BITCOIN AND CRYPTOCURRENCIES

Lecture 2: Blockchain History: From the Cypherpunk Movement to JP Morgan Chase

Professor Radjabov Mukhammad

This is not a Bitcoin introduction. This is a high-level introduction to Blockchain technology. However, we should acknowledge that Satoshi Nakamoto (pseudonym) and his/their creation, Bitcoin, popularized Blockchain technology. (There are currently arguments that Bitcoin was not the first blockchain.)

Today there are various *flavors* of Blockchain. This paper attempts to generalize Blockchain with samples in some of those flavors. Additional research, prototyping, and due diligence should be exercised before making any long-term decisions.

Lastly, it is the opinion of the author, no single Blockchain solution will fulfill all needs. As many of the Blockchain technologies are paradigm specific, one should educate themselves on when and how to implement a Blockchain solution. Perhaps more importantly, when NOT to implement a solution.

On October 31, 2008, *Satoshi Nakamoto* released the Bitcoin White Paper outlining a purely peer to peer electronic cash/digital asset transfer system. This is the first popular implementation of Blockchain and is attributed as birthing today's Blockchain industry. Since then, additional Blockchains have been popularized, Ethereum, various Hyperledger project solutions, as well as numerous others including "Blockchain like" solutions such as *GuardTime's KSI* products

Blockchain is a system comprised of..

- Transactions
- Immutable ledgers
- Decentralized peers
- Encryption processes
- Consensus mechanisms
- Optional Smart Contracts

Let's explore these concepts

As with enterprise transactions today, Blockchain is a historical archive of decisions and actions taken

Proof of history, provides provenance

Notable transaction use cases
Land registration – Replacing requirements for research of Deeds (Sweden Land Registration)
Personal Identification – Replacement of Birth/Death certificates, Driver's Licenses, Social Security Cards (Estonia)
Transportation – Bills of Lading, tracking, Certificates of Origin, International Forms (Maersk/IBM)
Banking – Document storage, increased back office efficiencies (UBS, Russia's Sberbank)
Manufacturing – Cradle to grave documentation for any assembly or sub assembly
Food distribution – Providing location, lot, harvest date Supermarkets can pin point problematic food (Walmart)
Audits – Due to the decentralized and immutable nature of Blockchain, audits will fundamentally change.

Demo - https://anders.com/blockchain/blockchain.html

As with existing databases, Blockchain retains data via transactions

The difference is that once written to the chain, the blocks can be changed, but it is extremely difficult to do so. Requiring rework on all subsequent blocks and consensus of each.

The transaction is, immutable, or indelible

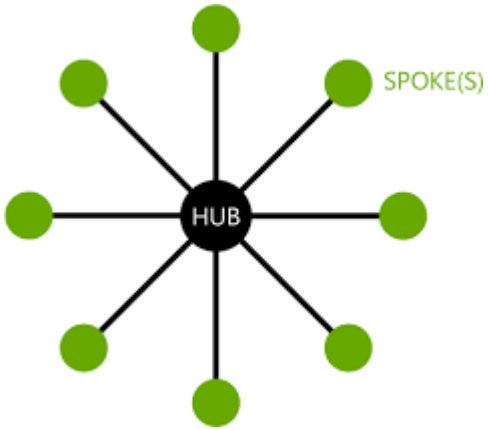
In DBA terms, Blockchains are Write and Read only

Like a ledger written in ink, an error would be be resolved with another entry

Rather than the centralized “Hub and Spoke” type of network, Blockchain is a decentralized peer to peer network. Where each NODE has a copy of the ledger.

