online computer code
- Backed by their respective networks
- Cryptocurrencies are restricted entries in a database.
- Specific conditions must be met to change these entries.
- Network ensures that there is no double spending; it does this with no central server or authority.
- Peer-to-peer network solves the “double-spend” problem in most cases by having every peer have a complete record of the history of all the entries made within the network.
- Created with cryptography, the entries are secured with math, not people.
- Cryptocurrencies are generated by the network in most cases to incentivize the peers, also known as *nodes* and *miners,* to work to secure the network and check entries.

Bitcoin Cryptocurrency

- Bitcoin was developed in 2008 as a concept by an anonymous developer going by the pseudonym of Satoshi Nakamoto.
- Bitcoin was devised as a non-fiat currency.
- The value arises from computing power, that is, the only way to create new coins is by allocating distributed CPU power through computer programs named “miners”.
- The algorithms that produce new BTC coins increase the amount of processing power necessary to create each new block, so producing new coins is more difficult.
- Each bitcoin consists of 100 million smaller units, with each unit called a satoshi.
- The operations performed to mine are precisely to authenticate other transactions, so the system both creates value and authenticates itself, an elegant and simple solution that is one of the appealing aspects of the currency.

Bitcoins

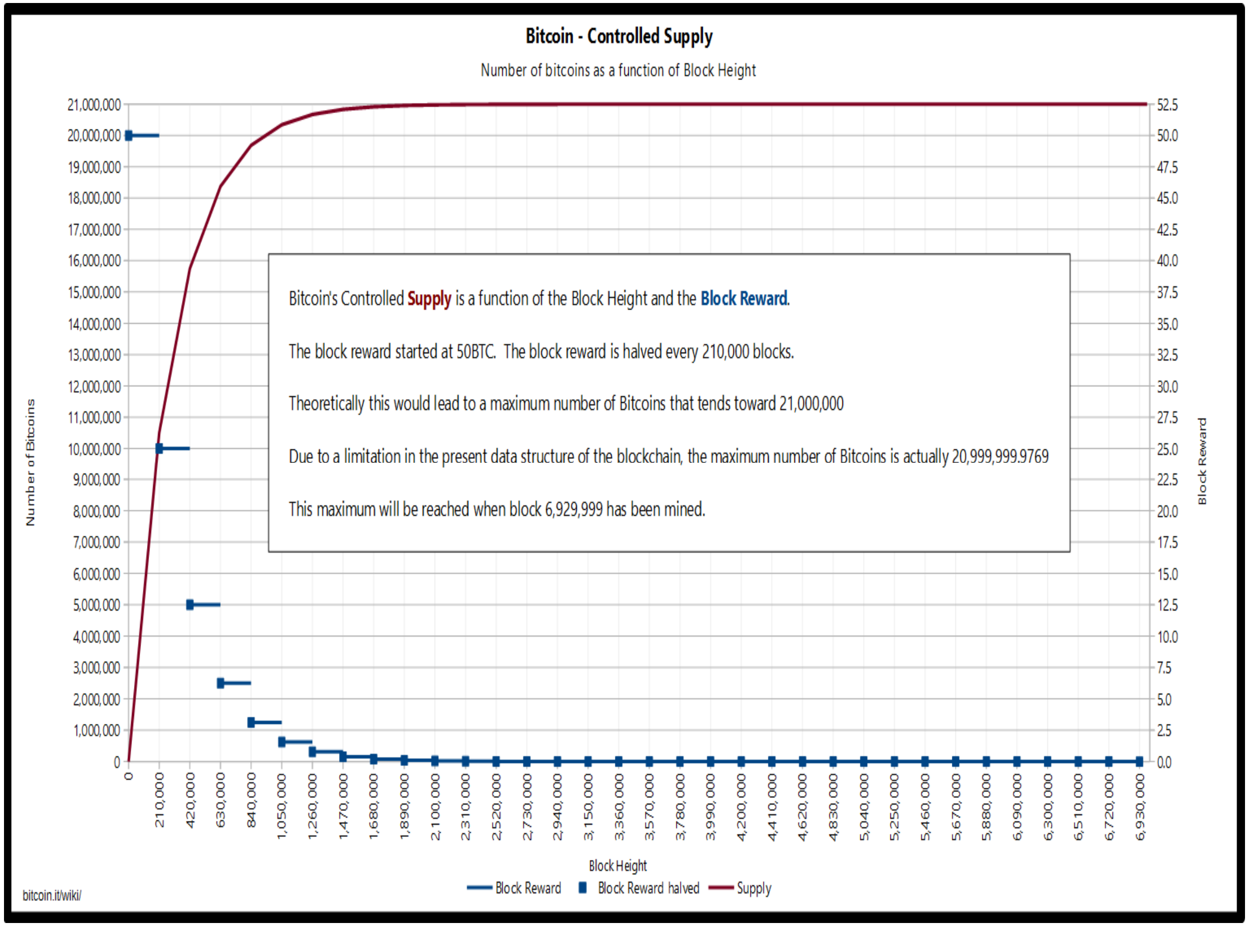
- Bitcoins also don’t move around when they are transferred. They are best understood as entries in a giant ledger, the “blockchain”, which contains the transaction history for every Bitcoin in circulation.
- It is kept up to date with the help of cryptography and copious computing power, provided by a global network of tens of thousands of computers.
- Again, openness helps the system remain secure: the blockchain is public so every participant can check whether a transfer comes from the rightful owner.
- Chain of possession/title is preserved.

