IFIC

THE INVESTMENT FUNDS INSTITUTE OF CANADA

L'INSTITUT DES FONDS D'INVESTISSEMENT DU CANADA

BLOCKCHAIN

WHAT OPERATIONS NEEDS TO KNOW

WHO AM I?

INTERNATIONAL FINANCIAL DATA SERVICES

DST®

MASTER COMPLEXITY™

PAUL IVES

Research & Development
Looking at Blockchain since 2015

IFIC

RESEARCH & DEVELOPMENT

Advance Business Concepts Quickly

Constructing prototype, proof of concepts and running pilots

Cutting Edge New Technology

Artificial Intelligence, Machine Learning, Blockchain, Cloud, Touch Computing,Eye Tracking, VR/AR, Gesture Recognition, Quantum Computing

University Relationships

Talent Attraction, Rotating student work placements, multiple universities (UoT, UoW, MO S&T, NU, ZJU, UNL, UMKC, KU, UCM)

Thought Leadership

Conversation provoking prototypes, white papers and breakthrough new products

TODAY - BLOCKCHAIN - WHAT OPERATIONS NEEDS TO KNOW

1. What is a **Bitcoin**?

2. What is a **Blockchain**?

5. What does this mean to **Operations**?

3. **Consortiums**

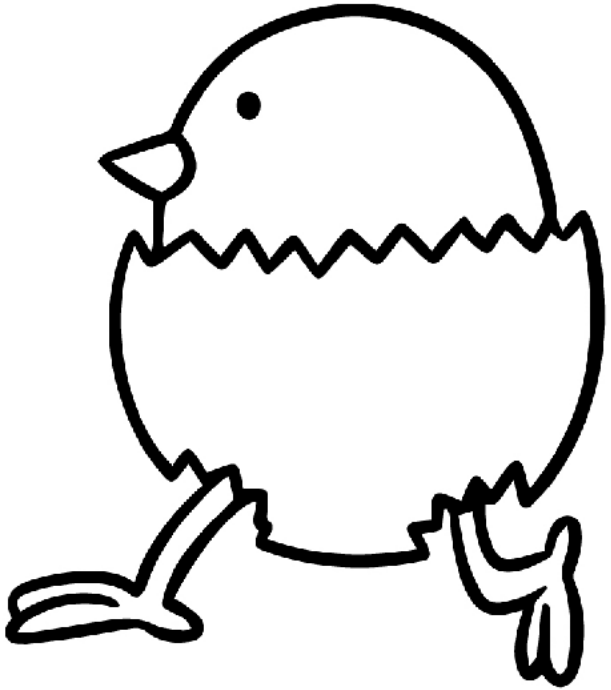
4. **Hype** vs Reality

CHICKEN AND EGG

*Understanding **Bitcoin** is understanding **Blockchain***

and

*Understanding **Blockchain** is understanding **Bitcoin***



WHAT IS A BITCOIN?

- approx. **$3 billion** in daily transactions
- **$70** billion market cap

WHAT IS A BITCOIN?

- Magic Internet Money
- A way a bunch of nerds got really, really rich

- Invented by Satoshi Nakamoto
  - **a pseudonym**

IFIC

WHAT IS A BITCOIN?

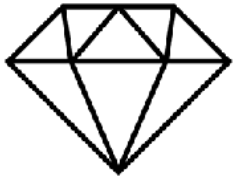
- **Digital Currency**
- Traded using a ledger called the **Blockchain**
- Allows participants to exchange currency **without a central authority**
- Nobody needs to **trusts** anyone else

IFIC

WHAT IS A BITCOIN?

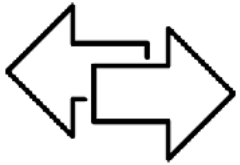
Invented to circumvent big banking after the financial crisis of 2008

WHERE DO BITCOINS COME FROM?



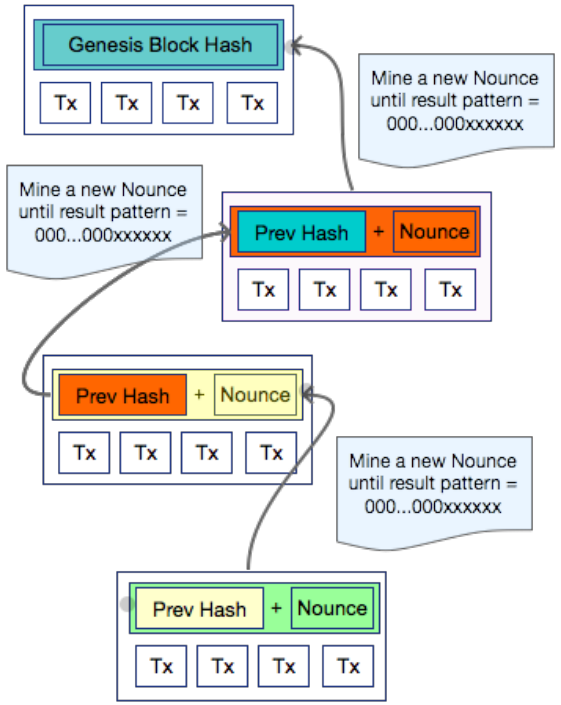
They are mathematically mined to keep a ledger called the **blockchain** in **consensus** across computers and large enough to record transaction history

