

Introduction to Blockchains and Smart Contracts for the Internet of Things

Presented by

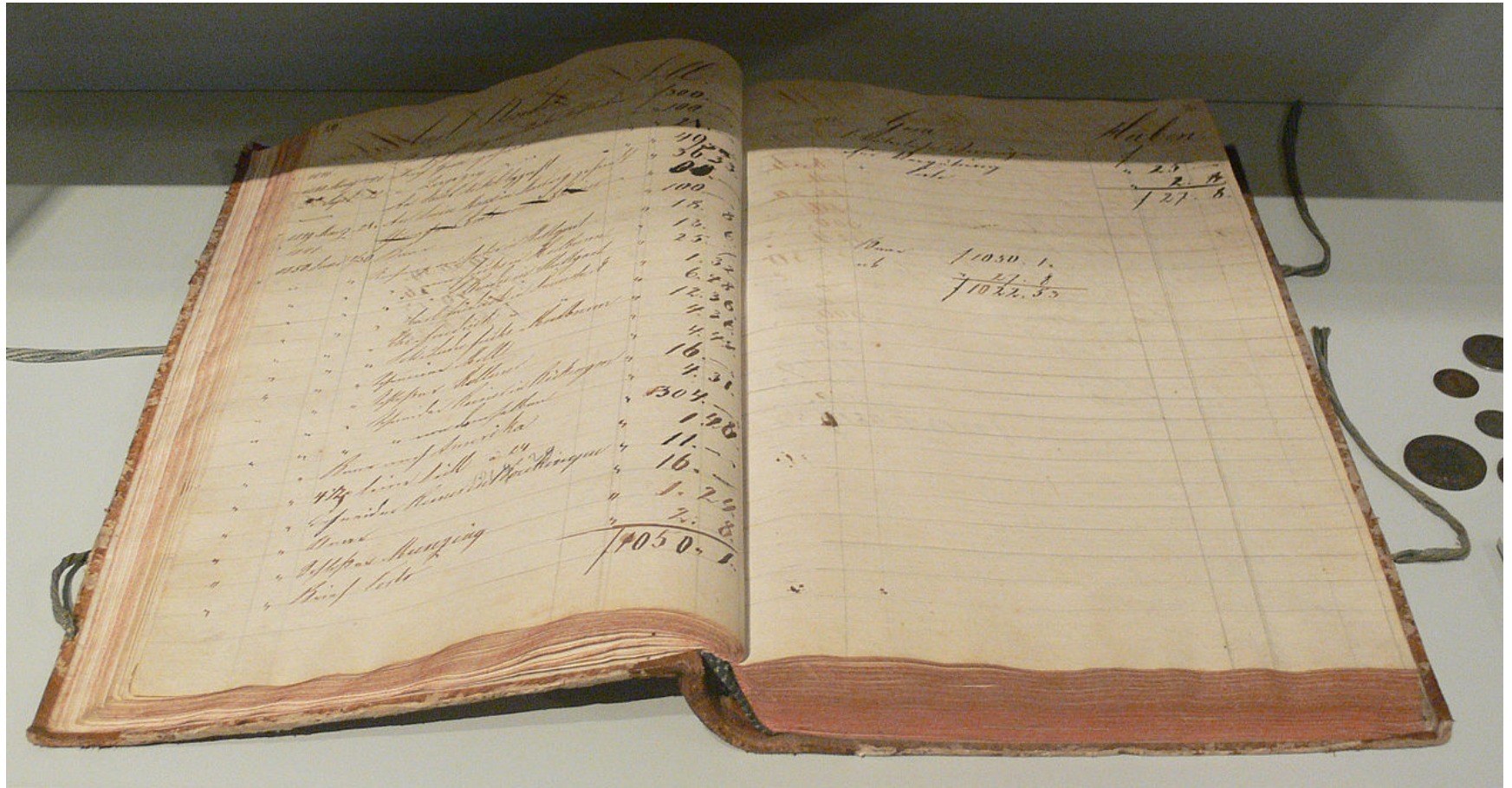
Mehmet Demir

mehmet.demir@ryerson.ca

Agenda

- Fundamentals.. Ledger, Distributed Ledger
- How science help .. Cryptography, keys, hash
- Blockchain.. Transaction, block, chain,
- Smart contracts
- What IoT needs?
- IoT Blockchain examples
- IoT Blockchain considerations