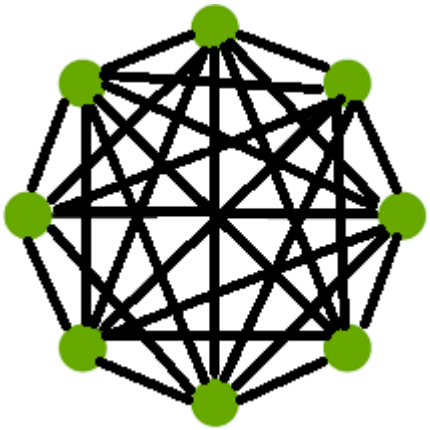
Legacy Network

Centralized DB



Blockchain Network

Distributed Ledgers



Standard encryption practices

Some Blockchains allow for “BYOE” (Bring Your Own Encryption)

Only as good as the next hardware innovation

All blocks are encrypted

Some Blockchains are public, some are private

- Public Blockchains are still encrypted, but are viewable to the public, e.g. https://www.blocktrail.com/BTC
- Private Blockchains employ user rights for visibility, e.g.
  - Customer – Writes and views all data
  - Auditors – View all transactions
  - Supplier A – Writes and views Partner A data
  - Supplier B – Writes and views Partner B data

Ensures that the next block in a blockchain is the one and only version of the truth

Keeps powerful adversaries from derailing the system and successfully forking the chain

Many Consensus mechanisms, each with pros and cons

Consensus Mechanism
Proof of Work
Proof of State
Proof of Elapsed Time
Proof of Activity
Proof of Burn
Proof of Capacity
Proof of Importance
And others….

Computer code

Provides business logic layer prior to block submission

Blockchain	Smart Contracts?	Language	
Bitcoin	No		
Ethereum	Yes	Solidity	
Hyperledger	Yes	Various	GoLang, C++, etc, depends
Others	Depends	Depends	

BLOCKCHAIN CAPABILITIES

A shared ledger technology allowing any participant in the business network to see the system of record (ledger)

Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

All parties agree to network verified transaction

Business terms embedded in transaction database & executed with transactions

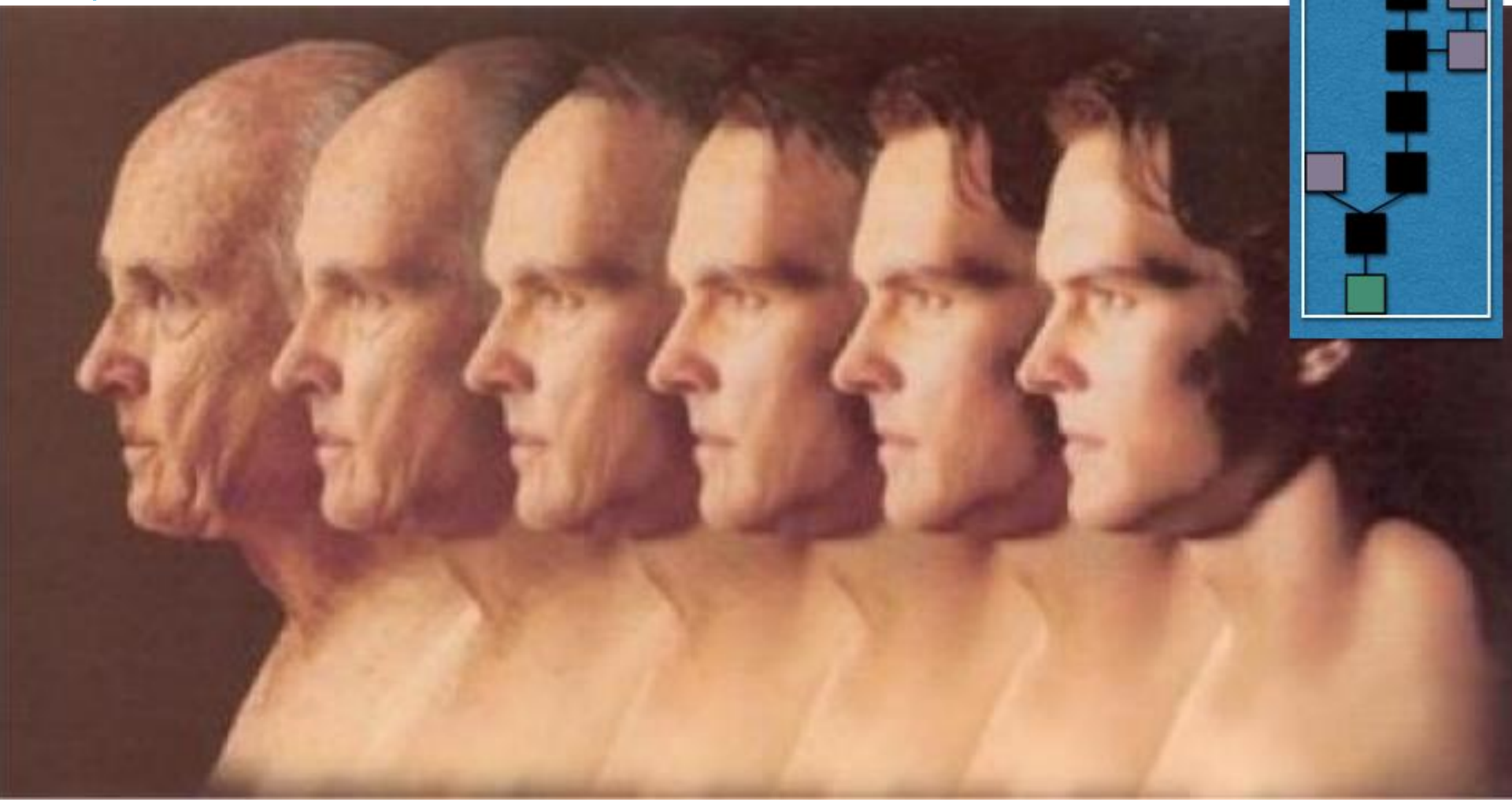
Blockchain Essentials

1. A business problem to be solved
   - That cannot be solved with more mature technologies
2. An identifiable business network
   - With Participants, Assets and Transactions
3. A need for trust
   - Consensus, Immutability, Finality or Provenance

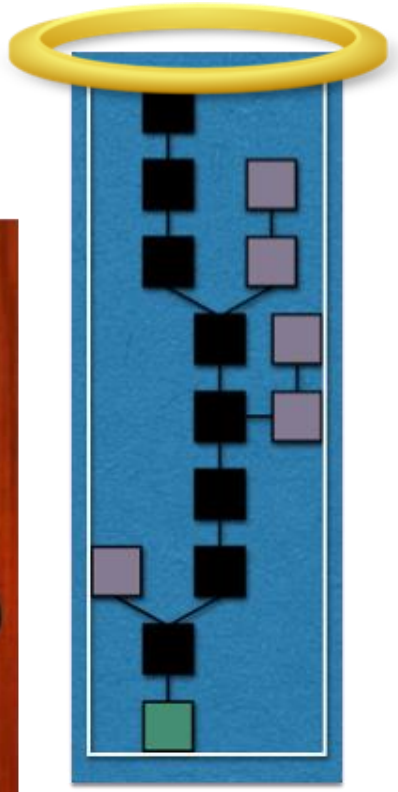
Negative Indicators, Anti-Patterns

1. **Need high performance (millisecond) transactions**
2. **Small organization (no business network)**
3. **Looking for a database replacement**
4. **Looking for a messaging replacement**
5. **Looking for transaction processing replacement**
6. **Process and metrics are not clear within the ecosystem**
7. **Value, velocity and/or variability are not present**

