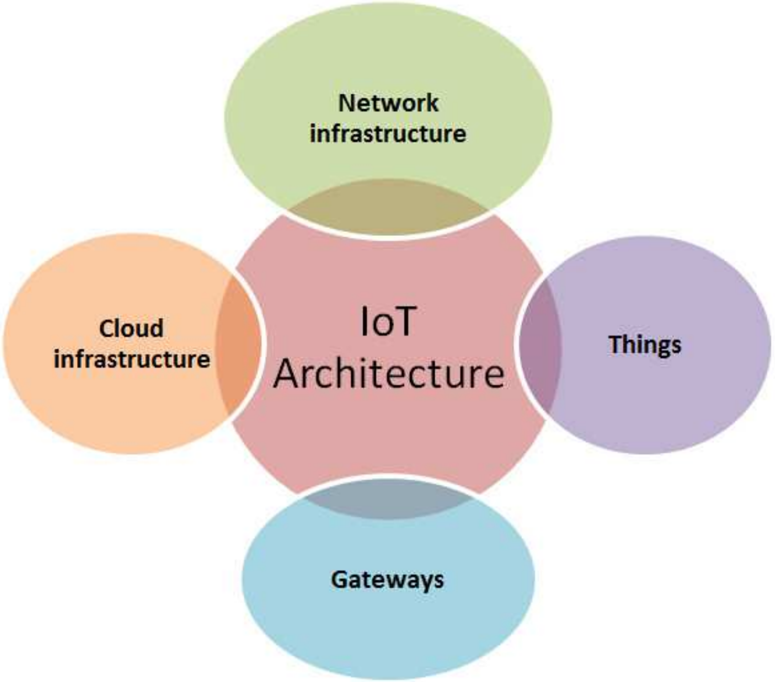
Blockchain and Smart Contracts:
Relevance of Security Facts and Myths to Industrial Control

R. R. Brooks – rrb@g.clemson.edu
Clemson University
Electrical and Computer Engineering

September 20th, 2018

IoT, SCADA, CPS Devices



- □ Devices have intelligence, networking, sensing, storage,
- □ Low cost, no upgrades, security an after thought,
- □ Control actuators,
- □ Limited to no human supervision,
- □ Vulnerable to tampering, insider threats, network exploitation,
- □ Documented use in DDoS, sabotage, infrastructure attacks.

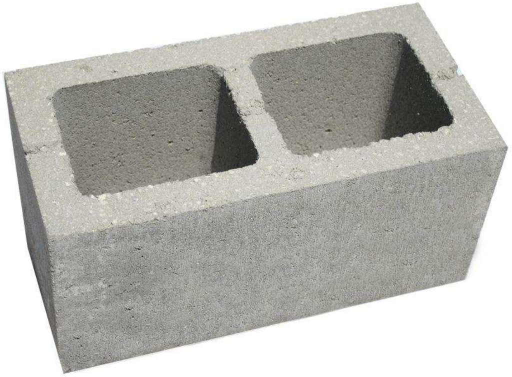
What IS a Blockchain?

□ A convenient way to get people to throw money at you.

What DEFINES a Blockchain?

Background
IoT, SCADA, CPS Devices
What IS a Blockchain?
▷ What DEFINES a Blockchain?
Blockchain hype
Blockchain anti-hype
Promising Blockchains
Promising Blockchains
Promising Blockchains
Flawed Blockchains
Blockchain IoT reality
Conclusions

- □ Original blockchain was a distributed trustless mechanism for timestamping files.[1]
- □ True blockchains are distributed.
- □ True blockchains are decentralized.
- □ True blockchains are trustless.
- □ True blockchains are immutable (theoretically).



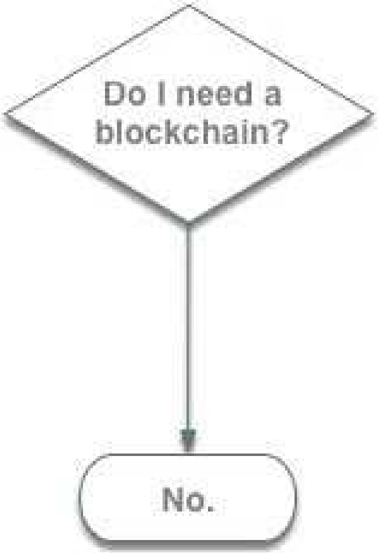
OR

[1] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

Blockchain hype

- □ Distributed ledger built from signed transactions,
- □ Security assured by the network,
- □ Data perfectly secure,
- □ Provides transparency,
- □ Provides global access,
- □ Smart contracts provide secure program execution.

Blockchain anti-hype


Do I need a blockchain?

No.