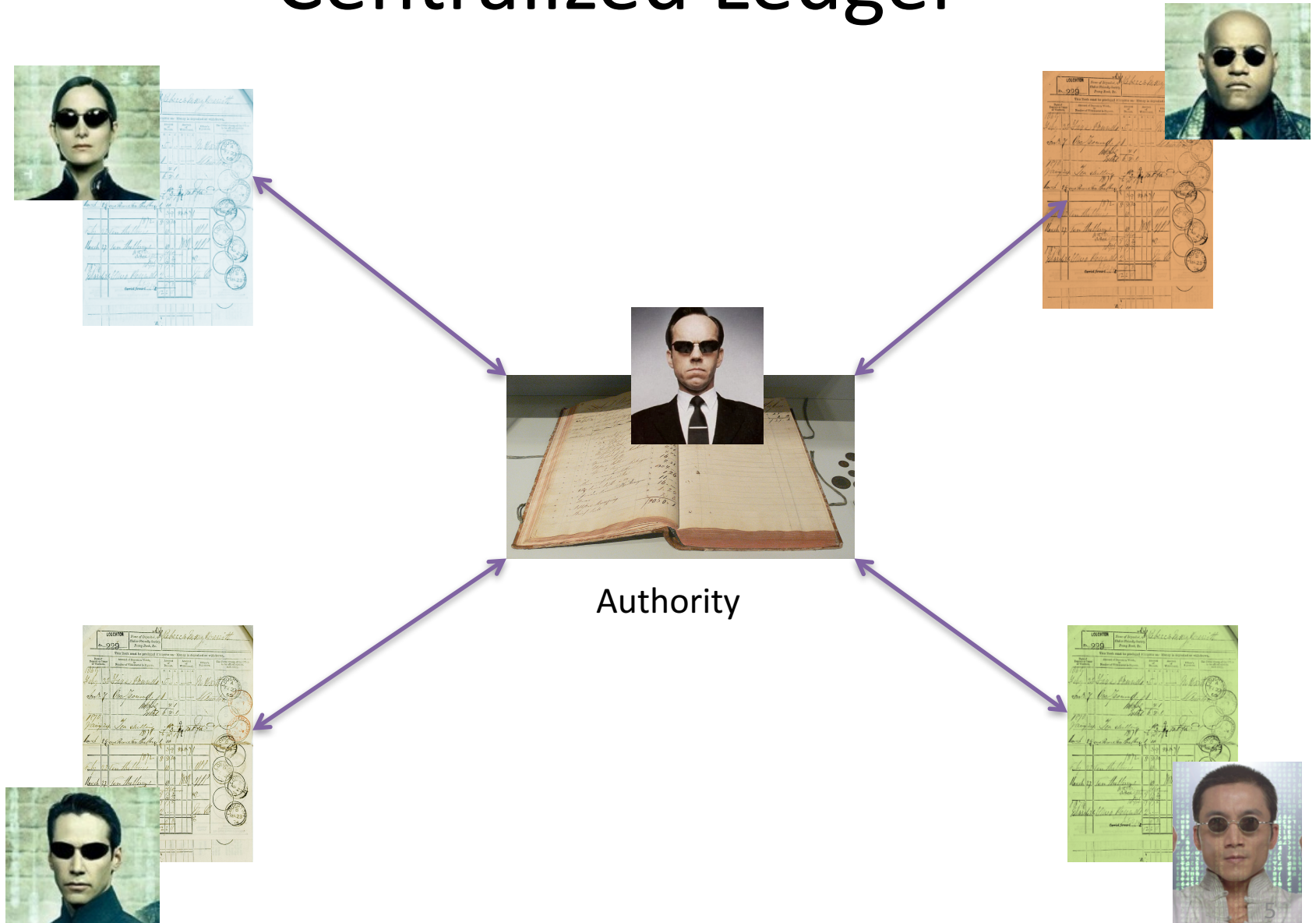
Ledger