Because Bitcoins are mathematically **hard to mine**, it gives them value

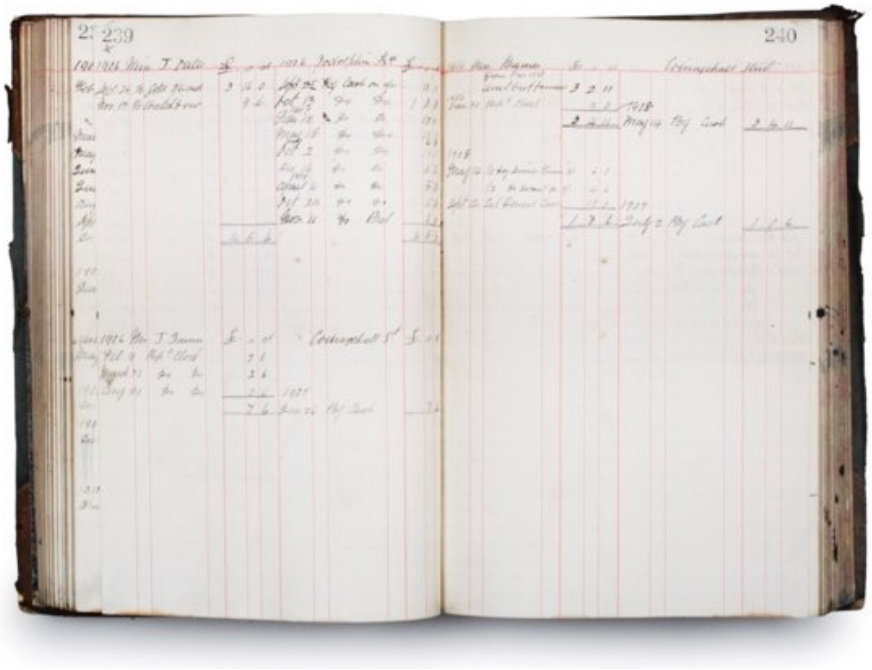


An **exchange** of **electricity** used to compute the **numbers** of a formula

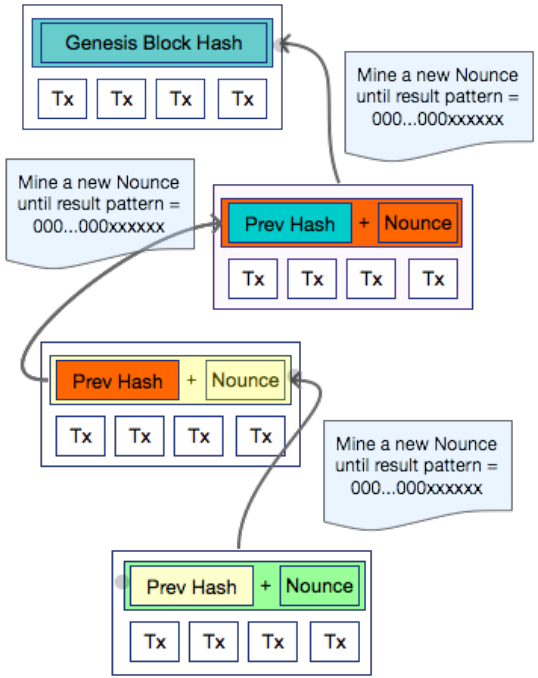
A CHAIN OF BLOCKS



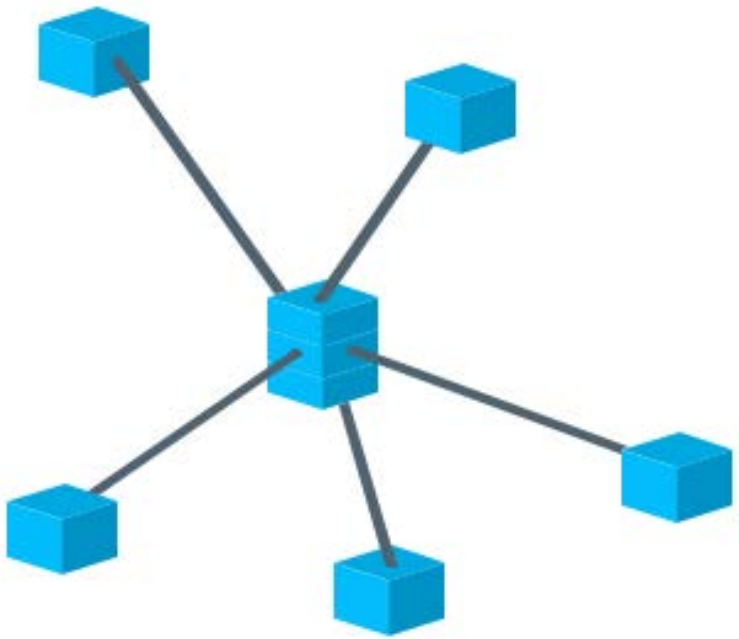