□ Blockchain is just a git,

□ Can not include any authorization,

□ Only good for buying drugs and money laundering,

□ Ethereum did rollback and hard fork after massive theft.

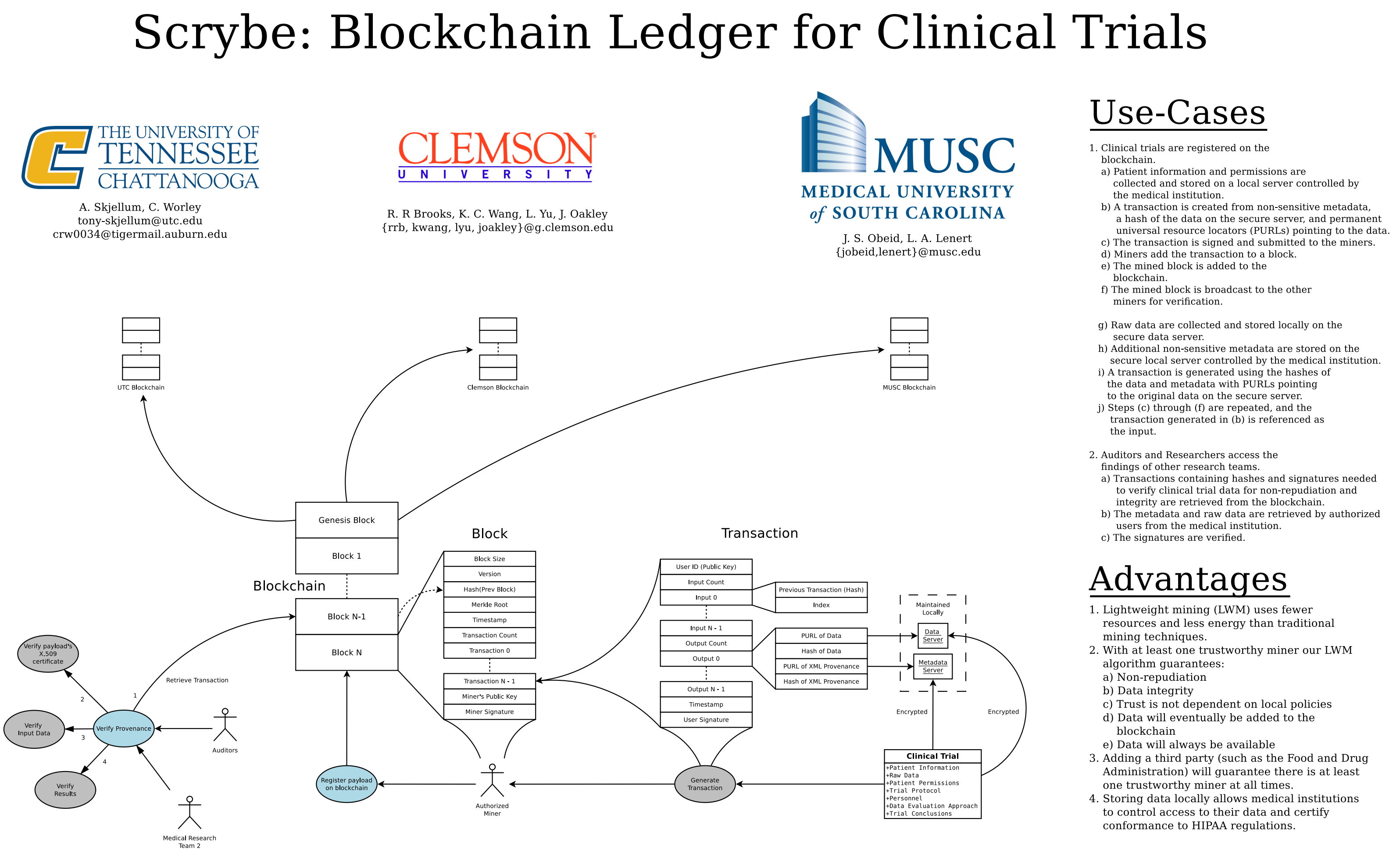
Promising Blockchains

- □ Hosted by the Linux Foundation,
- □ Focus on standardization,
- □ Modular blockchain,
- □ Modular mining algorithms.

https://www.hyperledger.org/

Promising Blockchains

Background
IoT, SCADA, CPS Devices
What IS a Blockchain?
What DEFINES a Blockchain?
Blockchain hype
Blockchain anti-hype
Promising Blockchains
▷ Promising Blockchains
Promising Blockchains
Flawed Blockchains
Blockchain IoT reality
Conclusions



Scrybe: Blockchain Ledger for Clinical Trials

THE UNIVERSITY OF TENNESSEE CHATTANOOGA
A. Skjellum, C. Worley
tony-skjellum@utc.edu
crw0034@tigermail.auburn.edu