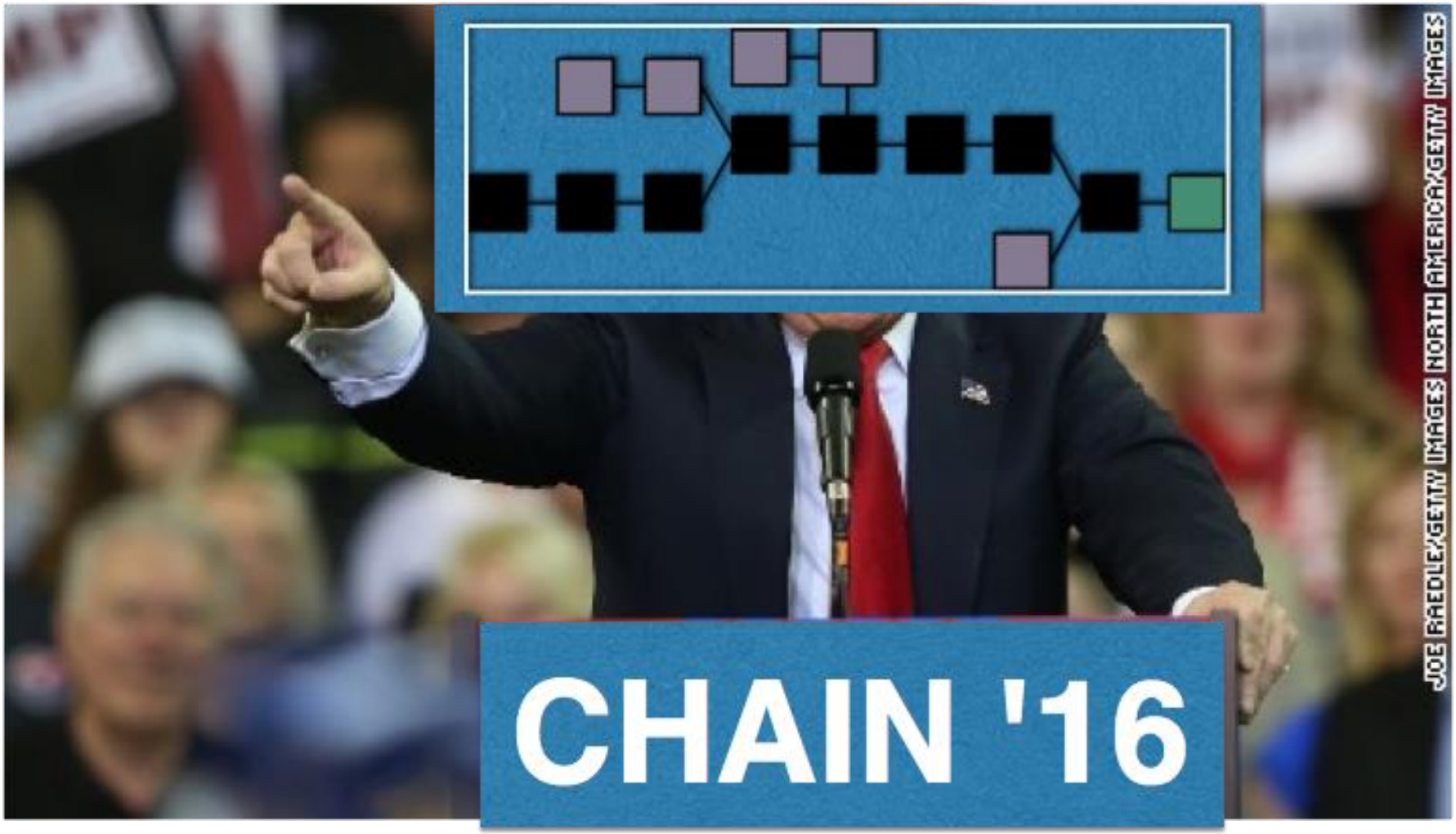
REVERSING AGING



BRINGING PEACE TO MIDDLE EAST



SAVING THE REPUBLICAN PARTY



REAL INDICES OF PROMISE

Incredible array of participants here today:

- **Bitcoin market cap: circa $7 Billion**
- **Blockchain VC funding to date: $1.1+ Billion**
- **Projected bank investment in 2017: $1 Billion[1]**

