

Blockchain Basics and Hands-on Guidance

Taking the Next Step toward Implementation and Adoption -
Classroom Use Case

By Deniz Appelbaum and
Sean Stein-Smith

Agenda

- Introduction
- Technology and Accounting
- The Basics of Blockchain and Updates
- Real World Applications
- Blockchain Demonstrations for the Classroom
- How Blockchain Will Change the Profession
- Moving Forward and Conclusion

Bios

Deniz Appelbaum

- Assistant Professor, Montclair State University of New Jersey
- Founder of Dronnovation LLC, advisory service for drones in auditing
- Speaks internationally on technology innovations in auditing
- Numerous academic papers
- Active member of the Rutgers CARLab

Sean Stein Smith

- Assistant Professor, Lehman College, City University of New York
- Member of Advisory Board of the Wall Street Blockchain Alliance
- 40 under 40 CPA Practice Advisor in 2017 and 2018
- Dozens of articles and publications on blockchain applications for accounting

Agenda

- Introduction

Kick off Questions

- Who here has dealt with cryptocurrency questions from clients, students, or colleagues?
- How many of you think you *will* be dealing with these types of questions more often going forward?
- The real question is, however, does everyone understand blockchain itself?

Introduction

- Our presentation will focus on blockchain technology
- 1) Definitions
- 2) Applications
- 3) Use cases
- 4) Options already in the marketplace
- 5) What you can do moving forward
- That said, blockchain is not the only force driving change

Agenda

- Introduction
- Technology and Accounting

Technology and Accounting

- Technology is nothing new for the accounting profession, or how accounting educators
- That said, there do appear to be several trends converging that are making the accounting and finance space, and accounting education, especially challenging

Technology trends to watch

- Robotic Process Automation
- Cryptocurrency
- Artificial Intelligence
- Automation
- Digitization

- Blockchain

Agenda

- Introduction
- Technology and Accounting
- The Basics of Blockchain and Updates

What is blockchain?

- A blockchain is a historical record of transactions, just like a database set up in Access or Excel
- It is NOT a general ledger or accounting platform
 - Popular misconception
- What this enables is security over the information stored in the blockchain, not in the journal entry process

Blockchain overview, cont.

- These blocks have a header that contains information and data about that block
 - Remember that the block contains information about the transactions that are included in the block
 - Reference to the previous block in the blockchain
 - A unique identifier “hash figure” that is assigned to each block in the chain
- Although all of this information is contained, the identities of the involved parties may not be

Blockchain overview, cont.

- Blockchain is a distributed ledger technology (DLT)
- In other words, this means that no single organization or participant owns the ledger or is in charge of validating and recording the individual transaction in the blockchain
- This information is available in real-time, to all participants who participate in the blockchain

Blockchain overview, cont.

- After these blocks of information have been entered in the blockchain, they must be verified by other participants
- Verification by consensus is a critical component of the blockchain technology
 - Requires that everybody involved in the blockchain network verify and validate transactions entered into the blockchain
 - Different options exist for validation
- After this validation, it gets better!

Validation Options

- Proof of work
 - Bitcoin
 - Ethereum
- Proof of Stake
 - Requires holders of the associated cryptocurrency to "stake" the blockchain to help validate transactions
- Proof of Elapsed Time

Consensus Options

- *Proof of Work (PoW)*: Requires only a single node to submit a solution to an algorithmic problem, which is very difficult to achieve but easy to verify once accomplished. This is the methodology used in both the Bitcoin and Ethereum blockchains, but consumes more electricity than other options, reducing applicability for large scale implementation. For midsize, and even large size CPA firms and clients, this approval protocol and consensus might not be efficient or applicable for daily utilization.

Consensus Options, cont.

- *Proof of Stake (PoS)*: Opposed to PoW, which is essential a competition to solve the algorithmic problem, the PoS protocol uses a lottery system to decide which nodes (members) will approve the transactions and information in question. The probability of being selected for approving transactions and information depends on the stake held by the organization or individual in question
 - Stake, in this conversation, refers to the number of Bitcoins or other altcoins held by the individual or organization
 - While this may result in some of the larger altcoin holders having outsize approval control over entries and blocks, these large stakeholders are also equally vested in the success and veracity of the network

Consensus options, cont.

- *Proof of Elapsed Time (PoET)*: Instead of the methodology underpinning the PoS protocol, the PoET assigns a random model to determine who will approve the block of pending information. The node (member) with the shortest wait time wins the lottery but will have to wait a certain amount of time before approving additional blocks. One item to keep in mind is that, in order to utilize the PoET the nodes involved must run Intel Software Guard Extension, which may pose issues for some organizations and clients.



Why does consensus matter?

- How should this be approached and discussed in conversation?

Blockchain validation

- Blockchain technology can contain both financial and non-financial information
- This information is available, or distributed, to all other members of the network in near real-time
- Every transaction, after approval by members of the blockchain network, is given a time stamp to validate the information contained in the transactions

Blockchain Breakdown

- By this point you already know the basics of what blockchain is, and the components therein
 - Decentralized Ledger Technology (DLT)
 - Consensus verification
 - Immutable
 - Trustless ecosystem potential
- That said, how might you want to start the conversation with your colleagues, students, or other external partners?

Explaining blockchain

- Various analogies that you can, and might, use to help breakdown and explain what exactly blockchain represents
 - Internet 2.0
 - Internet of value
 - A decentralized network to store and transfer information
- But what about the basic terminology that drives and forms the blockchain technology

Decentralized

- A decentralized model is completely different than existing ways of doing business
- Governmental entities
- Organizations
- Exchanges
- Credit card processors
- All are trusted third party entities

Public Blockchain

- Public blockchains represent the ideal version of what blockchain was constructed to
 - Open to anyone to join.
 - Free to download and use
 - Completely decentralized
 - What most practitioners think of
- When you think of Bitcoin
 - Think of a public blockchain

Public Blockchain Analogy (non-technical)

- Think of a public blockchain like a cloud based Excel sheet
- Anyone can add information to this sheet
- All information must be verified by 51% of all existing members
 - Requires lots of electricity and servers to verify this information
 - One option

Private Blockchain

- Not a “pure” blockchain
- Organized by one firm (the organizer), and other organizations are invited to join the network
- Organizer can set the rules for who has what access levels
 - Like a Google Doc that you have set up and invited others to edit

Private Blockchain Analogy (non-technical)

- A massive Google spreadsheet that you have set up, and invited others to either
 - View
 - Edit
 - Comment
- Blends many of blockchain characteristics, but is run by an organizing firm

Private blockchain question

- One question I'm asked a lot is if private blockchain members can see the information as it is uploaded and approved, does that breach confidentiality?
- No!
- Without diving into the weeds only some information is included in the "header" with public/private key combination needed to unlock the data within the block

Agenda

- Introduction
- Technology and Accounting
- The Basics of Blockchain and Updates
- Real World Applications

Insurance applications

- Swiss Re, a global insurer and re-insurer launched a blockchain enabled insurance product
- Blockchain Insurance Industry Initiative B3i to explore the potential of blockchain and develop products for the market
- Can automate the agreement and execution of contracts that drive insurance claims, verifications, and payments

Who is involved?

- Aegon
 - Allianz
 - Munich Re
 - Swiss Re
 - Zurich
-
- http://www.swissre.com/reinsurance/insurers_and_reinsurers_launch_blockchain_initiative.html

Blockchain in Commercial Real Estate (CRE)

- Blockchain can help digitize, automate, and transfer in real time information and data connected to processing the paperwork associated with real estate contracts
- Leases
- Mortgages
- Title Searches
- Escrow accounts
- Deloitte free CPE session - <https://www2.deloitte.com/us/en/pages/financial-services/articles/blockchain-in-commercial-real-estate.html>

Real estate blockchain example

- Ubitquity – a real estate management and services organization using both current technology, and blockchain technology to track and manage real estate information
- Launched in 2016, and officially released the blockchain enabled service in 2017
- Currently piloting a SaS pilot program with the Land Records Bureau in Brazil and other confidential clients

How does it work?

- Designed as a parallel tool to record and track and record information currently in legacy data and document systems
- Including augmenting paper based systems
- Already works with UXTO based blockchains
 - Ethereum
 - Hyperleger
 - Multichain

Agenda

- Introduction
- Technology and Accounting
- The Basics of Blockchain and Updates
- Real World Applications

Real estate funding

- <https://cointelegraph.com/news/european-startup-to-enable-access-to-commercial-real-estate-for-small-investors>
- Blocksquare
- “Historically, real estate has been an attractive investment option only accessible to institutional shareholders, but tokenized real estate is set to change that so the financial barrier to entry becomes almost non-existent,” Denis Petrovic, Blocksquare’s cofounder and CEO, said in a press release.

Royalties and blockchain

- The current royalty market is filled with a lack of consistency, trust, consistency, and an overall lack of information
- Creates a system that is both inefficient and expensive
- Since authors, artists, and other recipients of royalties may not see eye-to-eye this creates an environment that definitely is an opportunity
- Not just for artists, however, involves all kinds of business

Blockchain royalty Co.

- BRC has developed the framework for an advanced royalty tracking system leveraging blockchain technology. BRC's system includes functionality to use smart contracts to automatically execute protocols, calculate payments and track revenues, all but eliminating the risk of error.
- <https://blockchainroyalty.io/>
- Will use private networks to secure and share encrypted information and develop smart contracts tailored to the specific client

Blockchain and food safety

- Food safety is an issues that matters
- Business and personal perspective, including notable failures around food safety and quality testing
- What are some current pain points in the food safety and inspection process that cause stress and possible failures

Food safety – current state

- Food safety and the operations related to how food items are inspected have not changed all that much
- Periodic inspections
- RFID technology track shipments of perishable items
- Only able to address spoilage or other issues after the fact

Walmart and IBM

- Are teaming up to try and operationalize blockchain networks with food safety measures to reduce instances or other damage
- Solves on the biggest additional issues with food – just where does food come from and is that supplier reliable/trustworthy?
- Several examples illustrate the potential of blockchain for assisting with food safety and transparency

Bananas and Mangos

- Proof of concept partnership with IBM and Wal-Mart was developed to track back a package of sliced mangos
- Pre-blockchain it took 6 days, 18 hours, and 26 minutes
- Post blockchain it took 2.2 seconds
- Took Walmart and IBM 30 days to develop this prototype tool
- Not perfect

Carbon trading pain points

- Lack of transparency
- Different regulations in different markets
- Various markets value carbon credits in different manners
- On a firm by firm basis, carbon credits are worth different amounts depending on the situation
- How can blockchain help with this?