CLEMSON UNIVERSITY
R. R Brooks, K. C. Wang, L. Yu, J. Oakley
{rrb, kwang, lyu, joakley}@g.clemson.edu

MUSC MEDICAL UNIVERSITY of SOUTH CAROLINA
J. S. Obeid, L. A. Lenert
{jobeid,lenert}@musc.edu

Use-Cases

1. Clinical trials are registered on the blockchain.
   a) Patient information and permissions are collected and stored on a local server controlled by the medical institution.
   b) A transaction is created from non-sensitive metadata, a hash of the data on the secure server, and permanent universal resource locators (PURLs) pointing to the data.
   c) The transaction is signed and submitted to the miners.
   d) Miners add the transaction to a block.
   e) The mined block is added to the blockchain.
   f) The mined block is broadcast to the other miners for verification.

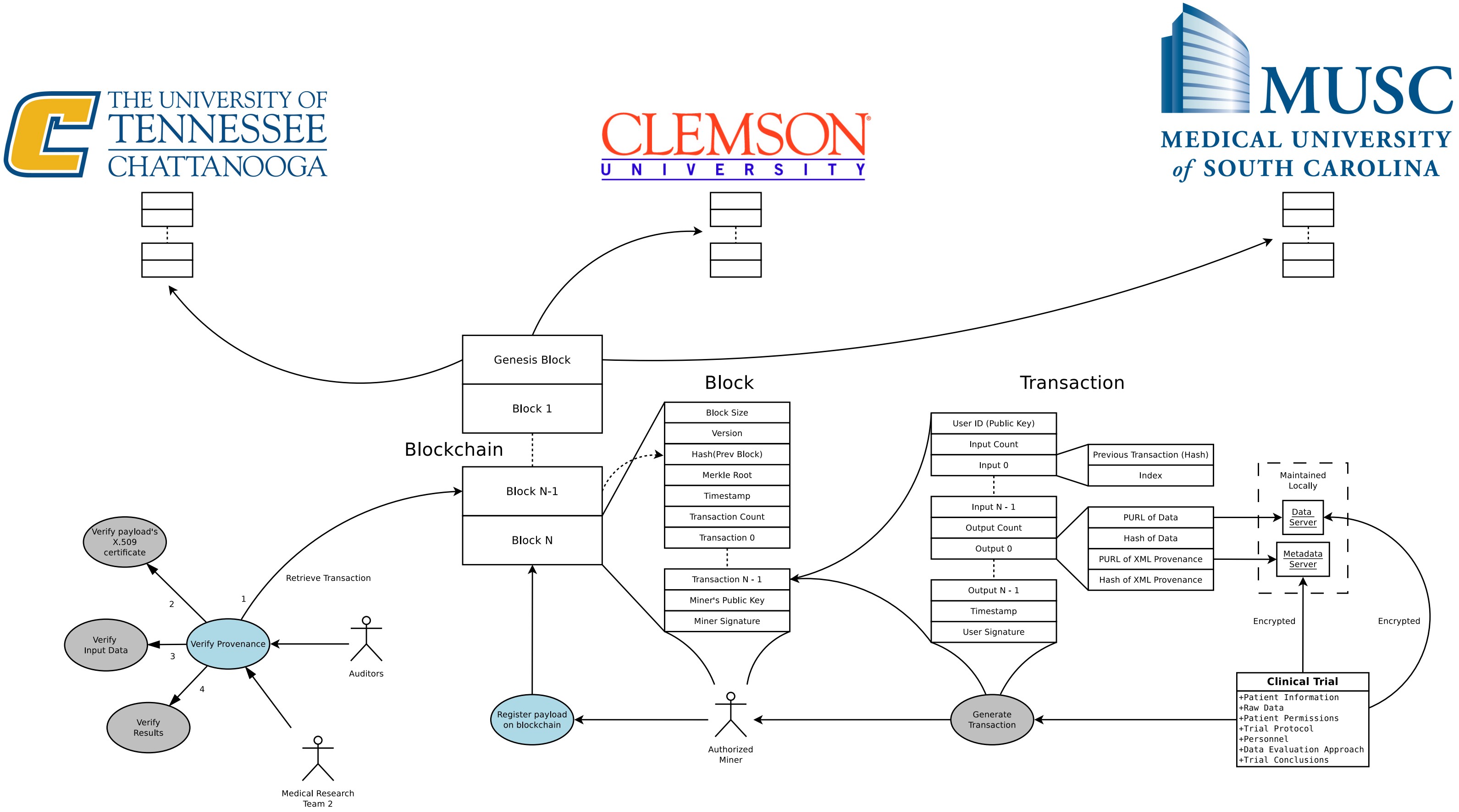
   g) Raw data are collected and stored locally on the secure data server.
   h) Additional non-sensitive metadata are stored on the secure local server controlled by the medical institution.
   i) A transaction is generated using the hashes of the data and metadata with PURLs pointing to the original data on the secure server.
   j) Steps (c) through (f) are repeated, and the transaction generated in (b) is referenced as the input.