WHAT IS A BLOCKCHAIN



≈

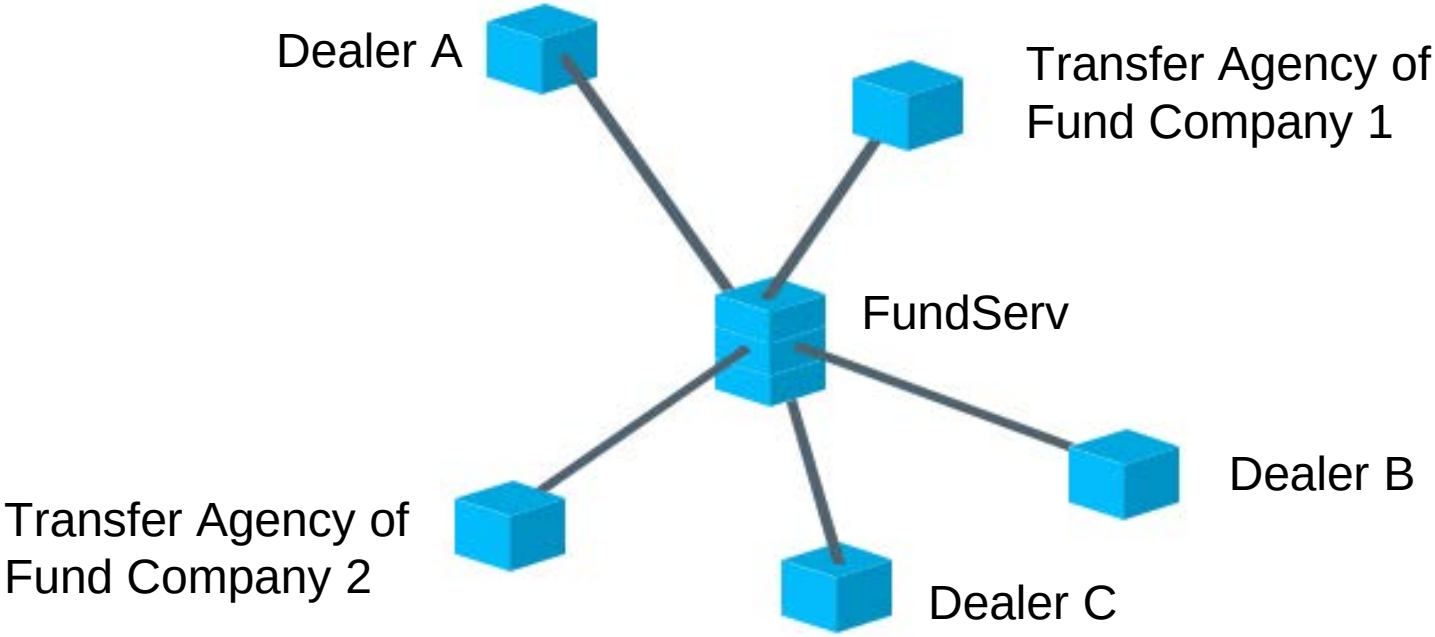


INTERMEDIARIES - WITHOUT BLOCKCHAIN



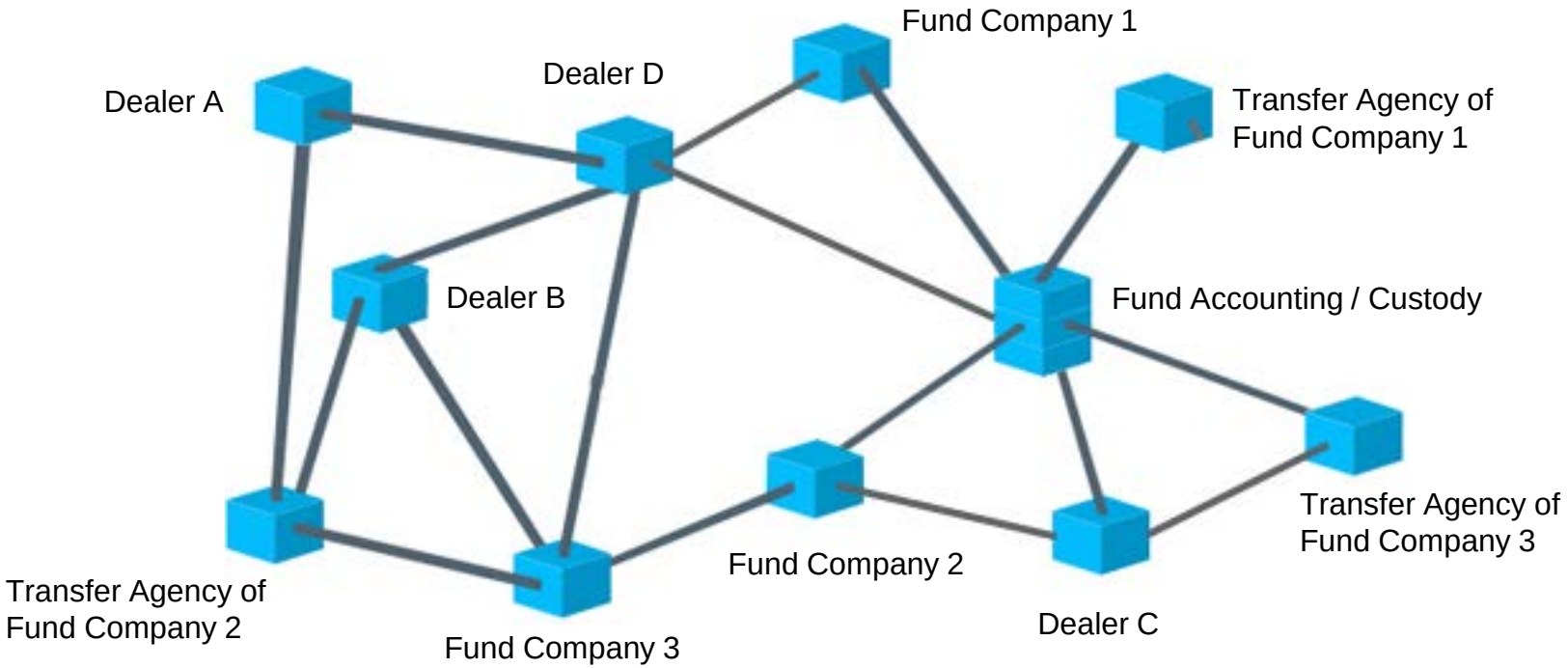
Centralized - Hub and Spoke - Point to Point

INTERMEDIARIES - HERE IN CANADA



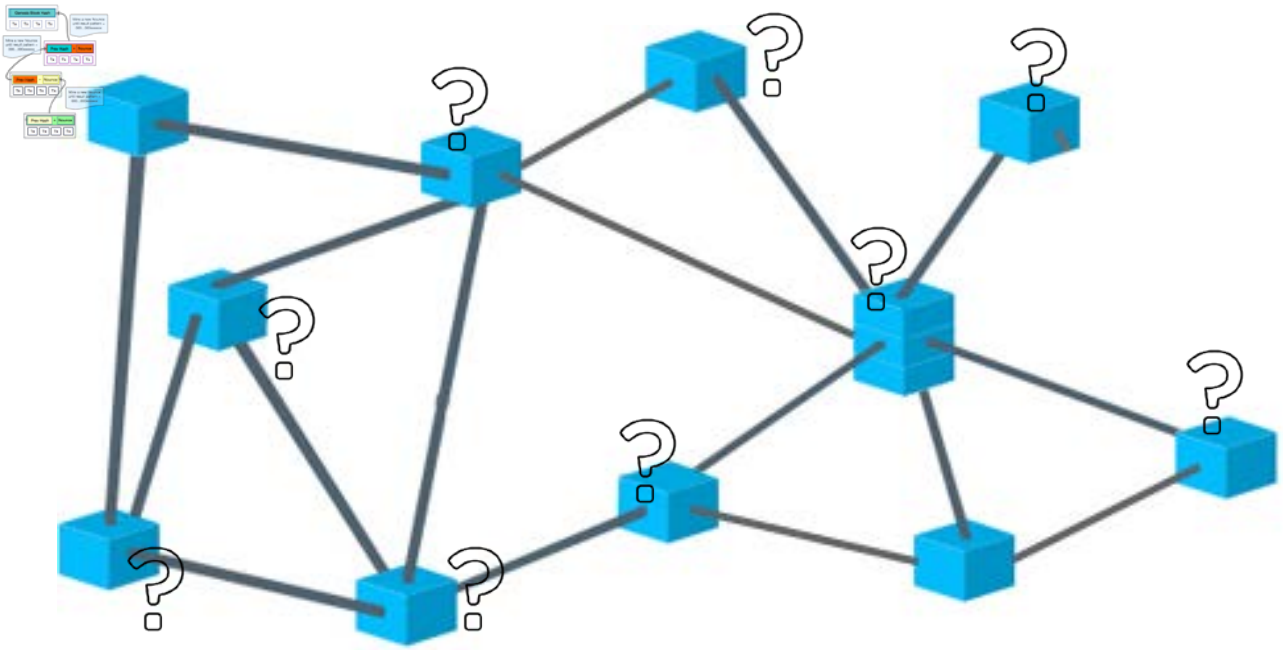
Centralized - Hub and Spoke - Point to Point