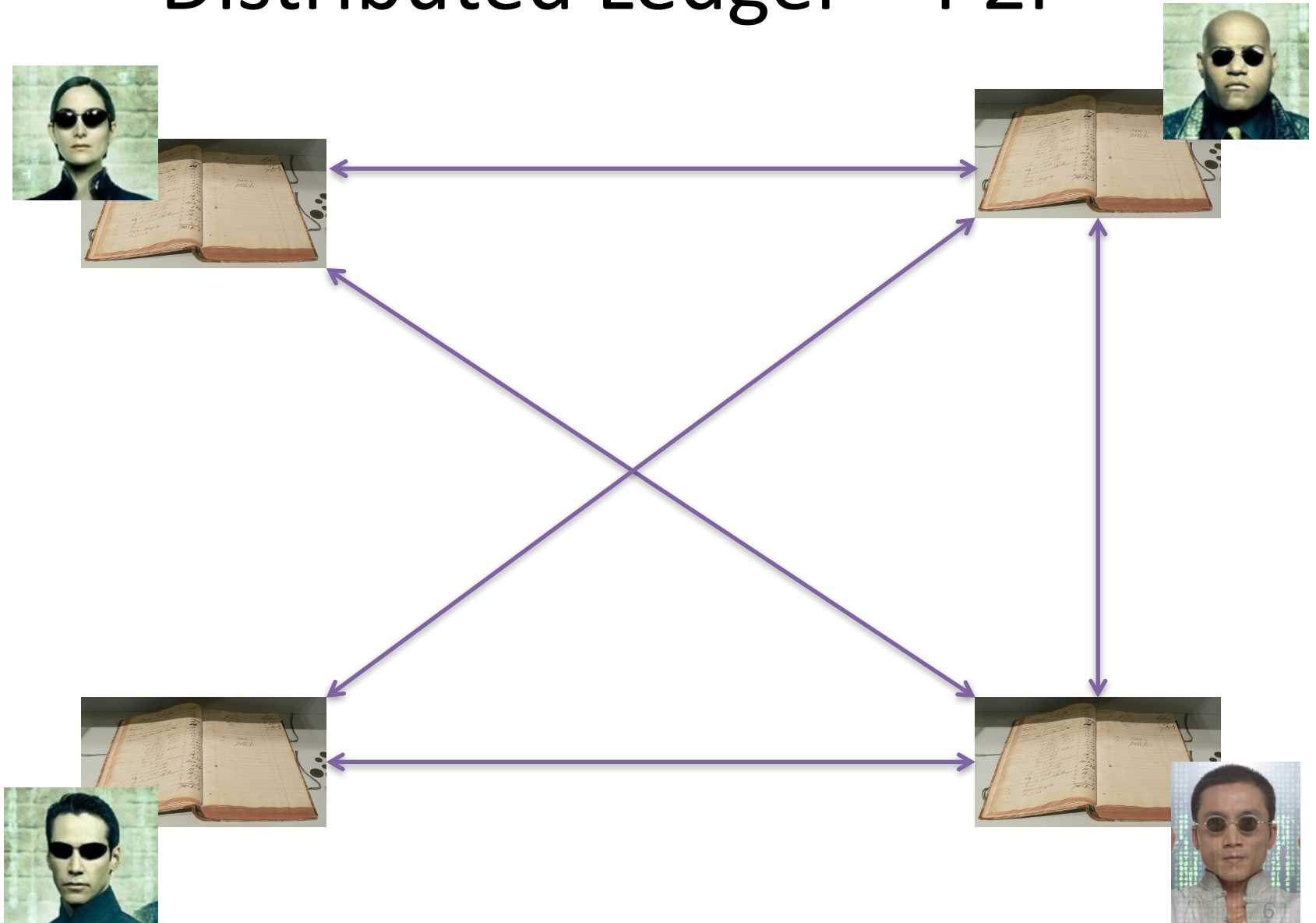
Distributed Ledger?