Real Life Example

- L03, an energy startup in Brooklyn New York is rolling out blockchain networks to help streamline carbon credit trading and energy trading in general
- Also piggybacks on the increased interest for a decentralized power grid.
- What's a decentralized power grid – all those solar panels you see being put onto buildings all over the place 😊

L03

- Focusing on energy trading and distribution
- Think about what electricity actually is – data and energy being communicated from different producers to end users
- That is exactly what blockchain is focused on improving
- <https://lo3energy.com/>



Blockchain and Conflict Minerals/Gems

<https://www.trustchainjewelry.com/>

Blockchain and Delivery Drones

Walmart's Drone Delivery Plan Includes Blockchain Tech

2017-06-02 07:06:32 The Editor

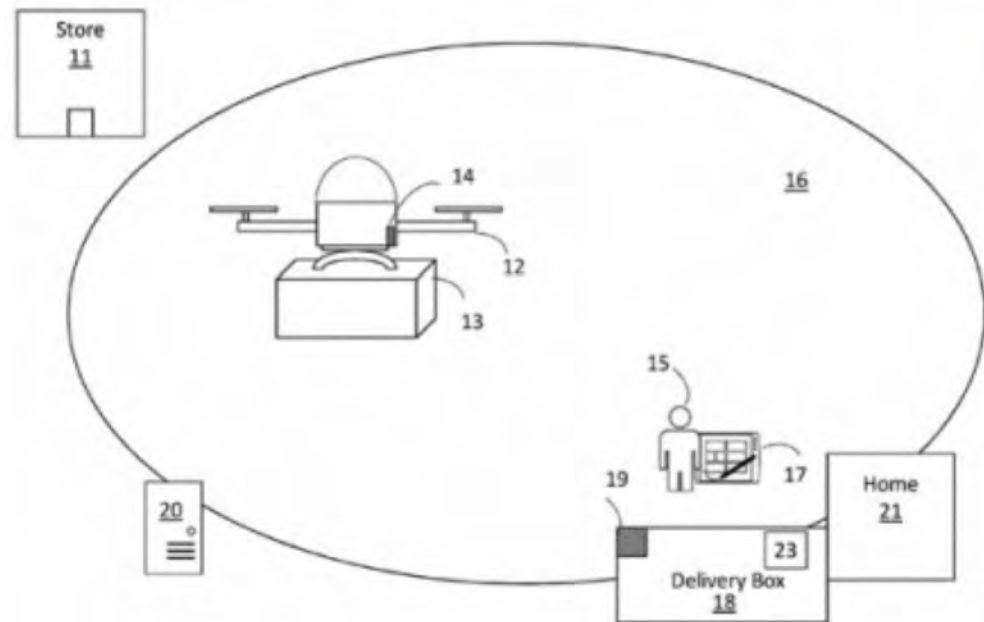


FIG. 1

Agenda

- Introduction
- Technology and Accounting
- The Basics of Blockchain and Updates
- Real World Applications
- Blockchain Demonstrations for the Classroom



BITCOIN
IN CRYPTOGRAPHY WE TRUST

[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#).

Bitcoin, Blockchain & Distributed Ledgers

By Deniz Appelbaum, PhD

(thanks to Lorraine Lee, PhD for template contribution)

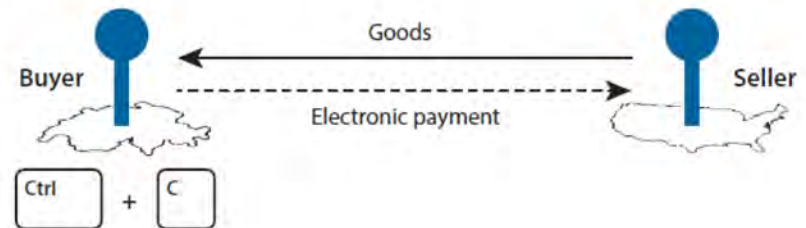


Cash and Electronic Payments

Figure 1
Cash Transaction



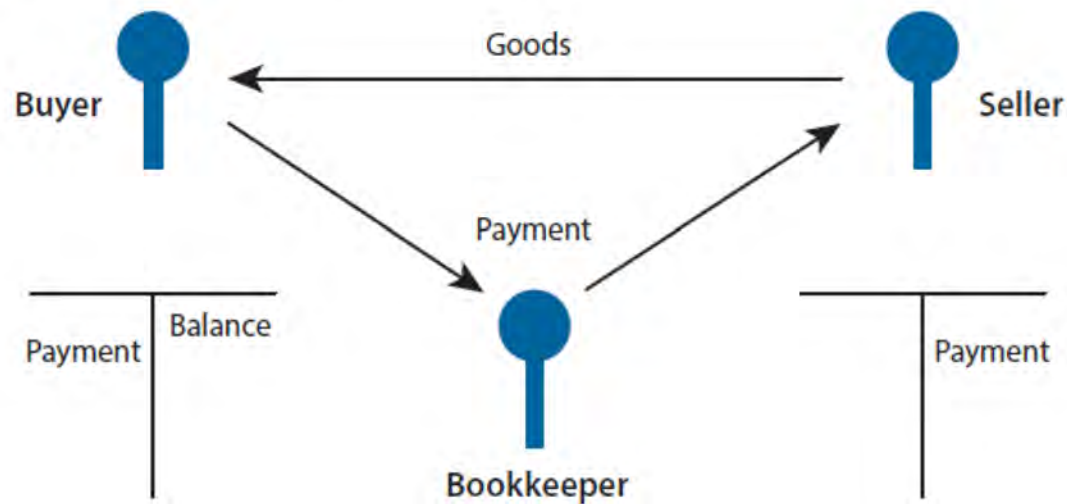
Figure 2
Electronic Payment



Payment System with a Central Authority

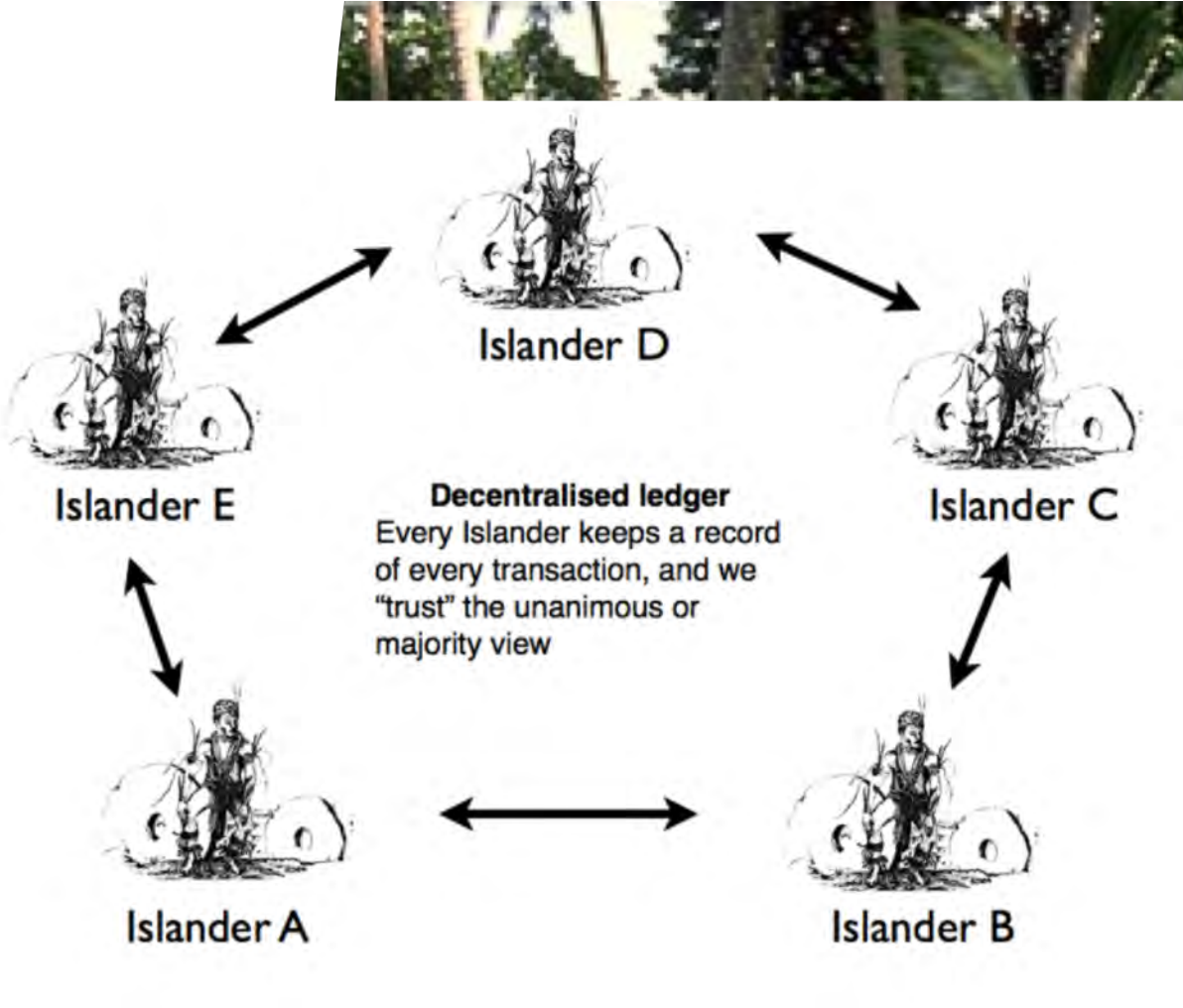
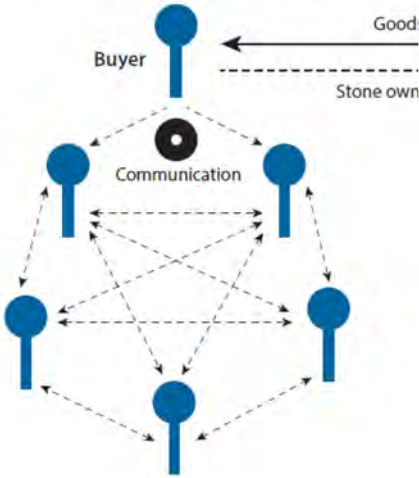
Figure 3

Payment System with a Central Authority



Stone Money Island of Yap

Figure 4
Payment System with a Distributed Ledger



Bitcoin | Previous attempts of digital money

- Bitcoin: m...
- Each bitco...
- Bitcoin Blo...
- Blockchain
 - No single
 - Every pa
 - “public r
- Bitcoin: cu

ACC	CyberCents	IKP	MPTP	Proton
Agora	CyberCoin	IMB-MP	Net900	Redi-Charge
AIMP	CyberGold	InterCoin	NetBill	S/PAY
Allopass	DigiGold	Ipin	NetCard	Sandia Lab E-Cash
b-money	Digital Silk Road	Javien	NetCash	Secure Courier
BankNet	e-Comm	Karma	NetCheque	Semopo
Bitbit	E-Gold	LotteryTickets	NetFare	SET
Bitgold	Ecash	Lucre	No3rd	SET2Go
Bitpass	eCharge	MagicMoney	One Click Charge	SubScrip
C-SET	eCoin	Mandate	PayMe	Trivnet
CAFÉ	Edd	MicroMint	PayNet	TUB
CheckFree	eVend	Micromoney	PayPal	Twitpay
ClickandBuy	First Virtual	MilliCent	PaySafeCard	VeriFone
ClickShare	FSTC Electronic Check	Mini-Pay	PayTrust	VisaCash
CommerceNet	Geldkarte	Minitix	PayWord	Wallie
CommercePOINT	Globe Left	MobileMoney	Peppercoin	Way2Pay
CommerceSTAGE	Hashcash	Mojo	PhoneTicks	WorldPay
Cybank	HINDE	Mollie	Playspan	X-Pay
CyberCash	iBill	Mondex	Polling	

Table 1: Notable electronic payment systems and proposals

Source: eBook of Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction

S
;
mous

Bitcoin Introduction

- How to buy Bitcoins:
 - Potential buyer downloads “bitcoin wallet” software
 - Load fiat currencies in the wallet/link credit card ~/open account in exchange
 - Bid to purchase satoshis/coins = options market, but with small bid-ask spreads
- Purchases and creations of bitcoin occur via consensus of “proof of work”
 - “proof of work” hashing algorithms and popular sentiment are the key value drivers for Bitcoin and virtual currencies
 - Is this a problem? How is it different from paper money, U.S. \$\$\$?
- How did bitcoin begin???.....

Introduction: The Advent of BitCoin-Blockchain

- Satoshi Nakamoto (2008)
- Provides a means for many participants of different locations to jointly record their transactions in a commonly shared master file.
- BC should be able to reduce assurance tests conducted by auditors



No one knows the real face behind Satoshi Nakamoto

Introduction

- Would a Bitcoin-Blockchain look like this:



- Or this?