WITHOUT INTERMEDIARIES USING BLOCKCHAIN



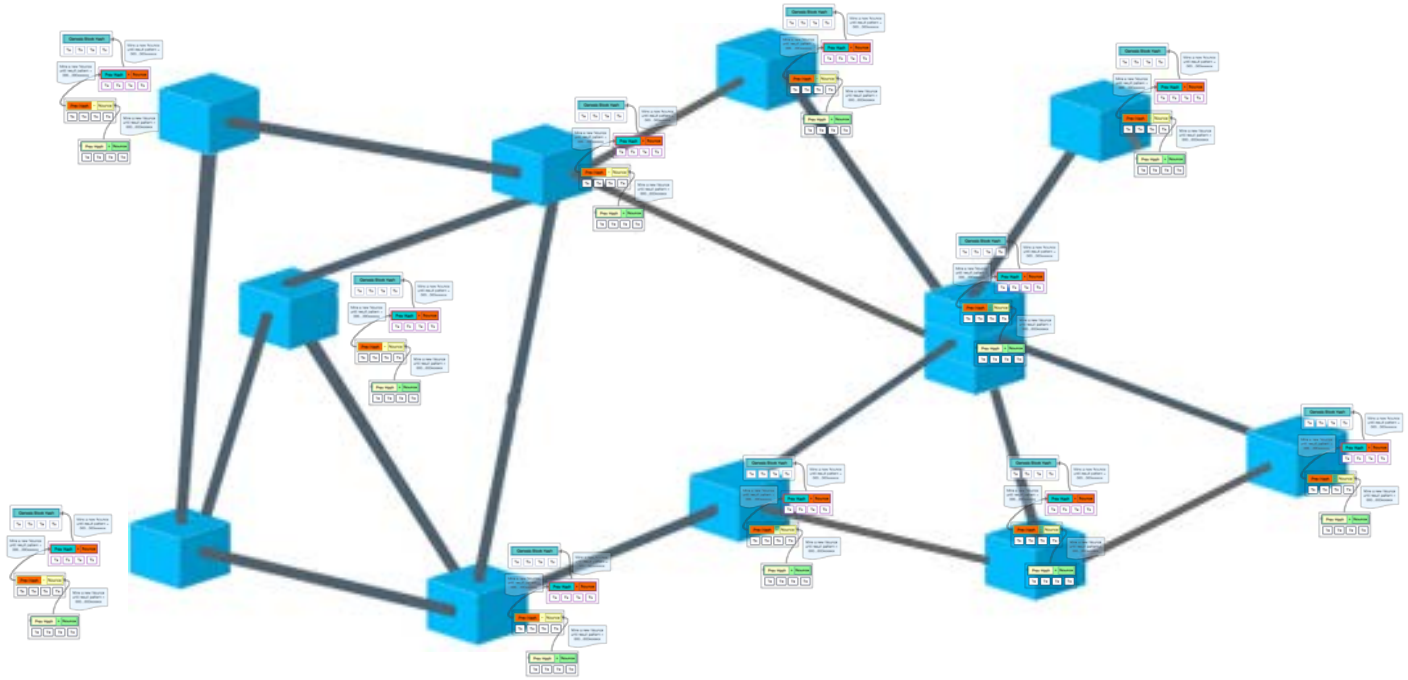
Distributed - Peer to Peer

HOW DOES EVERYBODY RECONCILE?



Distributed - Peer to Peer

CONSENSUS PROVIDES A SHARED LEDGER



Distributed - Peer to Peer

ZERO KNOWLEDGE PROOF

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

Sudoku is a good example of a zero knowledge proof,
hard to solve, but **quick to verify** the answer is correct.

IFIC

ZERO KNOWLEDGE PROOF

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

Solving a **Sudoku** is a lot **like** mining for a **Bitcoin**.

Proof of Work Algorithm

signature of
current data block
+
signature of last
block of data
+
n

where **n** = { 0… ∞ }

→

$$\int_0^{\infty} \sum_{n=0}^{\Omega} e^{n \sin^2 \theta} \, \partial x \, \cot \theta$$