LOUGHTON		Name of Depositor, of Club or Friendly Society, Penny Bank, &c.	
No. 229		Ally Rebecca Mary Knewitt	
This Book must be produced whenever any Money is deposited or withdrawn.			
Date of Deposit or Issue of Voucher.	Amount of Deposit in Words, or Number of Withdrawal in Figures.	Amount of Deposit. £ s. d.	Amount of Withdrawal. £ s. d.
1869 Feb 23	Five Pounds	5	
Sept 7	One Pound	1	
	Wd	21	
	Wd	6 2 1	
1870 May 24	Ten shilling	10 4	
March 29	one Pound ten shilling	1 10	
		39 8 1 1	
1872 July 22	Ten shilling	10	
March 27	Ten shilling	10	
	Wd	4 4 1	
	Wd	9 13 2	
	Wd	8 1 1	
	Wd	9 1 5	
1874 March 26	Two Pounds	2	
	Wd	6 3	
	Wd	12 2 11	
Carried forward.....			

Centralized Ledger



Distributed Ledger – P2P

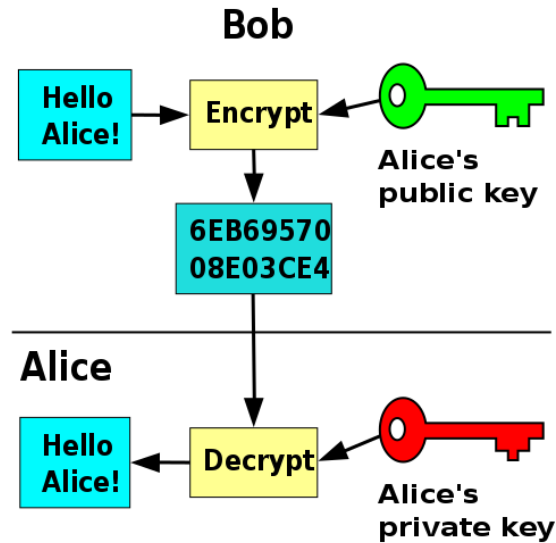


Trust

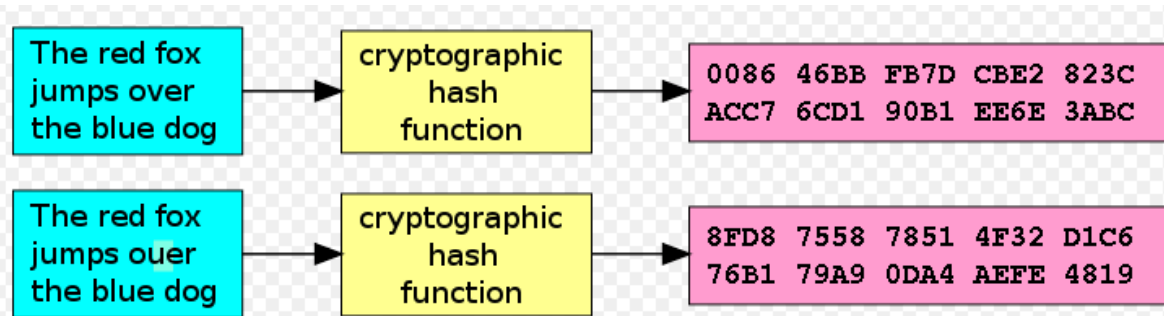


Cryptography

Public / Private keys

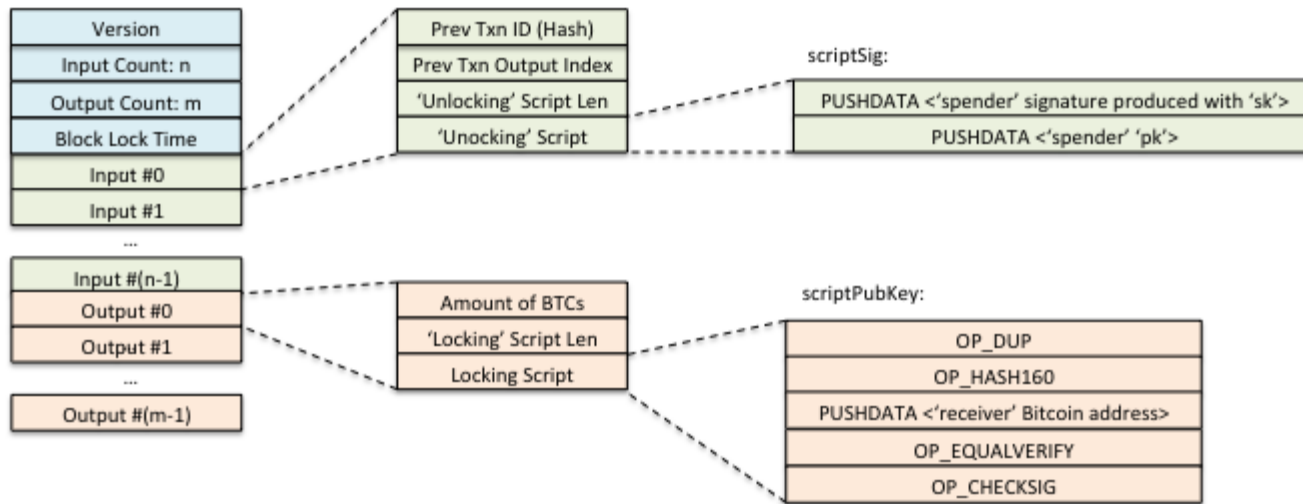


Hashing