Understanding Nakamoto: Problem Identification and Motivation

- Nakamoto's 2008 original paper on Bitcoin
- Core components of DLTs:
 - There is no trusted 3rd party required, network is peer-to-peer
 - New transactions are time-stamped and hashed onto an ongoing chain of transactions
 - The hashed record cannot be changed without redoing the proof-of-work
 - Proof-of-work is accomplished by a pool of CPUs from the peer-to-peer network through computation
 - The longest chain (block of transactions) includes the latest transaction and requires the most CPU work to create the hash, therefore it takes the most times, to date, to compute the hash (10 minutes per transaction)
 - The system works as long as the majority of peer-to-peer nodes are not colluding to subvert the chain since they could collectively represent the majority of the computing power and could compute the hash faster than any other group/participant

Working through each of these components

- First, as a design requirement, avoid the use of a third-party countersigner or oracle
 - Peer-to-peer level of trust:
 - Timestamping individual transactions
 - Hashing the transaction sequence of block using an algorithm with special properties
 - Publicly auditable cost function (hash) of Nakamoto
 - Takes longer to compute the hash value as the length of the block increases
 - Efficiently verifiable by anyone without any special information
 - Computationally expensive to alter a transaction in the hash
 - Hash for the transaction itself and all subsequent hashes will need to be re-computed
 - If valid transactions are subsequently added, perpetrator's work is increased
 - Not impossible, but infeasible and time consuming
 - But perhaps with quantum computers....

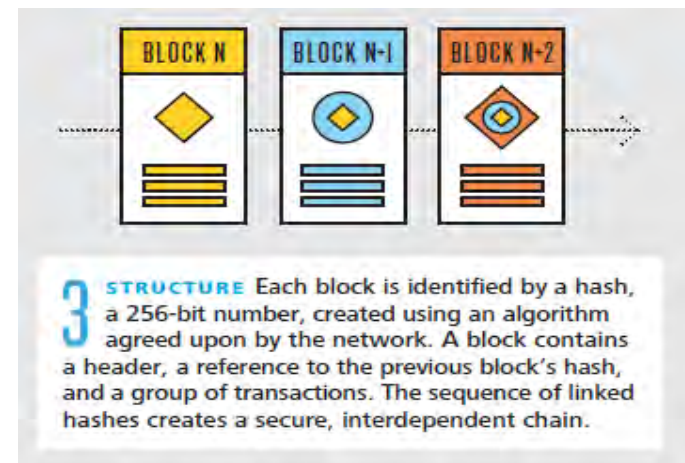
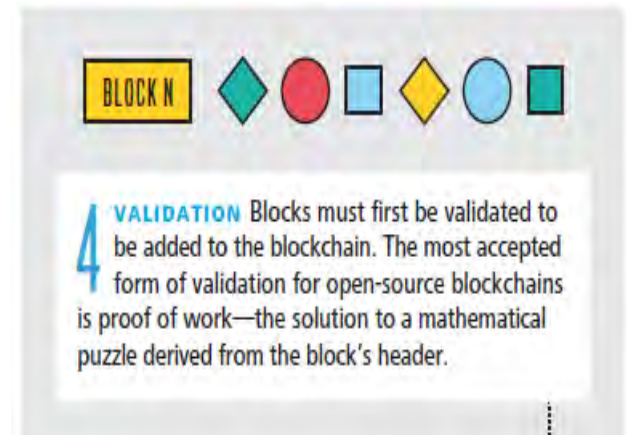
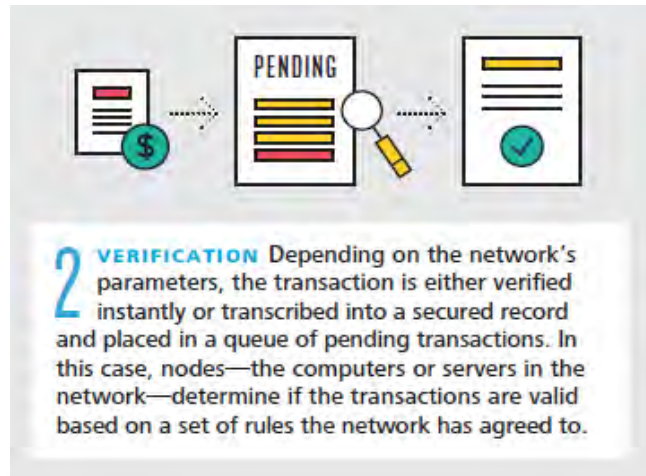
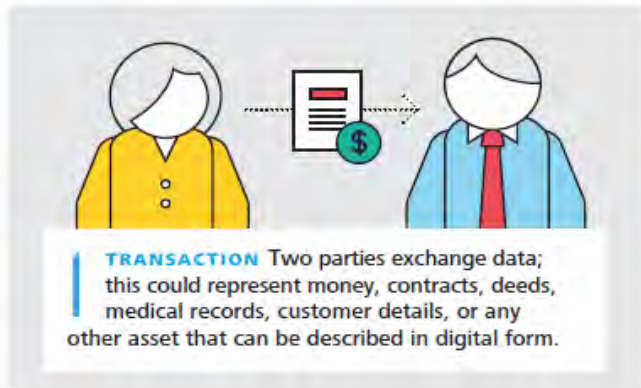
Working through each of these components

- Next design requirement: Hash as proof-of-work
- Third Component: The block cannot be changed without re-computing a new hash for every step and configuration!
- Fourth: Some cooperation amongst peers is required for operational efficiency.
- Fifth: The latest un-hashed block contains all of the transaction history of previous transactions and hashes.
- Sixth: as long as the majority of peer nodes are not actively trying to subvert the network, they can complete the future hashes faster than fraudulent peers

Deloitte -Blockchain: How it works

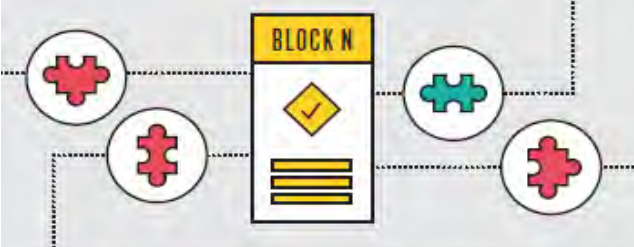
Figure 1. Blockchain: How it works

Blockchain allows for the secure management of a shared ledger, where transactions are verified and stored on a network without a governing central authority. Blockchains can come in different configurations, ranging from public, open-source networks to private blockchains that require explicit permission to read or write. Computer science and advanced mathematics (in the form of cryptographic hash functions) are what make blockchains tick, not just enabling transactions but also protecting a blockchain's integrity and anonymity.




Source: Deloitte, Blockchain: Democratized trust Distributed ledgers and the future of value

Blockchain: How it works (cont.)



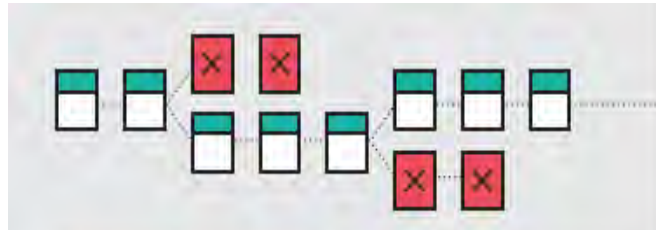
The diagram shows a central box labeled 'BLOCK N' containing a yellow diamond with a checkmark and three horizontal lines. This box is connected by dashed lines to four circular icons, each containing a puzzle piece. The puzzle pieces are red and green, representing the process of solving a cryptographic puzzle.

5 BLOCKCHAIN MINING Miners try to “solve” the block by making incremental changes to one variable until the solution satisfies a network-wide target. This is called “proof of work” because correct answers cannot be falsified; potential solutions must prove the appropriate level of computing power was drained in solving.



The diagram shows a network of five computer monitors connected by dashed lines. Each monitor has a checkmark on its screen. Small yellow squares are scattered between the monitors, representing the distribution of a validated block to the network.

6 THE CHAIN When a block is validated, the miners that solved the puzzle are rewarded and the block is distributed through the network. Each node adds the block to the majority chain, the network’s immutable and auditable blockchain.



The diagram shows a sequence of blocks in a chain. The first two blocks are white with green tops. The next two blocks are red with red 'X' marks, indicating they are rejected. The final three blocks are white with green tops, showing the chain continuing with the majority.

7 BUILT-IN DEFENSE If a malicious miner tries to submit an altered block to the chain, the hash function of that block, and all following blocks, would change. The other nodes would detect these changes and reject the block from the majority chain, preventing corruption.

Source: Deloitte, Blockchain: Democratized trust
Distributed ledgers and the future of value

Bitcoin Mining/Hashing/Proof of Work

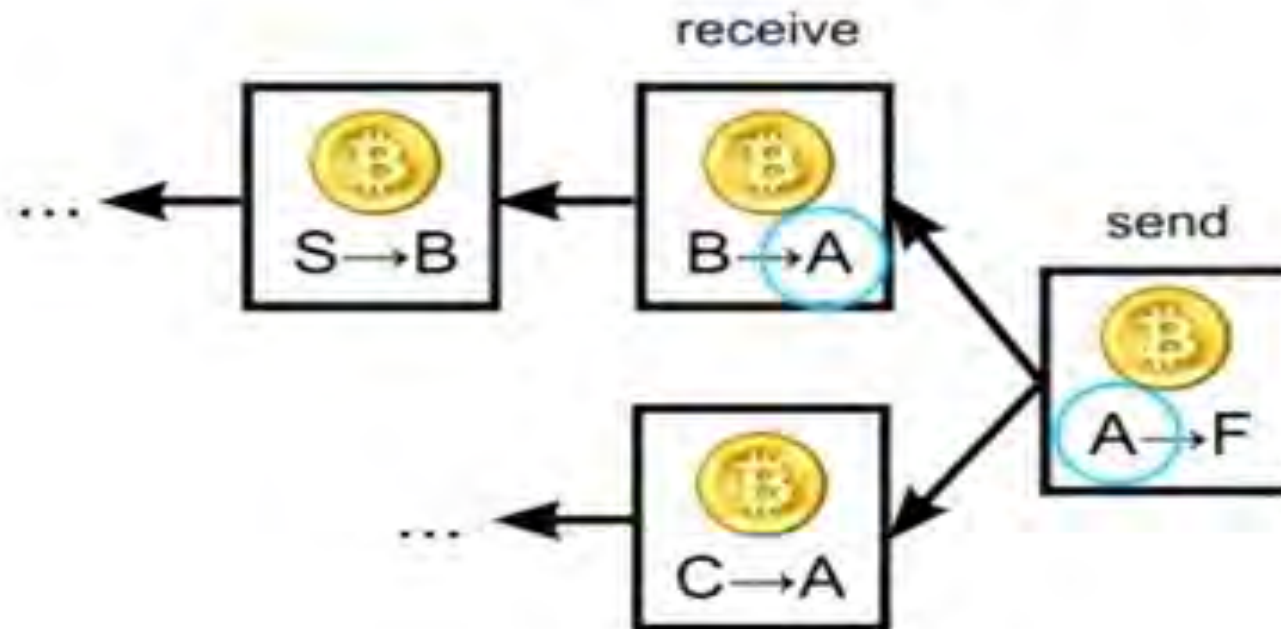
- Miner: collects transactions, verifies their legitimacy, then assembles them as a “block candidate”
 - Miner earns additional bitcoins by convincing others to accept the new block
 - Mining is permission-less, but huge power demands
 - Now only profitable for large mining concerns
- How is a block accepted?
 - All previous transactions must be legitimate
 - “fingerprint” of the block candidate: block candidate’s dSHA256 hash
 - <http://conversion-tool.com/sha256>
 - Deniz Appelbaum, PhD :
0309b0530cd5f4b9828807f465cdd3feb70be0d03c99cf12ce130c072180ab57
 - Deniz Appelbaum, PhD. :
6a7b896b85d97fccf16a6acb4da82041be3c09f0b58ac623db86882536ca47f8

Hash rate =
number of combinations guesses per second



The Blockchain

Bitcoin Generation



Transactions

A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

BLAST! OUR
EVIL PLAN
IS FOILED!