→

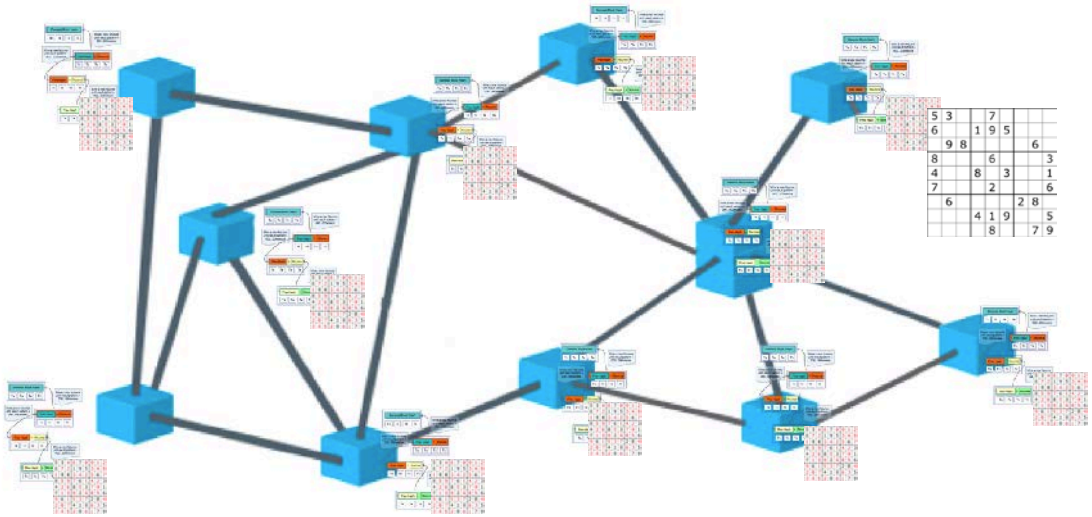
```
a591a6d4
0bf420404
a011733cfb
7b190d62c65
bf0bcda32b
57b277d9a
d9f146e8
```

answer must start with
***m** number of zeros (0)*

Sudoku is a good example of a zero knowledge proof,
hard to solve, but **quick to verify** the answer is correct.

IFIC

TAMPERPROOF



Distributed - Peer to Peer

Append only, tamperproof and has mathematically trust

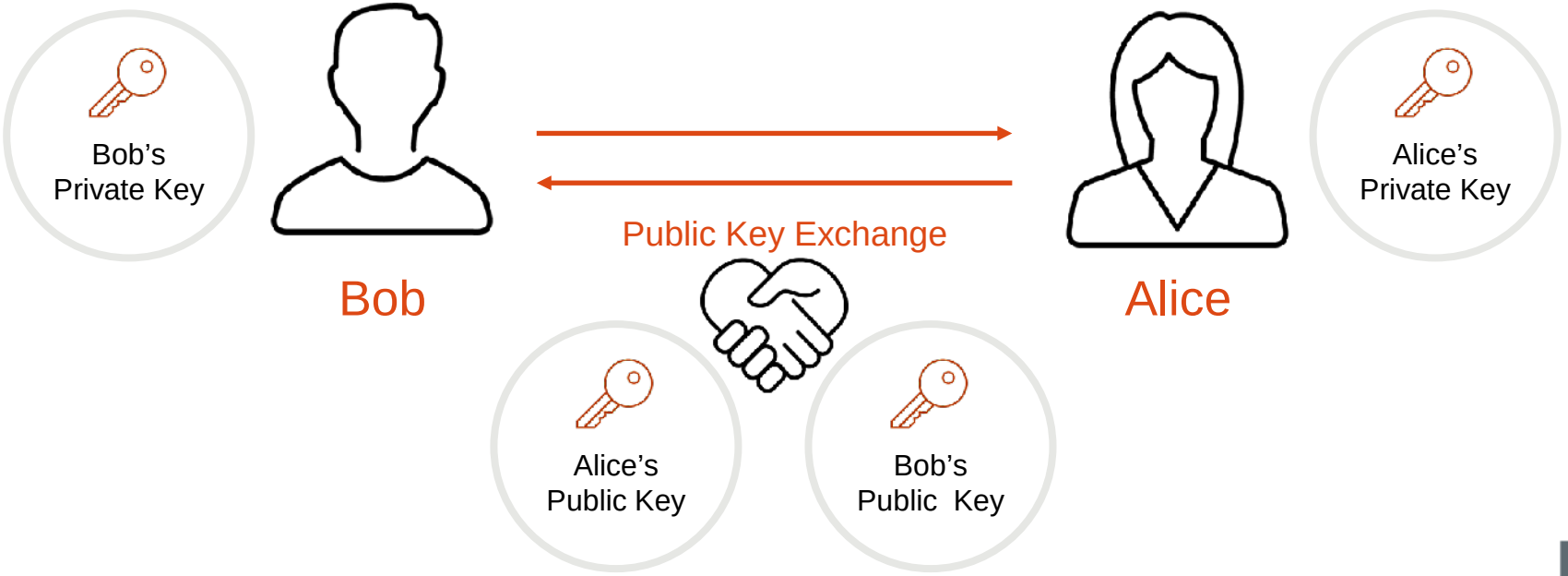
Everybody can trust that the data is from who it says it is from and that nobody is changing the data that has already been written, and nobody is in charge