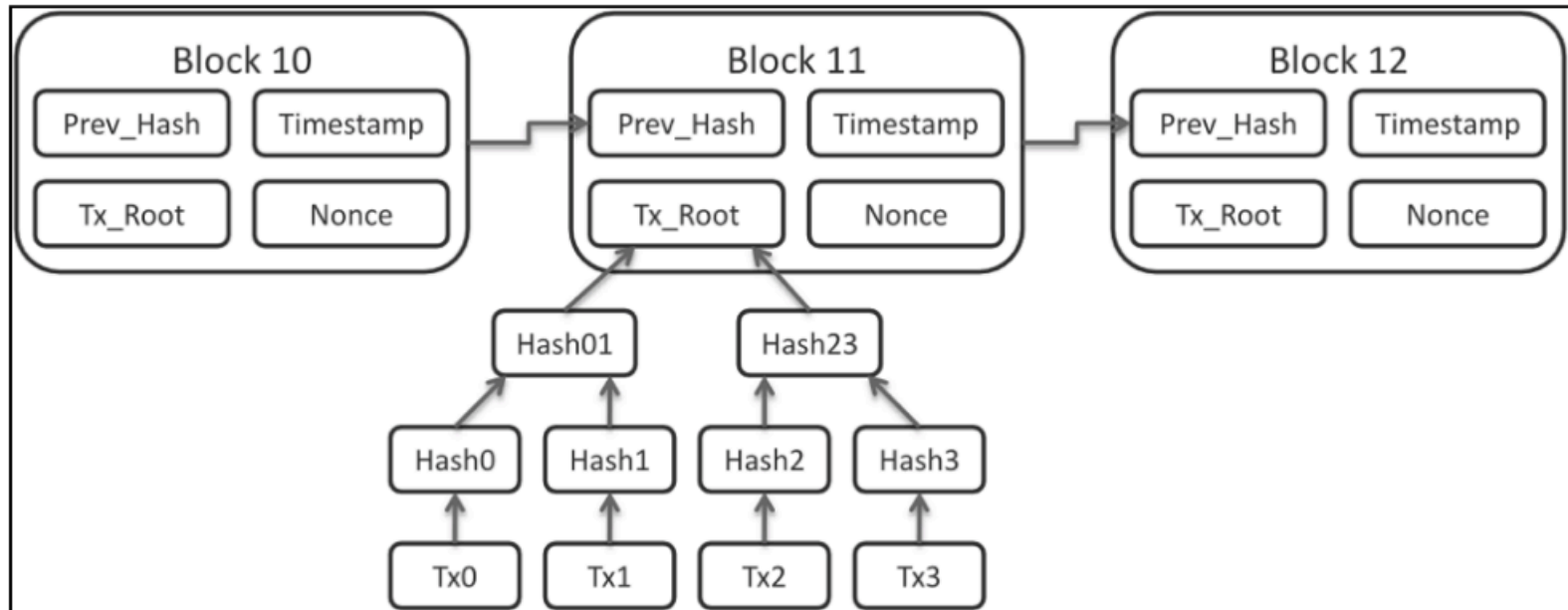
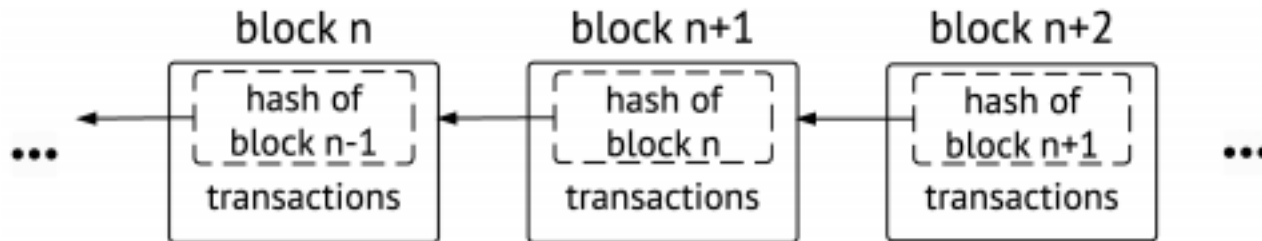
Transaction

Bitcoin Transaction Message



<https://letstalkpayments.com/blockchain-bitcoin-as-a-mainstream-case-study/>

BlockChain



Smart Contract

- Involves parties
- Computer Code
- Added to block chain
- Triggered by event(s)
- Execute transactions

*Get (\$5) from (Mehmet)
When Event (Pizza boy delivered)
Give (\$4) to PizzaX
Give (\$1) to PizzaBoy*