NO GOOD! IT'S
4096-BIT RSA!



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



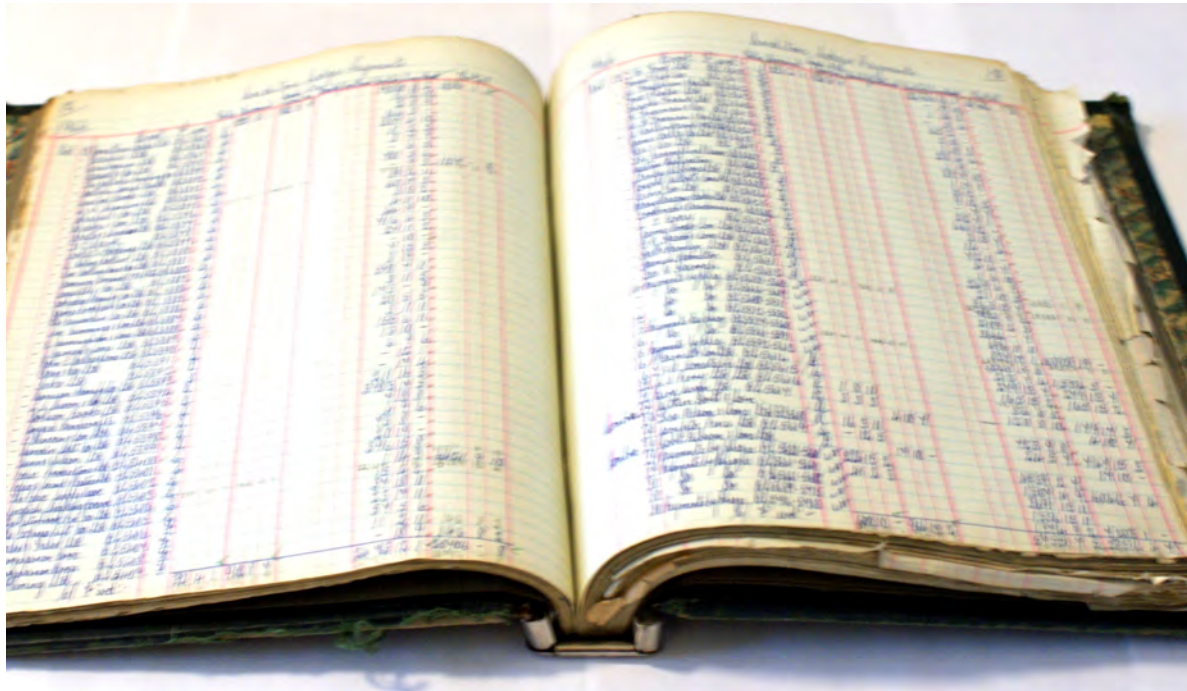
Blockchain Activity Overview

- Overview
- Traditional Ledgers
 - Transactions
 - Traditional Ledger System Diagram
- Distributed Ledgers
 - Transactions
 - Distributed Ledger System Diagram
 - Block Verifications
- Discussion/Assignment

Let's start by watching a video

Future Bank Today | Episode 4: BlockChain - Explain it like I am 5 (9:38)

- https://www.youtube.com/watch?v=tVmYaL_aBYc



Transactions – Traditional Accounting Ledger

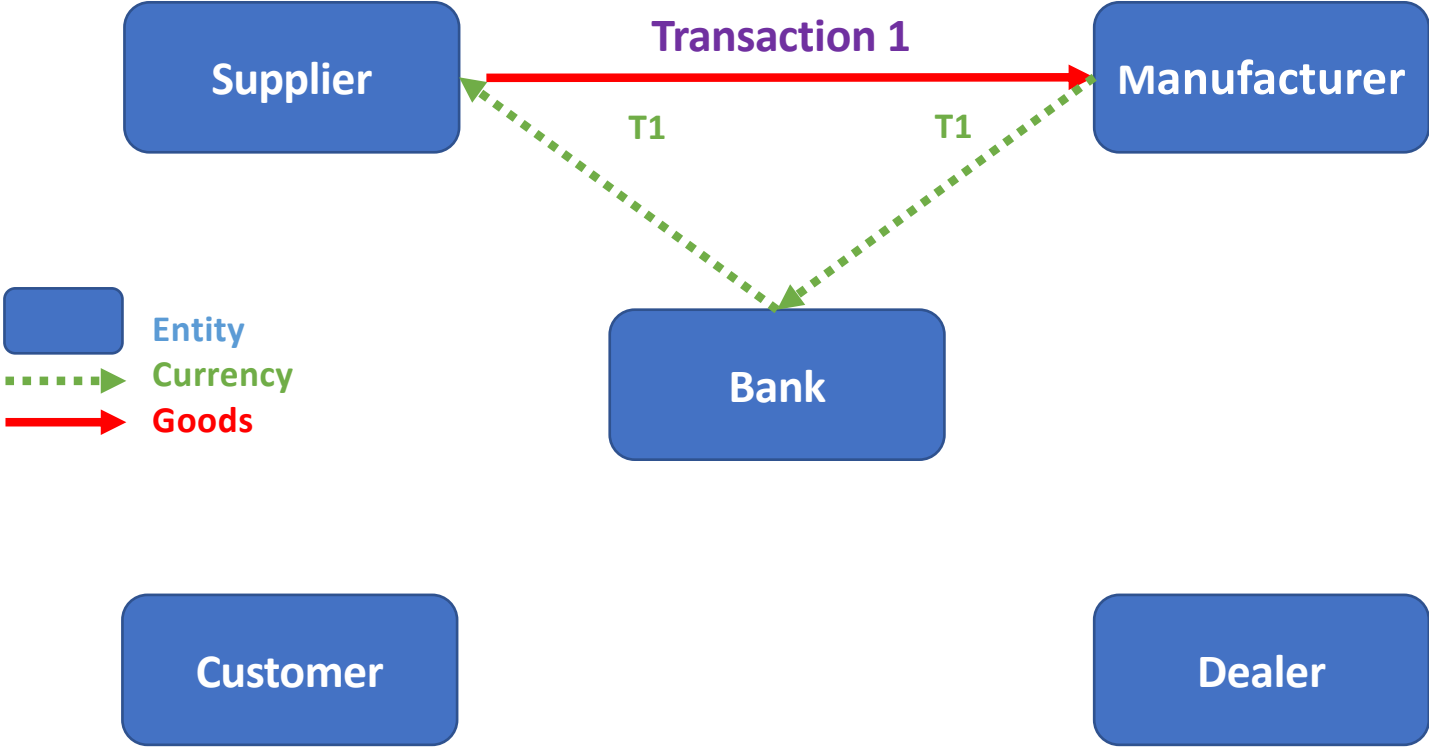
- For each transaction, three events occur:
 - Goods shipped from seller to buyer
 - Accounting information recorded by both parties
 - Payment remitted from buyer to seller