[1]Source: Magister Advisors, http://magisteradvisors.com/blockchain-bitcoin-2016-a-survey-of-global-lead

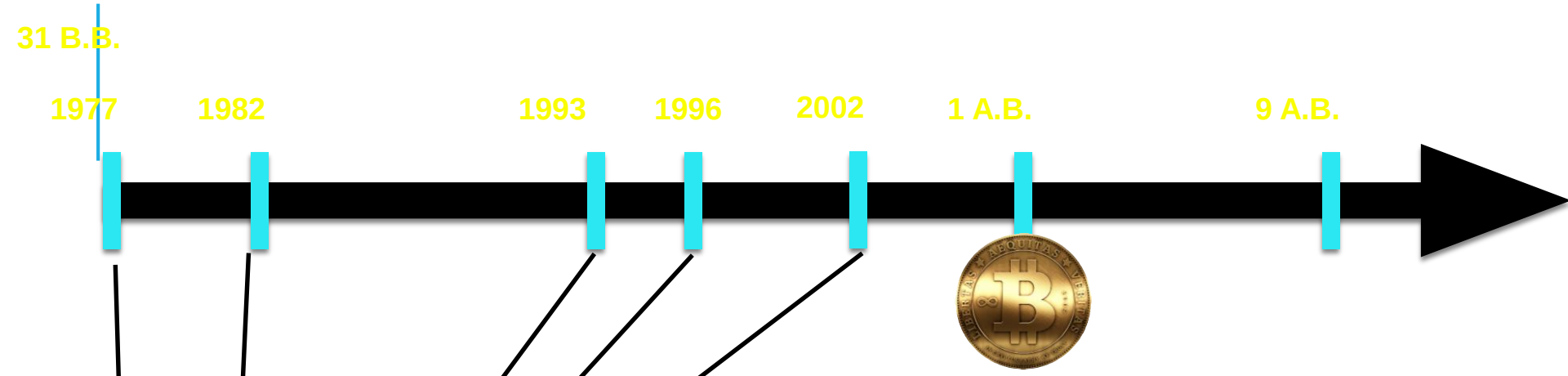
THE COMMUNITY OF CORE OVATORS IS FRACTURING…

… often over trifles

IN THE BEGINNING, THERE WAS THE COIN
THE YEAR 1 A.B. (A.K.A. 2008)

The Genesis Block

ACTUALLY…



- RSA invented—digital currency an early proposed application
- Anonymous cryptocurrency introduced (Chaum)
- Proofs of work introduced (Dwork and Naor)
- First proof-of-work-based cryptocurrency (Rivest a Shamir)
- Karma: P2P currency

Bitcoin / blockchains underpinned by academic / scientific innovation

IC3 GOALS

Bring *science of blockchains* to forefront of blockchain technology development

Partner academia with industry to deliver *innovation embodied in code*

Provide *independent expertise*

Try to solve biggest problems not monolithically, but in agenda of

Five Grand Challenges

TEMPEST IN A TEAPOT?