Instant Settlement*

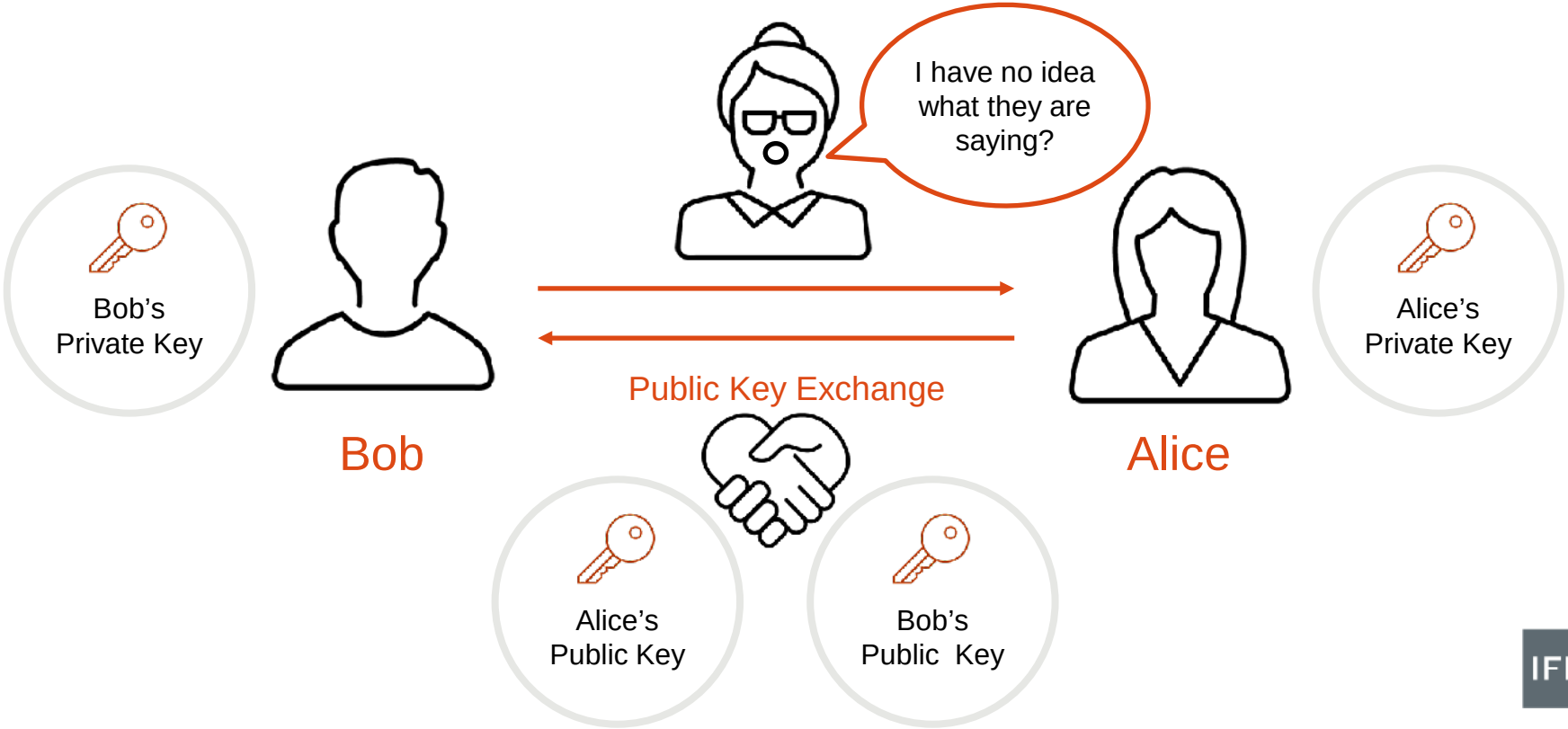
Once ownership information is written to the ledger, and the bitcoin(s) are assigned, the money has moved

** Not the real underlying fiat-currencies (e.g. CAD)*

ENCRYPTION


Bob's
Private Key
Bob
Public Key Exchange
Alice
Alice's
Private Key
Alice's
Public Key
Bob's
Public Key

ENCRYPTION


I have no idea what they are saying?
Bob's Private Key
Alice's Private Key
Public Key Exchange
Bob
Alice
Alice's Public Key
Bob's Public Key

SMART CONTRACTS

```
func getFundInfoAsJson(stub shim.ChaincodeStubInterface, fdParams *fundinfo.QueryFundInfoParams) strin
        uniqueKey := MakeFundInfoKey(fdParams)
        bytes := GetState(stub, uniqueKey)
        return string(bytes)
}

func GetFundCurrency(stub shim.ChaincodeStubInterface, pt PTradeJSON) (string, error) {
        var idf FundInfoJSON;
        if len(pt.FundCurrency) == 0 {
                idfKey := MakeFundInfoKey(&pt)
                bytes := GetState(stub, idfKey)

                if (bytes != nil){
                        JsonUnmarshal([]byte(bytes), &idf)
                        return idf.FundLevelDefaultCurrency, nil

                } else {
                        fmt.Printf("could not find the idf: %s\n", idfKey)
                        return "", errors.New("could not find fund info for " + idfKey)
                }
        } else {
                return pt.FundCurrency, nil
        }
}
```

ethereum

https://ethereum.org/

HYPERLEDGER

https://www.hyperledger.org/

Not just shared data, but **shared business logic code**! - **NO CENTRAL HUB**

IFIC

BLOCKCHAIN SUMMARY - THE FOUR PILLARS

1. Shared Ledger

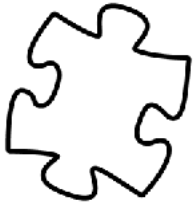
Append-only system of record shared across business network

2. Consensus

All parties agree to network-verified transaction

3. Encryption

Helps secure, authenticated and verifiable transactions



4. Smart Contracts

Business terms embedded in transaction database and executed with transactions

- A blockchain is the **shared ledger** where **Bitcoin transaction** are stored
- It is a piece of **computer software**
- **Lots of computers** each keep a copy of the **encrypted data**

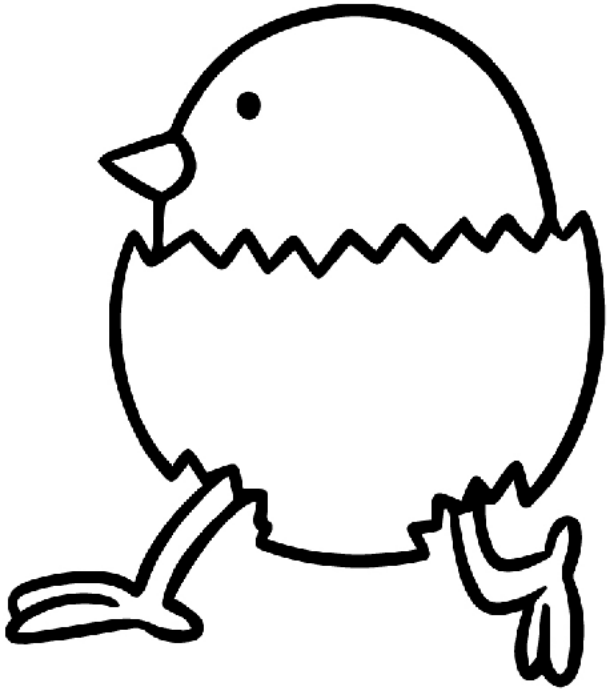
IFIC

CHICKEN AND EGG

*Understanding **Bitcoin** is understanding **Blockchain***

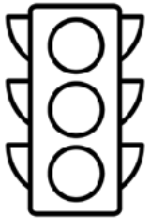
and

*Understanding **Blockchain** is understanding **Bitcoin***



IFIC

FINANCIAL SERVICES IS COMPLEX

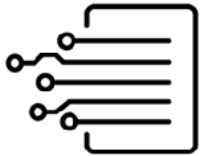


Post Trade Processing

Settlement and Clearing delays a liability (e.g. Client Asset Holding)