Transaction 1

Supplier sells raw materials to Manufacturer

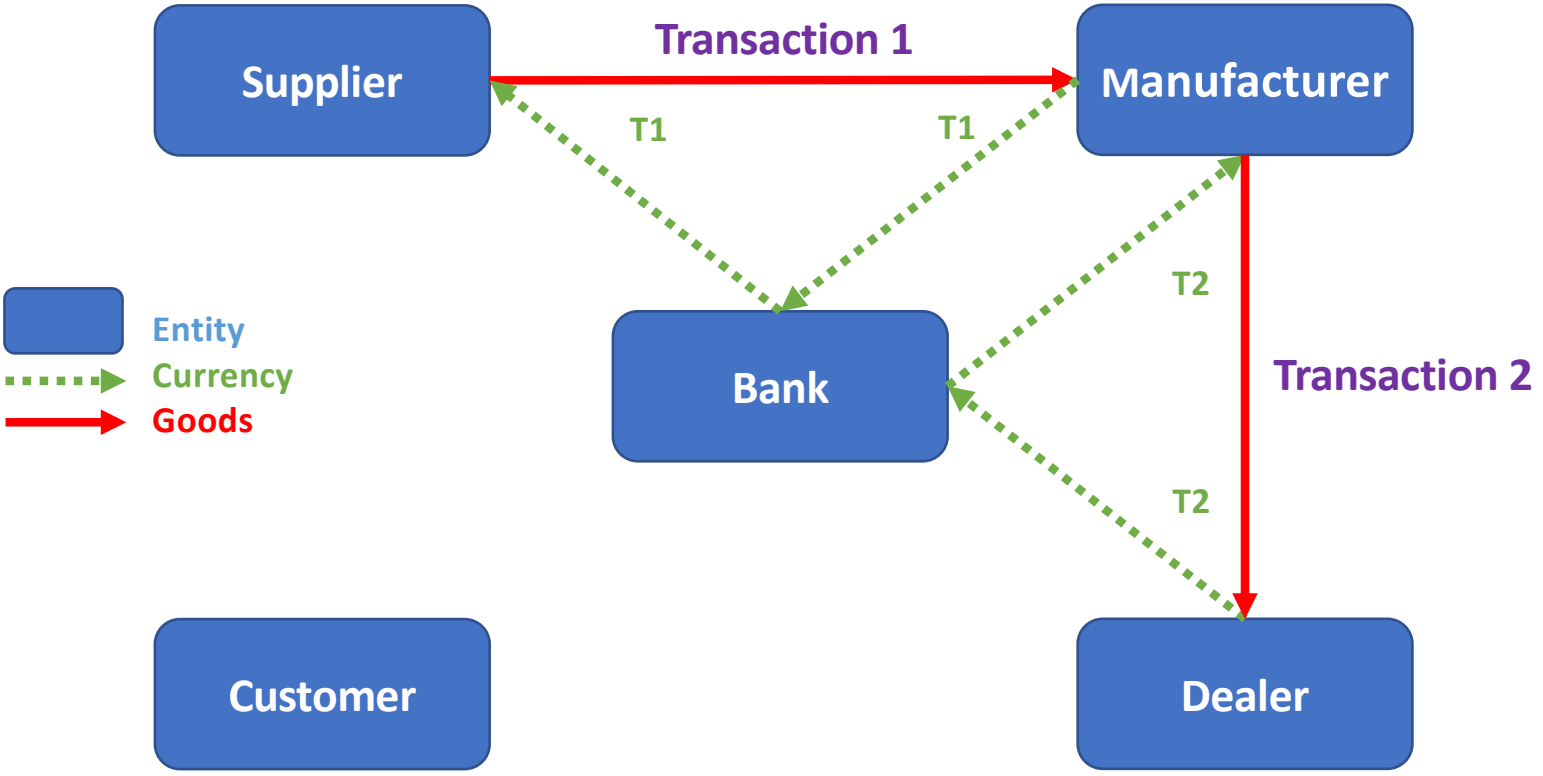
Traditional Ledger System Diagram



Transaction 2

Manufacturer sells finished goods to Dealer

Traditional Ledger System Diagram

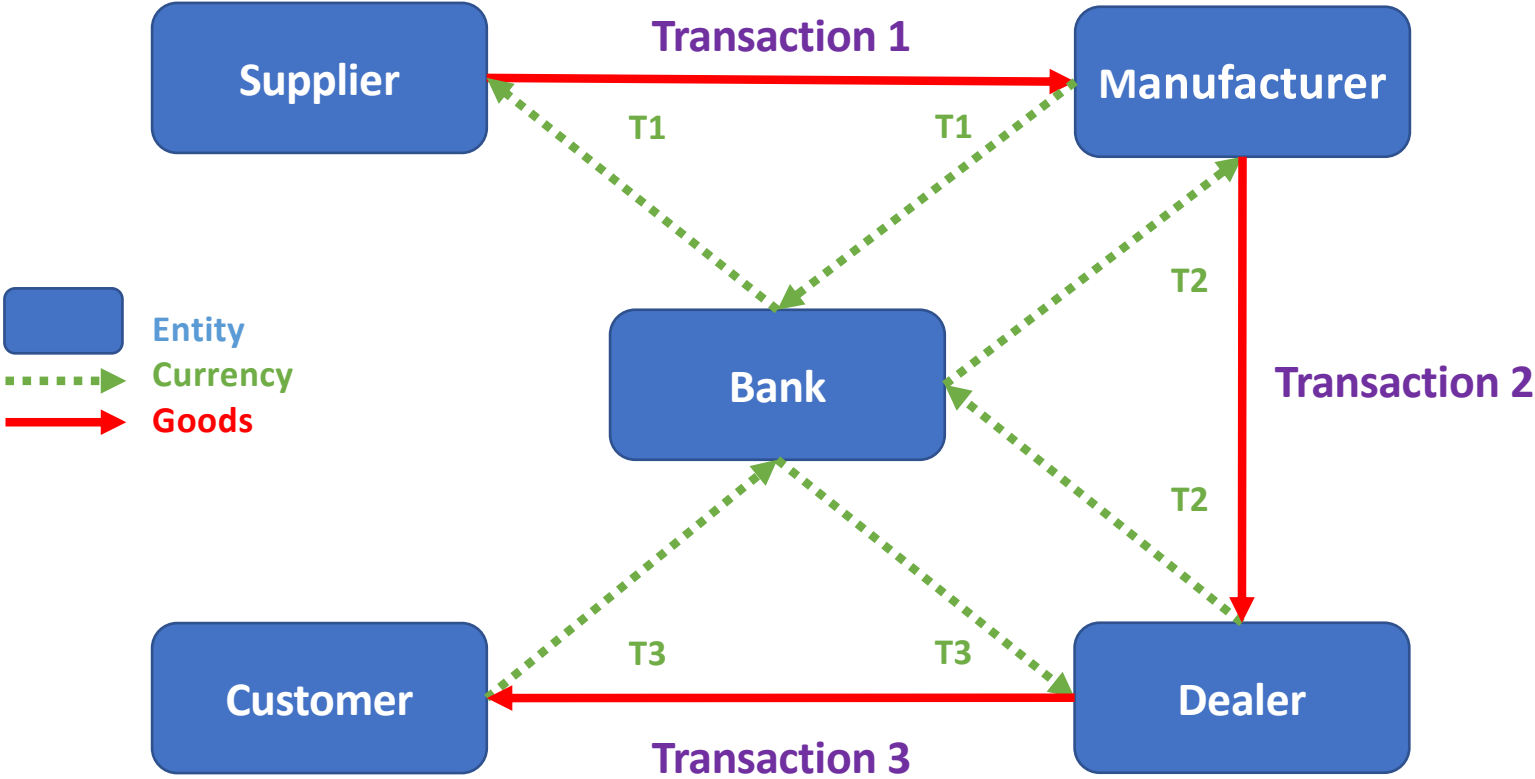




Transaction 3

Dealer sells inventory to Customer

Traditional Ledger System Diagram



Distributed Databases

- **Blockchain technology — a very special kind of Distributed Database**
- What is the difference between “blockchain technology” and “distributed ledger technology?”
 - So let’s clarify the conceptual & vocabulary issues that we have here.
- **Centralized relational databases**
- Relational databases (RDBMS) organize data in tables and use the SQL query language. They became the norm in the 80s. Even if their architecture evolved in complexity over time (n-tier, distributed processing, etc.) they remain essentially centralized i.e. located, stored, and maintained in a single location. This category represent more than 90% of the database market in terms of revenues and includes the most well-known vendors and systems: MySQL, Oracle, Microsoft SQL Server, IBM DB2, SAP, PostgreSQL, SQLite, Teradata, etc.

Source: <https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118>

Distributed Databases

Databases are distributed (DDBMS) when the storage devices are not all attached to a common processing unit such as the CPU, but are spread across a network. With the development of the internet, businesses needed solutions that could process huge amounts of structured & unstructured data, and that could scale across networks. DDBMS use consensus mechanisms to ensure fault-tolerant communications, and provide concurrency control through locking and/or time-stamping mechanisms. They come in different technology forms:

- **1. Peer network node data stores** are systems allowing users to replicate and share files across a network leveraging peer-to-peer protocols such as: BitTorrent, NNTP, Freenet, Mnet, etc.
- **2. Distributed SQL data warehouses** are systems designed by the major vendors (Microsoft, Oracle, SAP, IBM, etc.) to allow for the massively parallel processing of analytics-oriented tasks.
- **3. Hadoop** is an open-source software framework for storing data and running applications on clusters of commodity hardware. It provides massive storage for any kind of data, enormous processing power and the ability to handle virtually limitless concurrent tasks.
- **4. NoSQL** databases are non-relational DDBMS, horizontally scalable, designed for real-time web applications. The most well-known solutions are: MarkLogic, MongoDB, Datastax, Apache Cassandra, Redis, Riak, Google BigTable and CouchDB.
- **5. NewSQL** databases are relational DDBMS designed to combine the best of relational databases & NoSQL databases properties (horizontal scalability & distributed processing). Examples: Google Spanner, Clustrix, VoltDB, MemSQL, Pivotal's GemFire XD, NuoDB and Trafodion.

Source: <https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118>

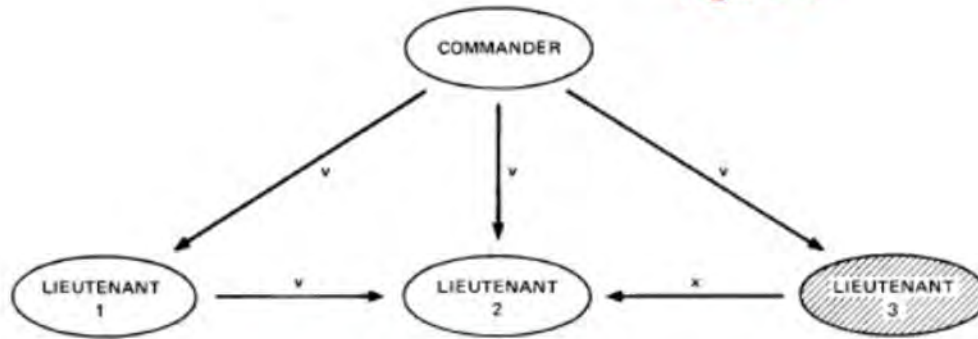
Distributed Ledgers

- **6. Distributed Ledgers (DL)** are DDBMS that leverage cryptography to provide a decentralized multi-version concurrency control mechanism and to maintain consensus about the existence and status of shared facts in trustless environments (i.e. when the participants hosting the shared database are independent actors that don't trust each other). Consensus is not a unique feature of DL per se: other distributed databases also use consensus algorithms such as Paxos or Raft. Same for immutability: immutable databases exist outside DL (Google HDFS, Zebra, CouchDB, Datomic, etc.). The two differentiators of DL in my opinion: (a) the control of the read/write access is truly decentralized and not logically centralized as for other distributed databases, and corollary (b) the ability to secure transactions in competing environments, without trusted third parties. Some people call this category "shared ledgers" but I prefer the term "distributed" because shared can mean "divided/split".
- **6.1.** The Bitcoin system was the first instance of DL, designed for one purpose: peer-to-peer bitcoin (cryptocurrency) payments. To avoid double spending, Bitcoin uses chained blocks of data (hence the "block chain") and a proof of work consensus among other mechanisms. Bitcoin is censorship resistant, its key features are: **byzantine-fault tolerant**, pseudo-anonymity, auditability (public), immutability, accountability (time-stamping) and non-repudiation (signature) at transaction level.
- **6.2.** Some systems are inspired by or somehow close to the Bitcoin system. They usually implement most of its features, but not all or with different characteristics. For instance:
- Other cryptocurrencies implement privacy mechanisms (Zcash), or different consensus protocols such as Proof of stake, Proof of burn, etc.
- Ethereum share many of Bitcoin features but is designed to execute programmable transactions (smart contracts)