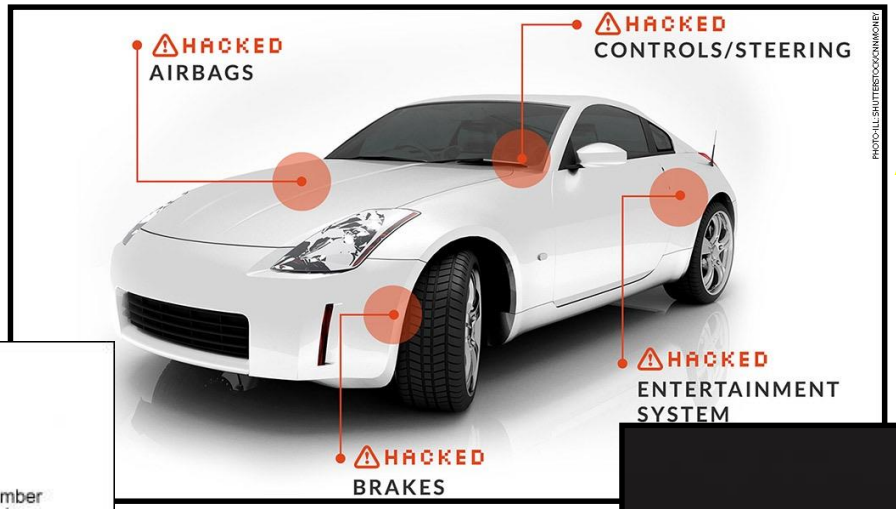
#1

#1: SCALING AND PERFORMANCE

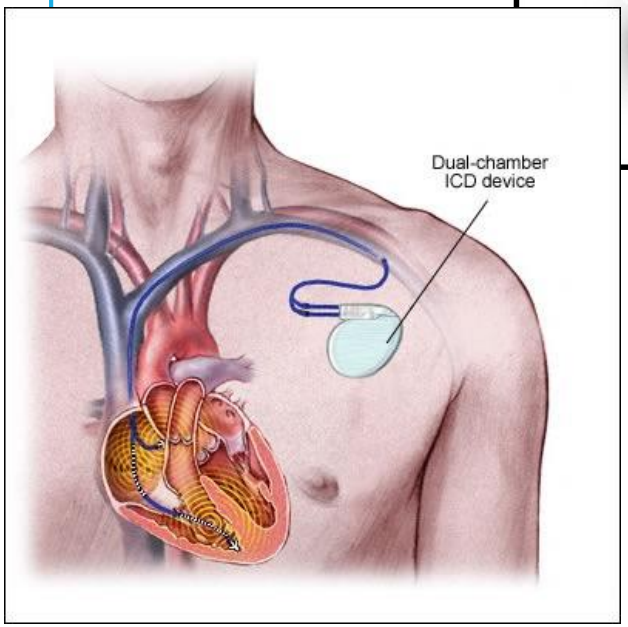
Don't tweak parameters. Reinvent consensus.

- **Challenge: Scale up blockchains to handle intensive global workloads**
- **What IC3 is aiming to do:**
  - **Decentralized blockchains:**
    - **Study of limitations in current systems**
    - **Achieving much higher throughput (100 tx / sec)**
  - **Permissioned / consortium blockchains:**
    - **Toward 100,000+ tx / sec via hybridization and sharding**

#2



Automobiles



Medical devices

RFID devices

Law of history? Every industry must (painfully) relearn the lesson that rigorous security is critical.

#2: CORRECTNESS

- **Challenge: Defy history! Make it easy for blockchain developers to produce secure protocols and code.**
- **What IC3 is aiming to do:**
  - **Programming language techniques to create useable semantics and correct code**
  - **Cryptographic protocols with security proofs**