Reconciliation Headaches

Multiple copies of the ledgers (e.g. subaccounting and aggregated trading)



Cyber Security

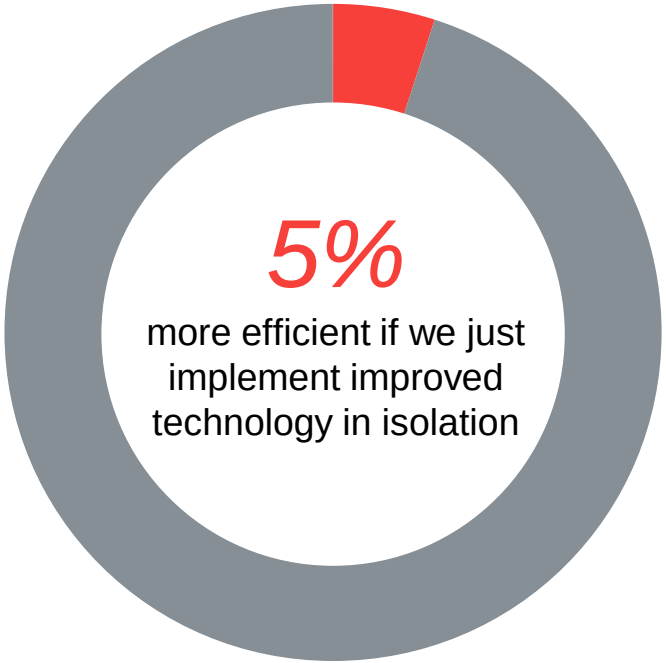
Bolted on, not designed within and very expensive

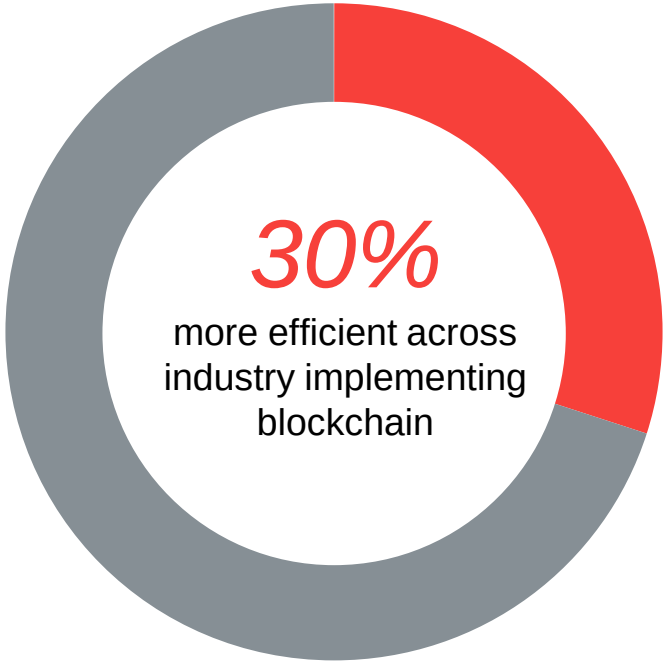
Regulation & Compliance

Bolted on, not designed within and very expensive, layers of legal complex, regulation .g. AML/KYC, auditing

IFIC

BETTER TOGETHER





* Predictions :-)

CONSORTIUMS

ENTERPRISE
ETHEREUM
ALLIANCE

HYPERLEDGER

Digital Asset
Holdings

IFIC

WHAT ARE PEOPLE DOING?

General

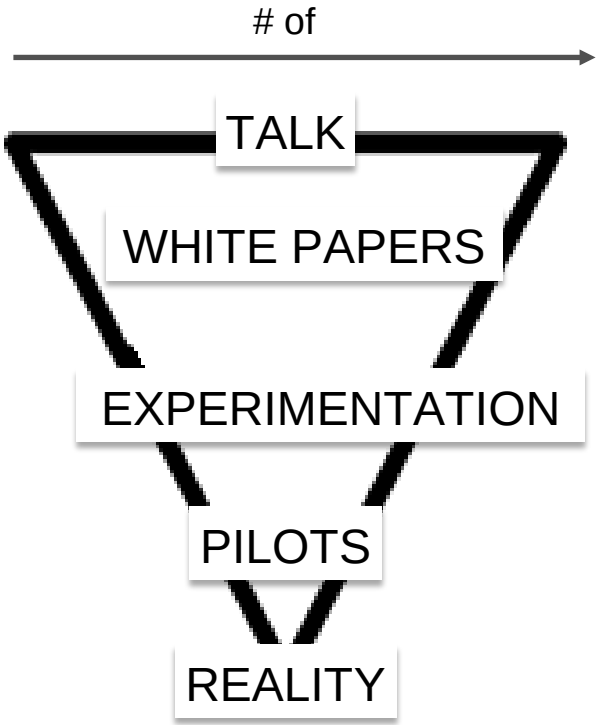
- Bitcoin, Ether, Litecoin
- Ownership
- Notary
- Authoring Rights
- Shipping and Logistics
- ICOs (Initial Coin Offerings) Venture Capital