Bitcoin Architecture

- The mathematic rules governing the bitcoin mining process are designed to mimic gold.
- A decreasing-supply algorithm was chosen because it approximates the rate at which commodities like gold are mined.
- Bitcoins are created each time a user discovers a new block.
- The rate of block creation is adjusted every 2016 blocks to aim for a constant two week adjustment period (equivalent to 6 per hour.)
- The number of bitcoins generated per block is set to decrease geometrically, with a 50% reduction every 210,000 blocks, or approximately four years.
- The result is that the number of bitcoins in existence will not exceed slightly less than **21 million**.

Total Bitcoins in Circulation

Graph



Bitcoin's Controlled Supply is a function of the Block Height and the Block Reward.

The block reward started at 50BTC. The block reward is halved every 210,000 blocks.

Theoretically this would lead to a maximum number of Bitcoins that tends toward 21,000,000

Due to a limitation in the present data structure of the blockchain, the maximum number of Bitcoins is actually 20,999,999.9769

This maximum will be reached when block 6,929,999 has been mined.

bitcoin.it/wiki/

Locked Formula

$$\frac{\sum_{i=0}^{32} 210000 \left\lfloor \frac{50*10^8}{2^i} \right\rfloor}{10^8}$$

Blockchain Transaction

- When two parties wish to engage in a transaction, they must broadcast it to the entire network, effectively asking network participants to determine its authenticity.
- Party A begins by broadcasting a message to the network signaling the terms of the agreement.
  - For example, “I, Party A, am giving Party B one bitcoin.”
- Next, Party B accepts the transaction by broadcasting its acceptance to the entire network and asking network participants to determine the authenticity of the transaction.
- The network automatically validates the transaction—or guards against the threat of double spending—through a “proof-of-work” validation system.
- If the transaction is validated, the ledger is updated and network users’ blockchain records are collectively updated. In other words, once a transaction has been recorded in this transparent public ledger, that transaction cannot be changed after the fact.

Criminal Conduct

- Because of bitcoin's decentralized nature, nation-states cannot shut down the network or alter its technical rules.
- However, the use of bitcoin can be criminalized, and shutting down exchanges and the peer-to-peer economy in a given country would constitute a "de facto ban“.
- Australian researchers have estimated that 25% of all bitcoin users and 44% of all bitcoin transactions are associated with illegal activity as of April 2017.
- There were an estimated 24 million bitcoin users primarily using bitcoin for illegal activity, who held $8 billion worth of bitcoin, and made 36 million transactions valued at $72 billion.

Ethereum vs. Bitcoin

- Bitcoin is only one of several hundred applications that use blockchain technology today.
- While all blockchains have the ability to process code, most are severely limited.
- While the Bitcoin blockchain is used to track ownership of digital currency (bitcoins), the Ethereum blockchain focuses on running the programming code of any decentralized application.
- Building blockchain applications has required a complex background in coding, cryptography, mathematics as well as significant resources.
- Ethereum provides developers with the tools to build decentralized applications.
- Rather than giving a set of limited operations, Ethereum allows developers to create whatever operations they want.
- This means developers can build thousands of different applications that go way beyond anything we have seen before.