TRANSPARENCY IS BEAUTIFUL

#3

But confidentiality is critical to business

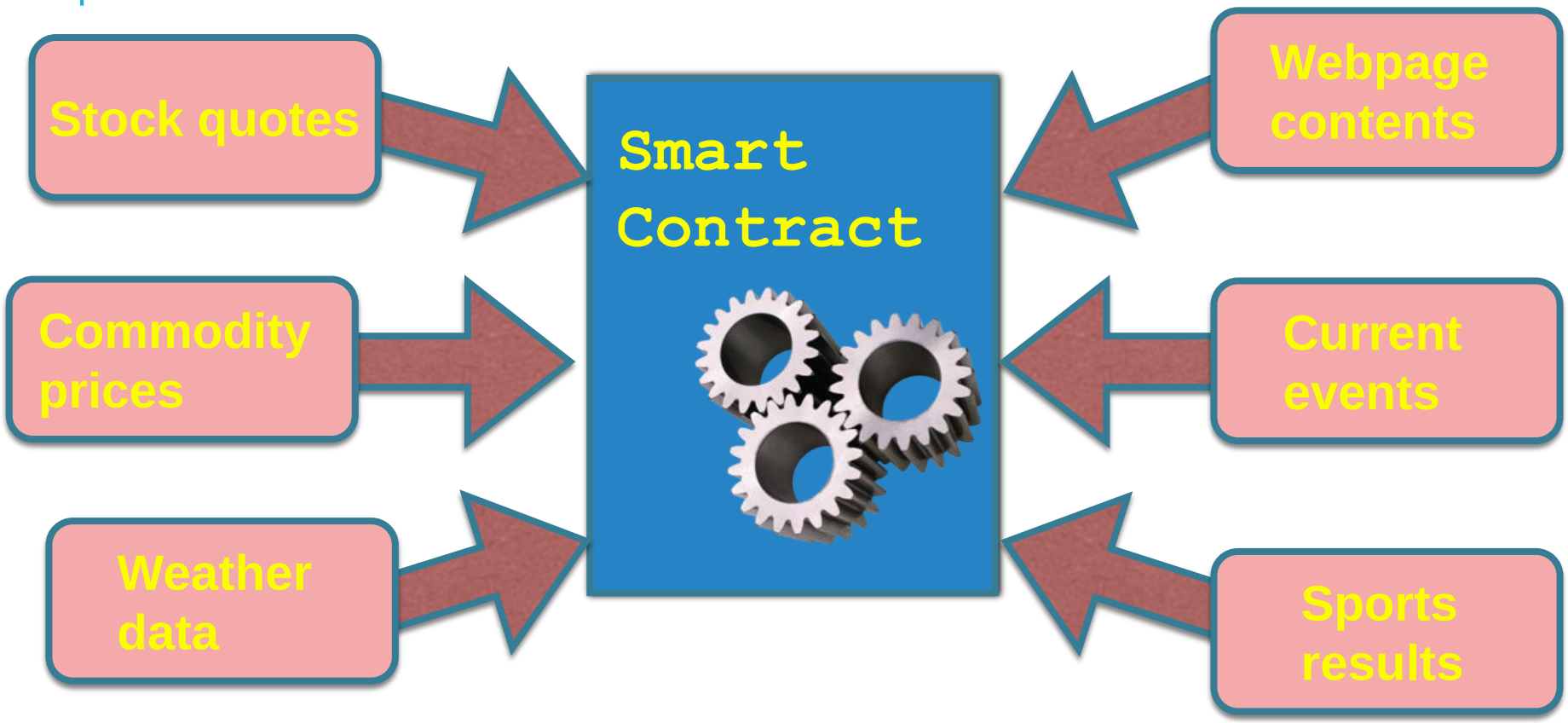
#3: CONFIDENTIALITY

Challenge: Square transparency with confidentiality in blockchains.

What IC3 is aiming to do:

- Cryptographic approaches (Hawk, Solidus)
- Trusted-hardware approaches

INTERESTING SMART CONTRACTS NEED *TRUSTWORTHY DATA*



Today there are no good sources.

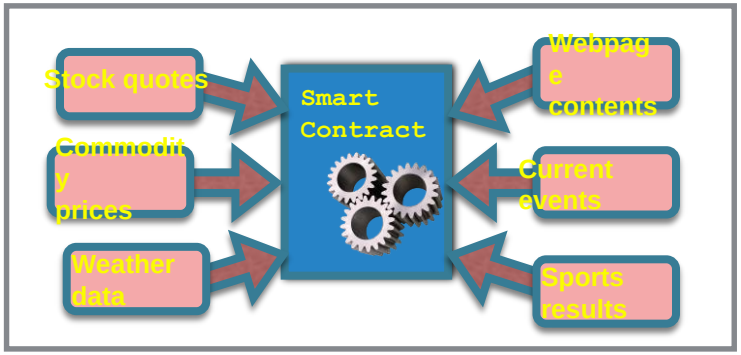
#4

#4: AUTHENTICATED DATA

Challenge: Create robust ecosystem of trustworthy data feeds for blockchains.