Source: <https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118>

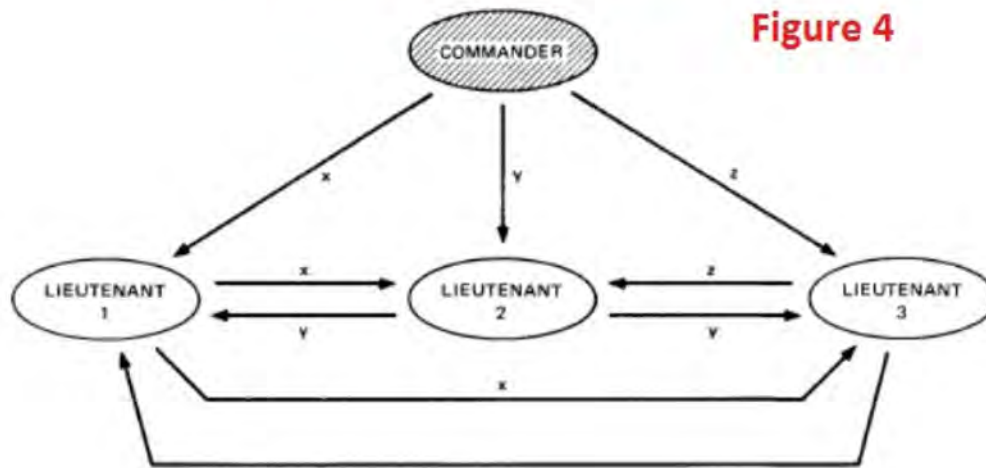
Byzantir

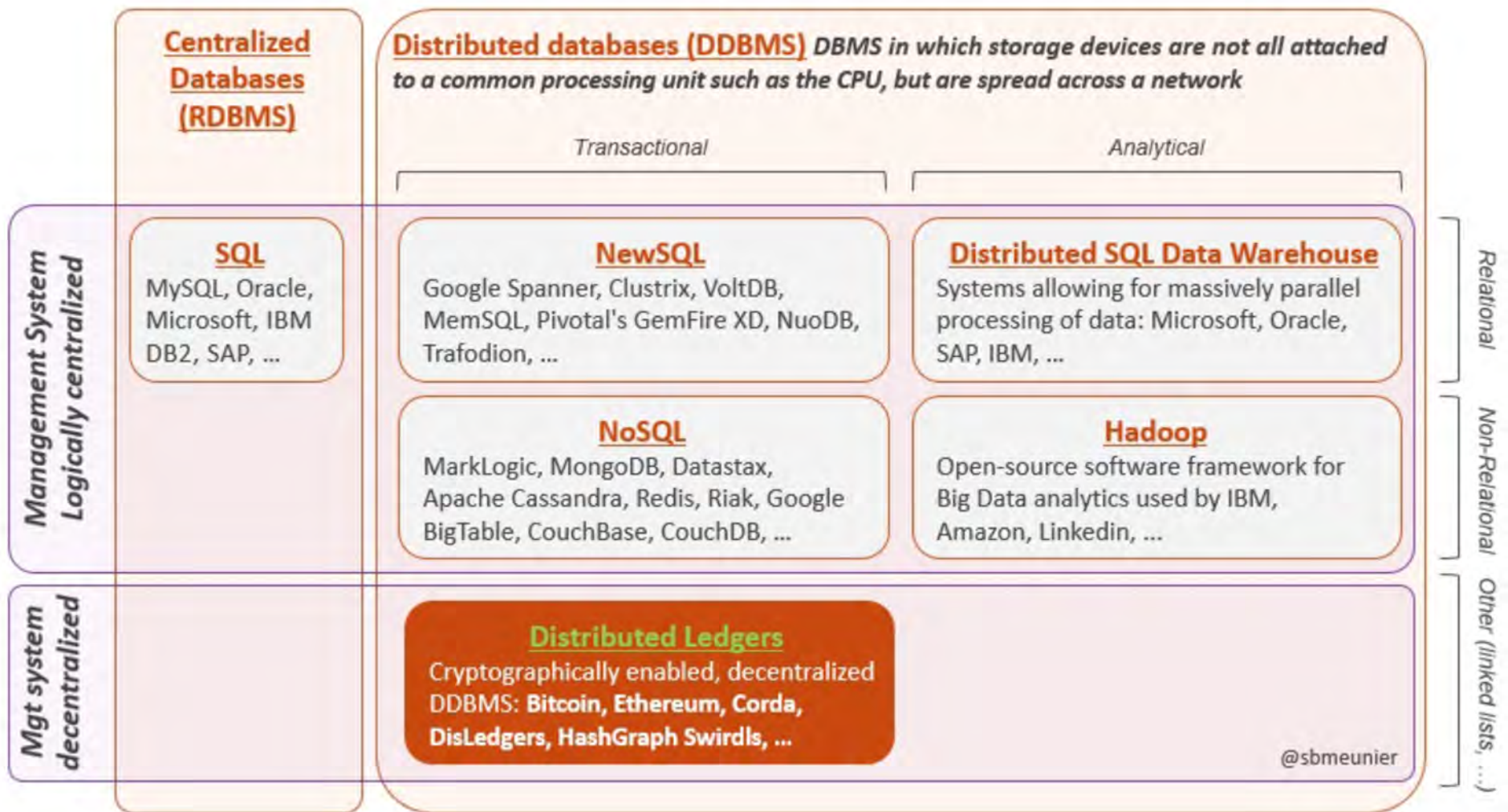
Figure 3



The one with stripes is the traitor because of which a consensus cannot be reached

Figure 4





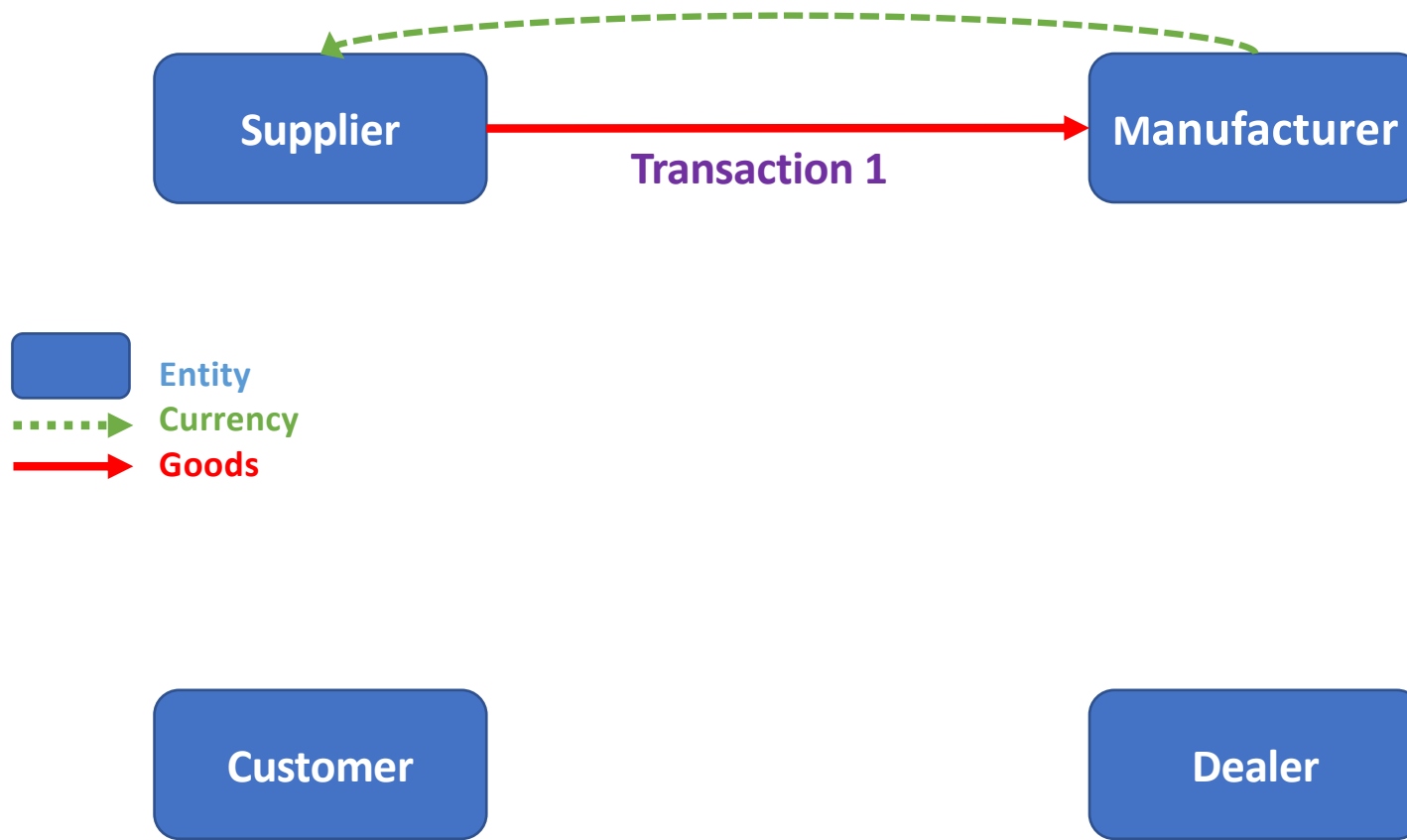
Source: <https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118>



Transaction 1

Supplier sells raw materials to Manufacturer

Distributed Ledger Transaction Diagram



Transaction 1: Blockchain – Block Verification Instructions

Go to a sha256 generator site: <http://hash.online-convert.com/sha256-generator>

Transaction 1:

Transaction ID: tx01

Description: “manufacturer purchased 10 widgets from supplier for 12BTC”

Value to Hash:

```
tx01:manufacturer purchased 10 widgets from supplier for 12BTC:xxxx
```

- xxxx is the “nonce”
 - Your job: Find the value of “xxxx” which will return a hashed value starting with a “0”
- Hash the transaction information + “ : ” + xxxx
 - Example:

Text you want to convert to a SHA-256 hash:

```
tx01:manufacturer purchased 10 widgets from supplier for 12BTC:0000
```

Your hash has been successfully generated.

```
hex: f5de8b125110f2bb6b56d13815787c8729a88c29c3dc6c63bf5a99d4f
HEX: F5DE8B125110F2BB6B56D13815787C8729A88C29C3DC6C63BF5A99D4F
h:e:x: f5:de:8b:12:51:10:f2:bb:6b:56:d1:38:15:78:7c:87:29:a8:8c
base64: 9d6LElEQ8rtrVtE4FXh8hymoJcN3Gxjv+tamdScjDE=
```


Blockchain – Post Transaction 1 Proof-of-Work

Text you want to convert to a SHA-256 hash:

```
tx01:manufacturer purchased 10 widgets from supplier for 12BTC:0036
```

Your hash has been successfully generated.

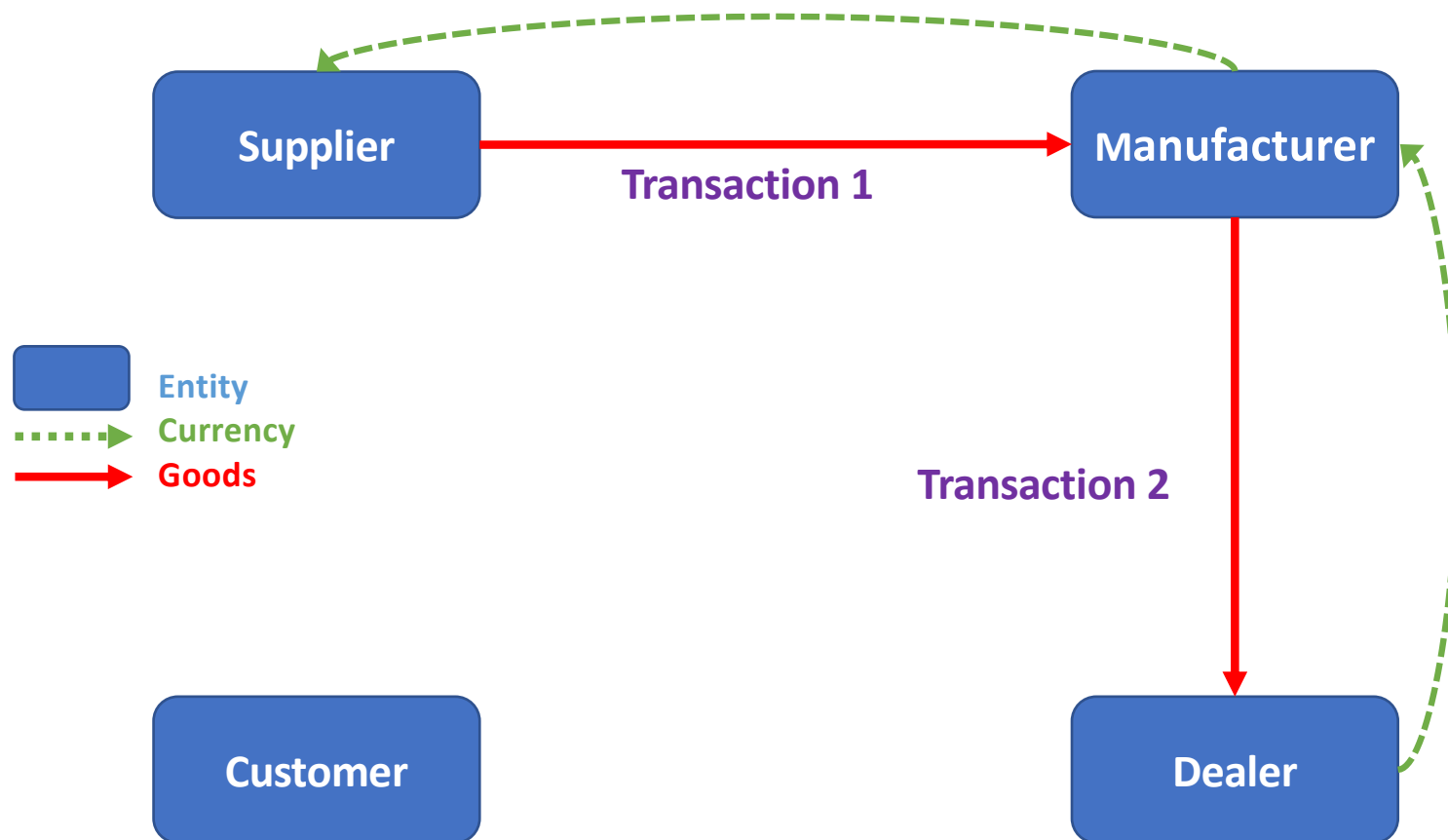
```
hex: 0584dccf9145ac2d2a422e1cda1ba384719432c5333e5a17e264566c8f  
HEX: 0584DCCF9145AC2D2A422E1CDA1BA384719432C5333E5A17E264566C8F  
h:e:x: 05:84:dc:cf:91:45:ac:2d:2a:42:2e:1c:da:1b:a3:84:71:94:32  
base64: BYTcz5FFrC0qQi4c2hujhHGUMsUzPloX4mRWbI9AAPk=
```



Transaction 2

Manufacturer sells finished goods to Distributer

Distributed Ledger Transaction Diagram



Blockchain –Transaction 2

- Transaction 2:
 - Previous block hash: 0584
 - Transaction ID: tx02
 - Description: “manufacturer sells final product to dealer for 15BTC”

Value to Hash:

0584-tx02-manufacturer sells final product to dealer for 15BTC:xxxx

Text you want to convert to a SHA-256 hash:

```
0584-tx02-manufacturer sells final product to dealer for 15BTC:0000
```

Your hash has been successfully generated.

```
hex: 4ce5c2d9b1c78ec0f45836082e9baf224c667c451d8a816dd41d6df8f0  
HEX: 4CE5C2D9B1C78EC0F45836082E9BAF224C667C451D8A816DD41D6DF8F0  
h:e:x: 4c:e5:c2:d9:b1:c7:8e:c0:f4:58:36:08:2e:9b:af:22:4c:66:7c  
base64: TOXC2bHHjsD0WDYILpuvIkxmfEUdioFt1B1t+PC88eY=
```


Bitcoin Blockchain – Post Transaction 2 Proof-of-Work

Text you want to convert to a SHA-256 hash:

```
0584-tx02-manufacturer sells final product to dealer for 15BTC:0006
```

Your hash has been successfully generated.