Example of Digital Hack

- In 2016, a startup working on one particular DOA project, got hacked.
- The DAO was a project developed and programmed by a team to build a humanless venture capital firm that would allow investors to make decisions through smart contracts.
- The DAO was funded through a token sale and ended up raising around $150 million dollars from thousands of different people.
- Shortly after the funds were raised, the DAO was hacked by an unknown attacker who stole Ether (digital coins) worth around $50 million dollars at the time.
- While the attack was made possible by a technical flaw in the DAO software, not the Ethereum platform itself, the developers and founders of Ethereum were forced to deal with the mess.

Digital Hack

- After much debate, the Ethereum community voted and decided to retrieve the stolen funds by executing what's known as a hard fork or a change in code.
- The hard fork moved the stolen funds to a new smart contract designed to let the original owners withdraw their tokens.
- The implications of this decision are controversial and the topic of intense debate.
- Ethereum is based on blockchain technology where all transactions are meant to be irreversible and unchangeable.
- By executing a hard fork and rewriting the rules by which the blockchain executes, Ethereum set a dangerous precedent that goes against the very essence of blockchain.
- The Ethereum community and its founders were placed in a perilous position. If they didn't retrieve the stolen investor money, confidence in Ethereum could be lost.
- On the other hand, recovering investor money required actions that went against the core ideals of decentralization and set a dangerous precedent.

Blockchain Reflections

- A blockchain is an electronic ledger—a list of transactions.
- Those transactions can in principle represent almost anything.
  - They could be actual exchanges of money, as they are on the blockchains that underlie cryptocurrencies like Bitcoin.
  - They could mark exchanges of other assets, such as digital stock certificates.
  - They could represent instructions - smart contracts, which are computerized instructions to do something.
- Instead of being managed by a single *centralized* institution, such as a bank or government agency, it is stored in multiple copies on multiple independent computers within a *decentralized* network.
- No single entity controls the ledger.
- Any of the computers on the network can make a change to the ledger, but only by following rules dictated by a “consensus protocol,” a mathematical algorithm that requires a majority of the other computers on the network to agree with the change.

Blockchain Reflections

- Once a consensus generated by that algorithm has been achieved, all the computers on the network update their copies of the ledger simultaneously. If any of them tries to add an entry to the ledger without this consensus, or to change an entry retroactively, the rest of the network automatically rejects the entry as invalid.
- Typically, transactions are bundled together into blocks of a certain size that are chained together (hence “blockchain”) by cryptographic locks, themselves a product of the consensus algorithm. This produces an *immutable,* shared record of the “truth,” one that—if things have been set up right—cannot be tampered with.
- A public, “permissionless” blockchain ledgers, permits anyone to become part of the network; these are what Bitcoin and most other cryptocurrencies belong to.
- A private, “permissioned” ledger systems that incorporate no digital currency, can be used by a group of organizations that need a common record-keeping system but are independent of one another and perhaps don’t entirely trust one another—a manufacturer and its suppliers, for example.
- The common thread between all of them is that mathematical rules and impregnable cryptography, rather than trust in fallible humans or institutions, are what guarantee the integrity of the ledger.
- It can be described as “triple-entry bookkeeping”: one entry on the debit side, another for the credit, and a third into an immutable, undisputed, shared ledger.

Summary Cryptocurrency

- **Irreversible**
  - After you send a cryptocurrency and the network has confirmed it, you can't retrieve it. Cryptocurrencies are one way, no chargebacks.
- **Anonymous – KEY BENEFIT FOR SOME**
  - Anyone can open a wallet, no ID required, and have varying stages of anonymity depending on which token you utilize.
- **Fast and Globally Accessible**
  - Entries are broadcast across the network immediately and are confirmed in a couple of minutes.
- **Secure**
  - Cryptocurrencies use the latest cryptographic techniques.
- **Controlled Supply Limited by the Network**

Thank you

Aiyaz A. Alibhai
E: aalibhai@millerthomson.com
T: 604.643.1233

FORWARD TOGETHER

MILLER THOMSON

AVOCATS | LAWYERS

MILLERTHOMSON.COM

This presentation is provided as an information service and is a summary of current legal issues. This information is not meant as legal opinion and viewers are cautioned not to act on information provided in this publication without seeking specific legal advice with respect to their unique circumstances.

VANCOUVER CALGARY EDMONTON SASKATOON REGINA LONDON KITCHENER-WATERLOO GUELPH TORONTO VAUGHAN MARKHAM MONTRÉAL