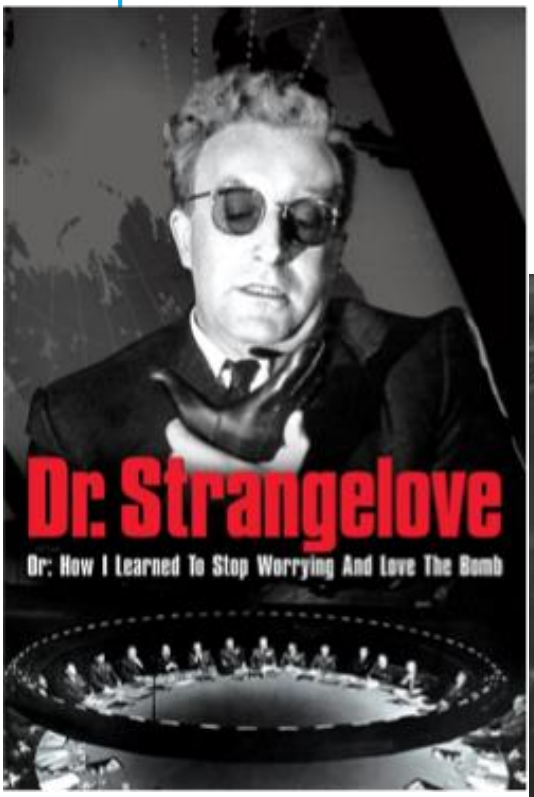
What IC3 is aiming to do:

- Building high-trust data feeds (Town Crier, Virtual Notary)



WHERE THERE ARE AUTONOMOUS AGENTS

#5



#5 WHERE THERE ARE AUTONOMOUS AGENTS

Little accidents will happen

#5: SAFETY AND COMPLIANCE

Challenge: Enable effective monitoring and targeted intervention in blockchains.

What IC3 is aiming to do:

- Studying traditional contract law and risks of crime in smart contracts
- Problem-solving session on regulatory challenges

GOAL OF RETREAT

Determine IC3 agenda over the next few years

- **Grand challenges are important but broad**
- **Let's understand problems of key interest to you.**
  - **Takeaway: research partnerships**
- **Our first retreat, but we have basic NSF funding for multi-year period**
- **Let's work together to *advance the science and applications of blockchains***

Bitcoin White Paper – Satoshi Nakamoto

Blockchain Demo – Anders Brownworth

- Videos

Blockchain for Business - An Introduction to Hyperledger Technologies - edX.org

Ethereum White Paper

Guardtime – Blockchain *like* official site

Hyperledger official site - Linux Foundation

IBM Blockchain for Business – IBM Dev Center

IBM Blockchain Essentials Course – IBM Dev Center

IBM Blockchain Foundation Developer – IBM Dev Center

- Many more and pages are always changing

REFERENCE

The Bitcoin Standard: The Decentralized Alternative to Central Banking – Illustrated, April 24, 2018 by Saifedean Ammous

The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Crypto Trading, Derivatives, Digital Assets) – Illustrated, September 15, 2018 by Antony Lewis (Author)

Blockchain Bubble or Revolution: The Future of Bitcoin, Blockchains, and Cryptocurrencies – June 12, 2019 by Neel Mehta (Author), Aditya Agashe (Author), Parth Detroja (Author)

Cryptocurrency Investing For Dummies – March 6, 2019 by Kiana Danial

Cryptocurrency Mining For Dummies– Illustrated, December 5, 2019 by Peter Kent

Cryptocurrency Mining: A Complete Beginners Guide to Mining Cryptocurrencies, Including Bitcoin, Litecoin, Ethereum, Altcoin, Monero, and Others – February 21, 2018 by Crypto Tech Academy (Author)