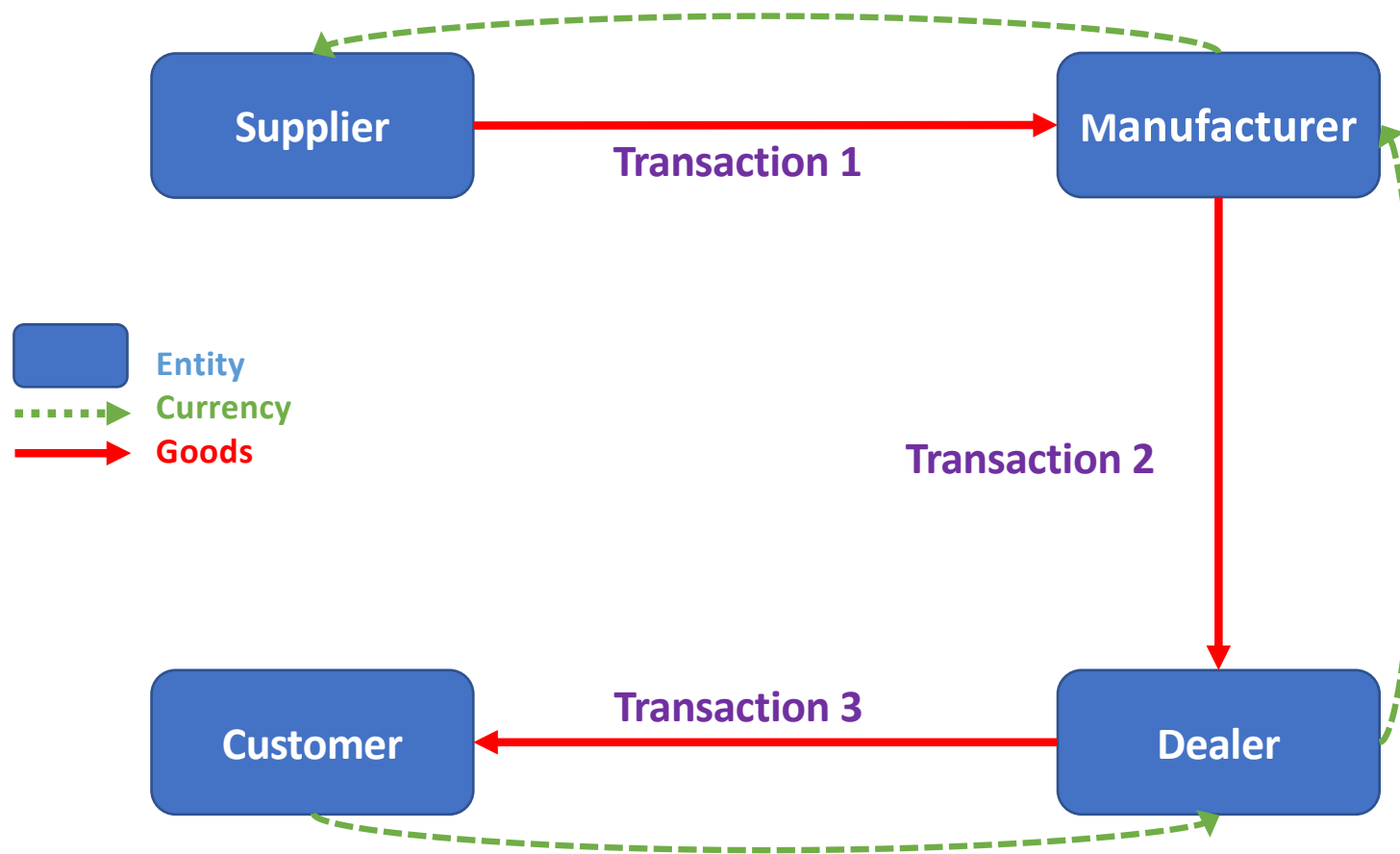
```
hex: 0ffc3f54352053828c4990ee683eebcc1d118a0d58b32da707d986d2  
HEX: 0FFCAF3F54352053828C4990EE683EEBCC1D118A0D58B32DA707D986D2  
h:e:x: 0f:fc:af:3f:54:35:20:53:82:8c:49:90:ee:68:3e:eb:cc:1d:11  
base64: D/yvP1Q1IFOCjEmQ7mg+68wdEYoNwLMTpwfZhtJFm74=
```



Transaction 3

Dealer sells inventory to Customer

Distributed Ledger Transaction Diagram



Blockchain –Transaction 3

- Transaction 3:
 - Previous block hash: 0ffc
 - Transaction ID: tx03
 - Description: “dealer sells final product to customer for 20BTC”

Value to Hash:

0ffc-tx03-dealer sells final product to customer for 20BTC:xxxx

Text you want to convert to a SHA-256 hash:

0ffc-tx03-dealer sells final product to customer for 20BTC:0000

Your hash has been successfully generated.

```
hex: c2dfd2ace66e055099330ade16e89596ad987164b7861a86e6fa97278c!  
HEX: C2DFD2ACE66E055099330ADE16E89596AD987164B7861A86E6FA97278C!  
h:e:x: c2:df:d2:ac:e6:6e:05:50:99:33:0a:de:16:e8:95:96:ad:98:71  
base64: wt/Sr0ZuBVCZMwreFuiVlq2YcWS3hhqG5vqXJ4yWX58=
```


Blockchain – Post Transaction 3

Text you want to convert to a SHA-256 hash:

```
0ffc-tx03-dealer sells final product to customer for 20BTC:0010
```

Your hash has been successfully generated.

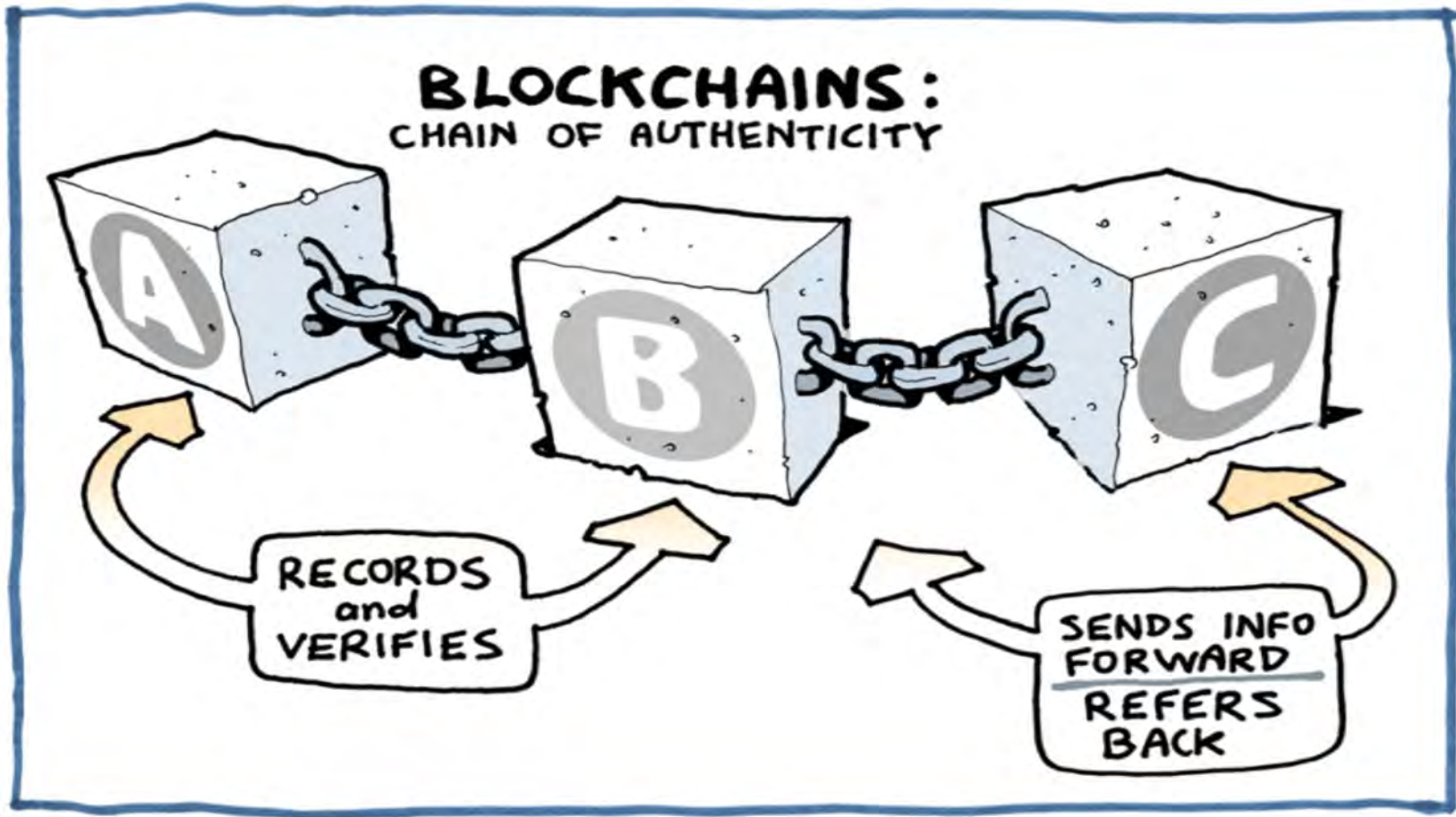
```
hex: 0f8e94c0cc1f9e208da7f5f1efc1ebd6d12c20d3e78b288868294df3f3.  
HEX: 0F8E94C0CC1F9E208DA7F5F1EFC1EBD6D12C20D3E78B288868294DF3F3.  
h:e:x: 0f:8e:94:c0:cc:1f:9e:20:8d:a7:f5:f1:ef:c1:eb:d6:d1:2c:20  
base64: D46UwMwfniCNp/Xx78Hr1tEsINPniyiIaClN8/M4wfI=
```

Let's watch another video...