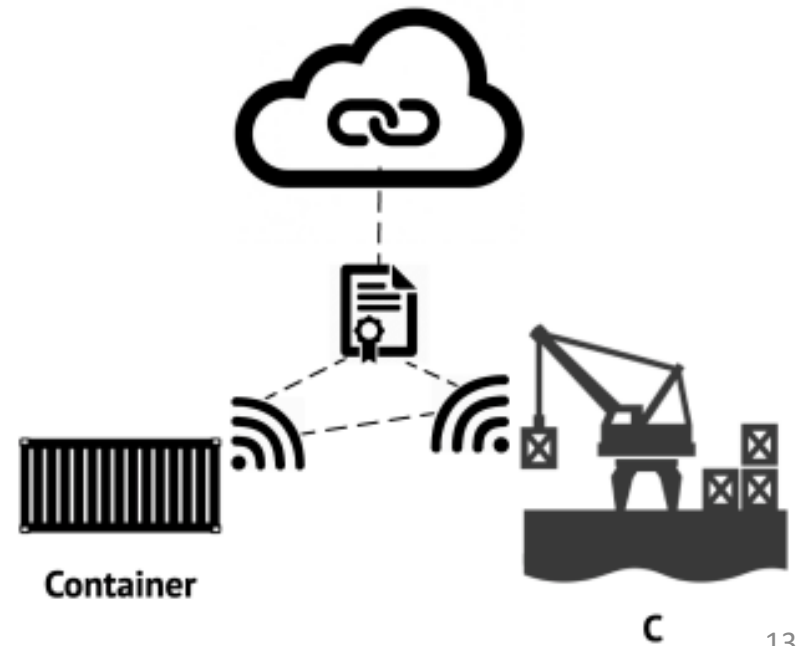
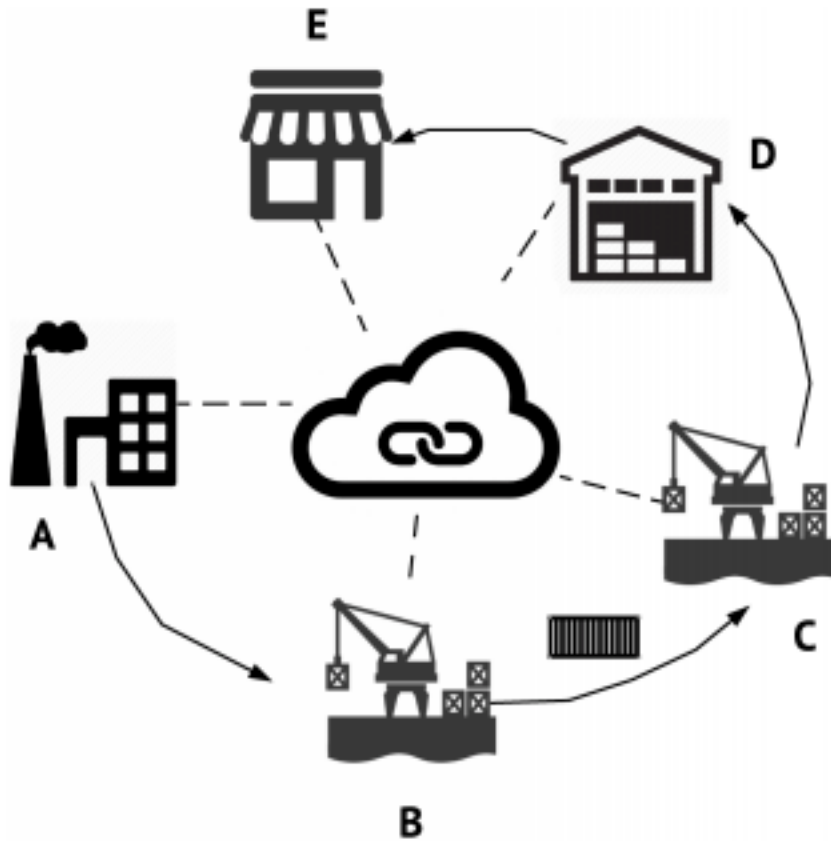
*If deliveryTime > requestTime + 30 min
Return (\$4) to Mehmet
Give (\$1) to PizzaBoy*

*If no delivery in 60 min
Return (\$5) to Mehmet*

IOT Examples

- Firmware upgrade
- Marketplace of services
- Smart Locks
- Supply Chain

Supply Chain



Considerations

- Transaction throughput – latencies
- Maintaining privacy – new key for every Tx
- Legal enforceability
- Complete autonomy
- Secure communication
- Private blockchains
- Ability of the IOT devices

Q&A

E-mail:

mehmet.demir@ryerson.ca

Please e-mail your comments and ideas

References

Beside several public resources I used, I got ideas and content from

KONSTANTINOS CHRISTIDIS, (Graduate Student Member, IEEE), AND MICHAEL DEVETSIKIOTIS, (Fellow, IEEE)
Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27606,
USA