Financial Services

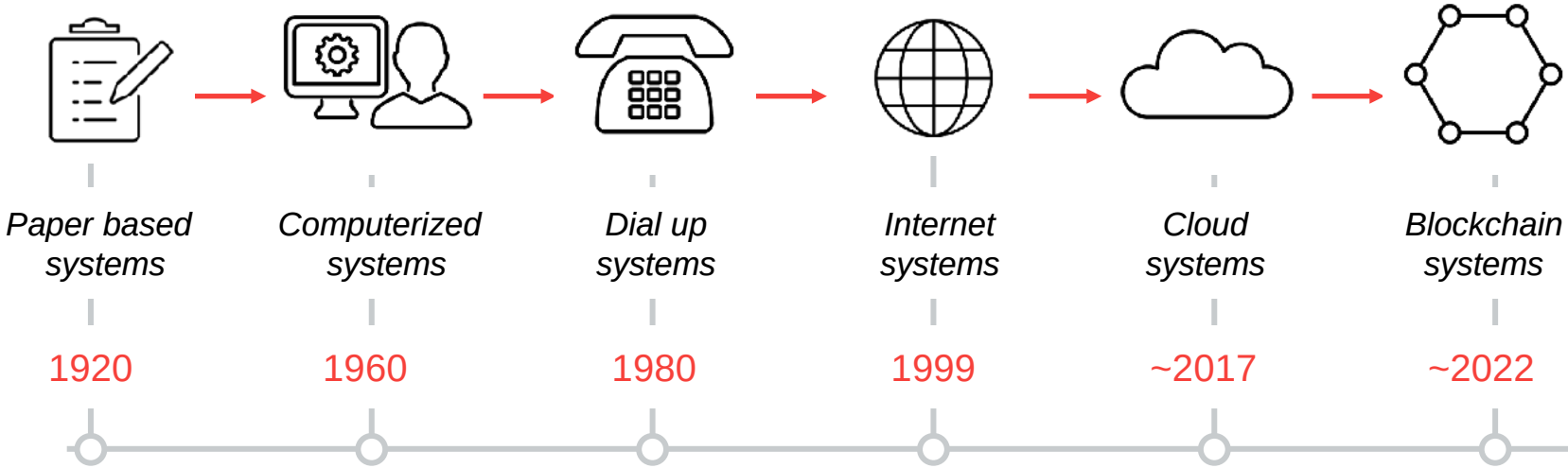
- Interbank Clearing & Settlement
- Payments
- Smart TA
- TA & Custody
- AML/KYC
- Messaging & Workflow
- Blockchain Consulting

HYPE IN FINANCIAL SERVICES

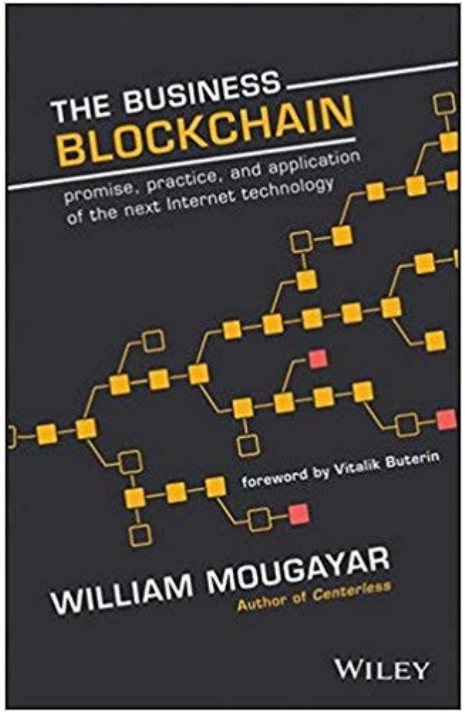
- A **boat load** of innovation **talk** and **slides**
- Loads of people having **similar ideas** - not fully thought out
- Some **white papers** { DTCC, Calastone, KPMG, PWC, Deloitte etc. }
- Lots of **experimentation** prototype code
- A handful of internal **production parallel pilots**
- A couple **limited real uses**, e.g. Private Equity
- **Nothing real** involving multiple Enterprises

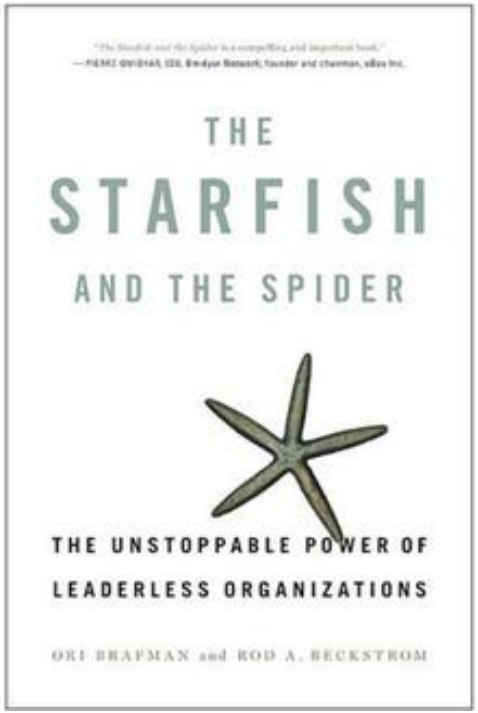


TECHNOLOGY EVOLUTION



FOR THE KEEN


THE BUSINESS
BLOCKCHAIN
promise, practice, and application of the next Internet technology
foreword by Vitalik Buterin
WILLIAM MOUGAYAR
Author of Centerless
WILEY


THE
STARFISH
AND THE SPIDER
THE UNSTOPPABLE POWER OF
LEADERLESS ORGANIZATIONS
ORI BRAFMAN and ROD A. BECKSTROM

SUMMARY - ALMOST AT THE END…

Bitcoin

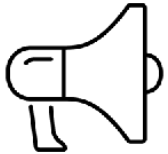
- A volatile digital computer-currency
- Mined from mathematics
- Currently $8500CAD

Blockchain

- Secure, tamperproof, shared ledger
- Alternative to centralized systems
- Nobody in charge?
- Spread the infrastructure across the network

Consortiums

- Slow moving
- Those with industry influence already are best placed to change
- Changing something that isn't broken is an uphill battle



Hype

- Technology is maturing
- Security vs Scalability issues
- Currently at the spreadsheet level of capabilities (Q4 2017)

Operations - what do you need to know?

- Still somewhat a puzzle how to apply for everybody - what's the business case?
- Just moving out of innovation labs, risky implementation projects
- Efficiencies promises - no more reconciliation, faster settlement, fewer middle men and lower fees?

IFIC

THANK YOU

PAUL IVES

IFDS, Suite 1, 30 Adelaide St E, Toronto, M5C 3G9
Tel: **416 506 8004**

pmives@dstsystems.com
https://ca.linkedin.com/in/pmives

I like coffee :-)