Future Bank Today | Episode 5: Blockchain - The Great Disruptor (8:16)

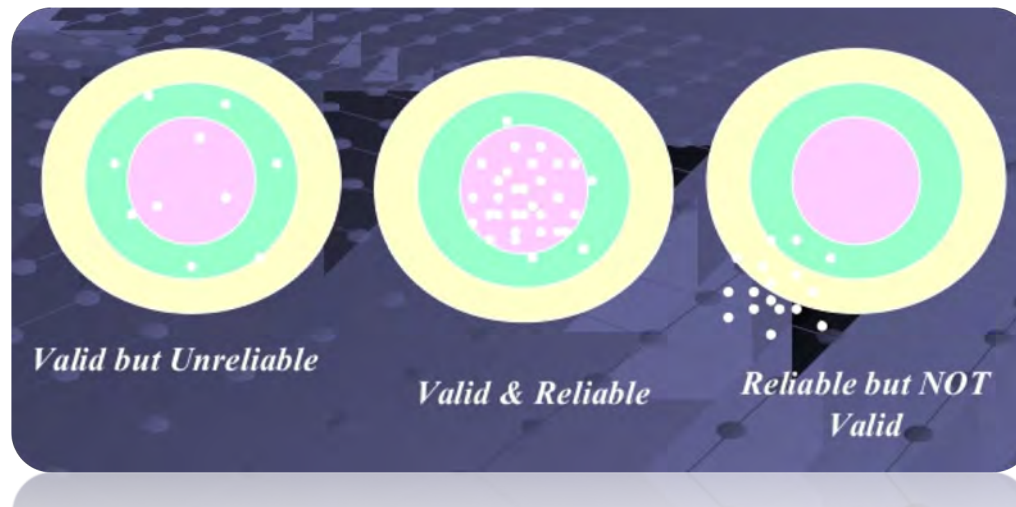
- <https://www.youtube.com/watch?v=EHTgqHy-jLk>

Blockchains and Auditing



Define the Objectives of the engagement

- Reliable and valid evidence is that which can be trusted, verified, and “seen” by the auditor
- Data sources external to the client are considered to be more reliable
- Are these two ideas the same for private or semi-private blockchains?



Transaction Transparency

- Data generation process should be transparent, observable, reliable
- Blockchain for transactions provides a record of the series of blocks (events) and maintains their immutability because of the hashing algorithm



The Design and Development of Audit Procedures in the Audit of Blockchain

- Standards on evidence collection:
 - “all the information used by the auditor in arriving at the conclusions on which the audit opinion is based.” (SAS No. 106, AICPA 2006; AS No. 15, PCAOB 2010)
 - “The reliability of audit evidence is influenced by its source and by its nature and is dependent on the individual circumstances under which it was obtained.” (SAS No. 106.08, AICPA 2006)
 - Generally, audit evidence is more reliable if it is obtained from sources external to the entity, if it is in documentary form, or if obtained directly from the auditor.” (SAS No. 106.20, AICPA 2006)
 - Continuous evidence gathering

Traditional evidence collection versus hypothetical DLT enabled continuous method

Procedure	“Traditional” Method	Blockchain enabled Continuous Method
Inspection of Records or Documents	Pull samples of records and trace/verify/match	Evaluate entire datasets in ERP using blockchain
Inspection of Tangible Assets	Physical inventory, walk through, open boxes	RFID tagging , back end software records sensor reading with BC format in a real-time basis (minimal lag)
Observation	Stand/sit with worker(s) and observe	Use blockchains or process mining to verify work flows
Inquiry	Written or oral interviews	Monitor processes and controls, identify process violators for examination
Confirmation	Verify account balances	Link data streams using blockchain applications
Recalculation	Extract and recalculate figures to verify	Monitor all data and run BC calculations automatically at intervals desired
Re-performance	Re-perform procedures to verify	Automatically replicate all transactions and identify exceptions using BC
Analytical Procedures	Scanning and statistics	Filter real-time data with continuity equations and statistics

Discussion of BC Accounting and Auditing: Observation/Inquiry

- Supports the assertions of existence, occurrence, and valuation
- Blockchain provides proof of observation/scanning for many instances
 - Auditors can observe time-stamping of transactions that are added to a chain and its hash
 - They can also observe if the length of the hashes are increasing over time
- Inquiry can be used to obtain evidence from the peer network as to their understanding of the governance characteristics of network and blockchain

Discussion of BC Accounting and Auditing: Confirmation

- Existence of transactions with third party/external validation already exist with the blockchain methodology
 - Real time, immediate conformations provided by banks, clients, attorneys, regulators, and suppliers, to name a few
- Specifically, a conformation relating to the BC process components would be to confirm with members of the peer network as to the design and function of the hashing algorithm

Discussion of BC Accounting and Auditing: Inspection of Records, Documents, and Tangible Assets

- Auditors or audit software can easily scan or inspect the documents that support the configuration or governance structure of the Blockchain process
- Auditors or audit software can scan the chains for outliers/abnormalities
- Tangible assets: drone recording directly to blockchains

Recalculation and Re-performance

- If the hash in a DLT is verifiable, then the peers of the network and the auditor can verify the blocks stored in the chain.
- Provides accurate recording of process streams for IC audit
- Supports the accuracy assertion

Analytical Procedures

- Depend on reliable and accurate data for effectiveness
- Foreseeably could permit a greater reliability on many Analytical Procedures in the audit and less reliability on manual detailed examination



Audit Plan

- Develop plan, control objectives and review steps
- Interview IT management to understand client's position on cloud and Blockchain
- Select relevant Blockchain cloud applications for sampling

Fieldwork

- Gather Blockchain evidence in relation to audit objectives
- Interview stakeholders
- Perform Tests of Design and Operational Effectiveness against Audit Review steps

Results

- Document any gaps with Blockchain and cloud controls objectives and risks
- Provide suggestions to address any issues identified in the audit of Blockchain in the Cloud

Summary

- **Now what is “blockchain technology” you might ask? Ironically, there is no consensus on the definition:**
- Minimalists will argue it is only Bitcoin
- Some people think it should include any DL with chained blocks
- Some experts think it should include any DL with some key features: chained blocks, immutability & consensus protocol
- Maximalists say “blockchain technology” equals “distributed ledger technology” equals “cryptographically enabled DDBMS”. Also it is easier to use the term “blockchain” for marketing & communication purposes, even if it can be misleading...
- The final equation is: bitcoin blockchain \subseteq blockchain technology \subseteq distributed ledger technology \subseteq distributed databases.

Source: <https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118>

“No-Coiners”



Kiran Vaidya @kiranvaidya · Feb 5

Also attacking academicians like @el33th4xor is the exact problem in current cryptocurrency space. Any culture that attacks researchers has a BIG problem. It actually reminds me of similar thing happening in #Germany in 30s and #China in 60s. We all know how that ended, eh!

nocoiner

A **Nocoiner** is a person who has no Bitcoin. Nocoiners (**usually** Socialists, Lawyers or MBA Economists) are **people** who missed their opportunity to buy Bitcoin at a low price because they thought it was a scam, and who is now bitter at having missed out. The **nocoiner** takes out his or her bitterness on Bitcoin Hodlers, by constantly claiming that Bitcoin **will crash**, is a scam, is a bubble, or other types of easily refuted FUD. Nocoiners have **little** to no computer skills or imagination; even when they see the price of Bitcoin go up and its adoption spread they consider all Bitcoin users to be in a collective delusion, with only themselves as the ones who can see what is happening. This attitude comes from being steeped in the **elitist** priest cultures found at Harvard, Yale and Columbia, where anyone who is not part of their **clique** is treated with suspicion by default. The worst nocoiners are tenured academics and goldbugs. Nocoiners believe that the world owes them everything they want because they are part of an elite; they are hysterical liars, brats, prostitutes and losers.

*I'm pretty sure Emin is a **Nocoiner**. Yesterday he made a Tweet about how Bitcoin going up was **just** a fad, and that a crash was inevitable. He's always **talking** Bitcoin down; if he had Bitcoin, he would never trash his own stash.*

1 2 3

Show this thread



Bloomberg

STREET SMART

BILL GATES
BILL & MELINDA GATES FOUNDATION CO-CHAIR

Assignment for ACC - AIS

- Each group submit in Canvas by X/XX/XXXX the group's responses to the Bitcoin and Blockchain exercise assignments (excluding the essay/presentation Part 5/step 5). On X/XX, each group will submit a short memo discussing their assigned topic and group presentations will occur on X/XX.
- (Word document available upon request – appelbaumd@Montclair.edu)

BITCOIN & BLOCKCHAIN

FURY!

- DRUG-DEALERS WILL USE IT!
- SHITCOIN!
- PONZI SCHEME!
- SCAM!
- A WAY TO SPECULATE!

AT FIRST...



- HOPE? -

- TRUST ENABLING SYSTEM
- CO-OPERATION AT SCALE
- BUT ARE WE FETISHISING DECENTRALIZATION?
- NAIVE TO PUT EVERYTHING IN THE CHAIN
- RIGHT, LEFT, BANKS, ACTIVISTS → EVERYONE IS INTERESTED
- RESTORE TRANSPARENCY TO PUBLIC SYSTEMS
- NOW

#FUTUREFEST
CARTOON BY
@VOINONEN

Other “fun” blockchain applications

- **Factom Dloc:**

- Creates a seal that incorporates a special security chip that can hold contextual information, such as images and text, which can be stored as public data or as private data accessible to authorized parties only.
- One can choose from a range of different chip platforms with storage capacities between 1kB and 64kB. DLoc stickers support all the standard security features including UV print, microtext, or latent images. The document’s data is tagged to the unique ID of the NFC chip and is only recognizable via a private key. The document can then be managed in a client-customizable DLoc mobile app.
- DLoc has a seamless integration with the secure Factom blockchain. Once the sticker is applied, it can be verified using a desktop reader or a mobile app on an NFC-enabled phone.
- Scanning the documents reveals their true history and authenticity.
- DLoc provides secure document provenance, minimizing the time required to confirm documents and contracts. Freeing up time from information tracking and authentication, and from reviewing and analyzing paperwork, will allow CPAs to instead focus on higher-level tasks.

Other “fun” blockchain applications

- Trying this blockchain with a demo example can be completed as follows:
- Go to <https://freefactomizer.com/>.
- Upload an unimportant test document to be hashed.
- Obtain an estimate for how long the hashing will take by clicking “Factomize the File Signature.”
- Wait to receive your link, and then view your document on the Factom blockchain.

Agenda

- Introduction
- Technology and Accounting
- The Basics of Blockchain and Updates
- Real World Applications
- Blockchain Demonstrations for the Classroom
- How Blockchain Will Change the Profession

How Blockchain will change the profession

Areas of high impact:

- Reconciliations
- Expansion of accounting function
- Establishing a single source of date internally
- Reducing paperwork
- Continuous Auditing



Benefits of
Blockchain
for the
Accounting
Process

Process	Pre-Blockchain	Post-Blockchain
Reconciliation of accounts	Time-consuming process of obtaining both internal and external documentation and manually comparing two sets of data	Streamlined process—all information is on the blockchain and approved by the organization and counterparties in real time
Preparation of internal ad hoc reports	Majority of time spent verifying that information is correct and matches other sources within the organization	Less time spent verifying—transactional information is available to any member of the network and more time can be spent on advice and advisory activities.
Closing of books at month, quarter, and year end	Occupies a large amount of internal accounting time to 1) get the necessary information to close the books and 2) run reports to ensure entries and information are posted correctly	Possible to imagine scenarios where financial statements, fed from the blockchain, are updated every day, making periodic closes a routine and less painful process

Agenda

- Introduction
- Technology and Accounting
- The Basics of Blockchain and Updates
- Real World Applications
- Blockchain Demonstrations for the Classroom
- How Blockchain Will Change the Profession
- Moving Forward and Conclusion

Moving Forward and Conclusion

- What is blockchain's time horizon?
- When will CPA's encounter it in daily practice?
- Is widespread adoption still years away?
- What about a costs/benefits analysis?
- What factors might change the equation?

Please see: <https://www.cpajournal.com/2018/06/19/blockchain-basics-and-hands-on-guidance/>

An aerial night view of a city, likely New York City, with a network of white lines and glowing nodes overlaid on the image. The city lights are visible in the background, and the network lines connect various points across the scene.

Thanks!

For additional inquiries:

Deniz Appelbaum: appelbaumd@Montclair.edu

Sean Stein-Smith: Sean.Steinsmith@lehman.cuny.edu