2. Auditors and Researchers access the findings of other research teams.
   a) Transactions containing hashes and signatures needed to verify clinical trial data for non-repudiation and integrity are retrieved from the blockchain.
   b) The metadata and raw data are retrieved by authorized users from the medical institution.
   c) The signatures are verified.

Advantages

1. Lightweight mining (LWM) uses fewer resources and less energy than traditional mining techniques.
2. With at least one trustworthy miner our LWM algorithm guarantees:
   a) Non-repudiation
   b) Data integrity
   c) Trust is not dependent on local policies
   d) Data will eventually be added to the blockchain
   e) Data will always be available
3. Adding a third party (such as the Food and Drug Administration) will guarantee there is at least one trustworthy miner at all times.
4. Storing data locally allows medical institutions to control access to their data and certify conformance to HIPAA regulations.

Scrybe: Blockchain Ledger for Clinical Trials



Flawed Blockchains

- □ Any private blockchain that isn't checked in to the main chain,
- □ Testnet blockchains,
- □ Blockchains with weak mining algorithms,
- □ Blockchains with broken consensus algorithms,
- □ Blockchains with centralized authorities,
- □ Blockchains promising to solve all your problems.

Transparency

□ **Blockchain == global transparency and perfect security**

- You decide what data is in the chain,
- Signed hashes of transactions necessary, reveals nothing,
- Add other information as needed to support reliable audit,
- Store data mainly off-chain, access controlled, hash guarantees security,
- Our project works with clinical trial data, stores HIPAA information consistent with HIPAA,
- Blockchain provides audit capability consistent with FDA.

Efficiency

□ Proof of work == inefficient, bad for environment,

- Random search for nonces that give right hash,

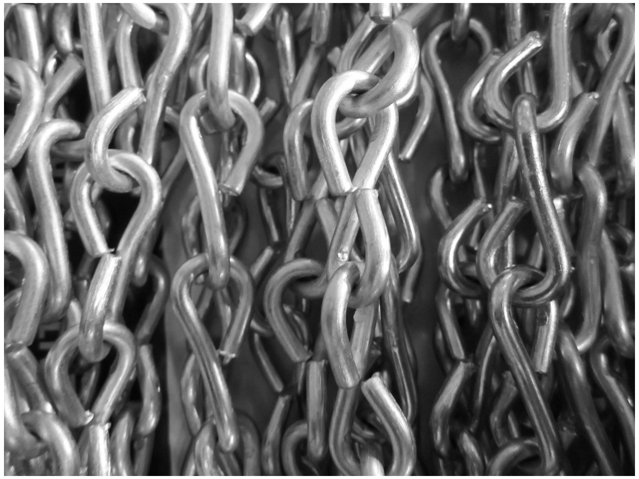
□ Proof of stake == users with most controls systems,

- Lets system predict miners for next round,

□ Our system has *light weight mining*,

- Applying for IP protection, efficient random choice,
- Provides same or better security.

Sidechains



- □ BTC, Ethereum Blockchains have global name space,
- □ IoT data either globally shared or private,
- □ Lightning and other extensions defining sidechains,
- □ Provides not quite same security,
- □ Partitions global system into regions with trusted data sharing,
- □ Might fight BGP route injection to partition net, which has attacked mining pools.

Smart contracts

- □ Currently only inputs data from blockchain,
- □ Same program runs on each miner,
- □ Race conditions leveraged to steal millions of USD,
- □ Need to interface with side-chains, allow efficient resource use,
- □ Need verifiable contracts without exploits.

Open problems

- □ Lots of privacy enhanced alt-coins,
- □ Not convinced that alt-coins really are secure and private. *Side-channels.*
- □ Lots of exploits in wallets lead to theft,
- □ Lots of fake wallets distributed leading to theft,
- □ *Mining* has many alternatives. Security and efficiency trade-offs need more study,
- □ *Mining malware* is wide-spread, but for BTC mining you really need ASICs. Not a good use of infected zombies,
- □ Applications other than currency are probably a better fit,

Blockchain Checklist

□ Is it truly decentralized?

- How many nodes are currently participating?

□ Is it leveraging existing blockchain technology?

- Will it be limited by existing blockchain technology?

□ How expensive is the mining algorithm?

- Will it limit scalability?
- Will it be broken in a year?

□ Are there any centralized authorities?

- Can they be trusted? – No.

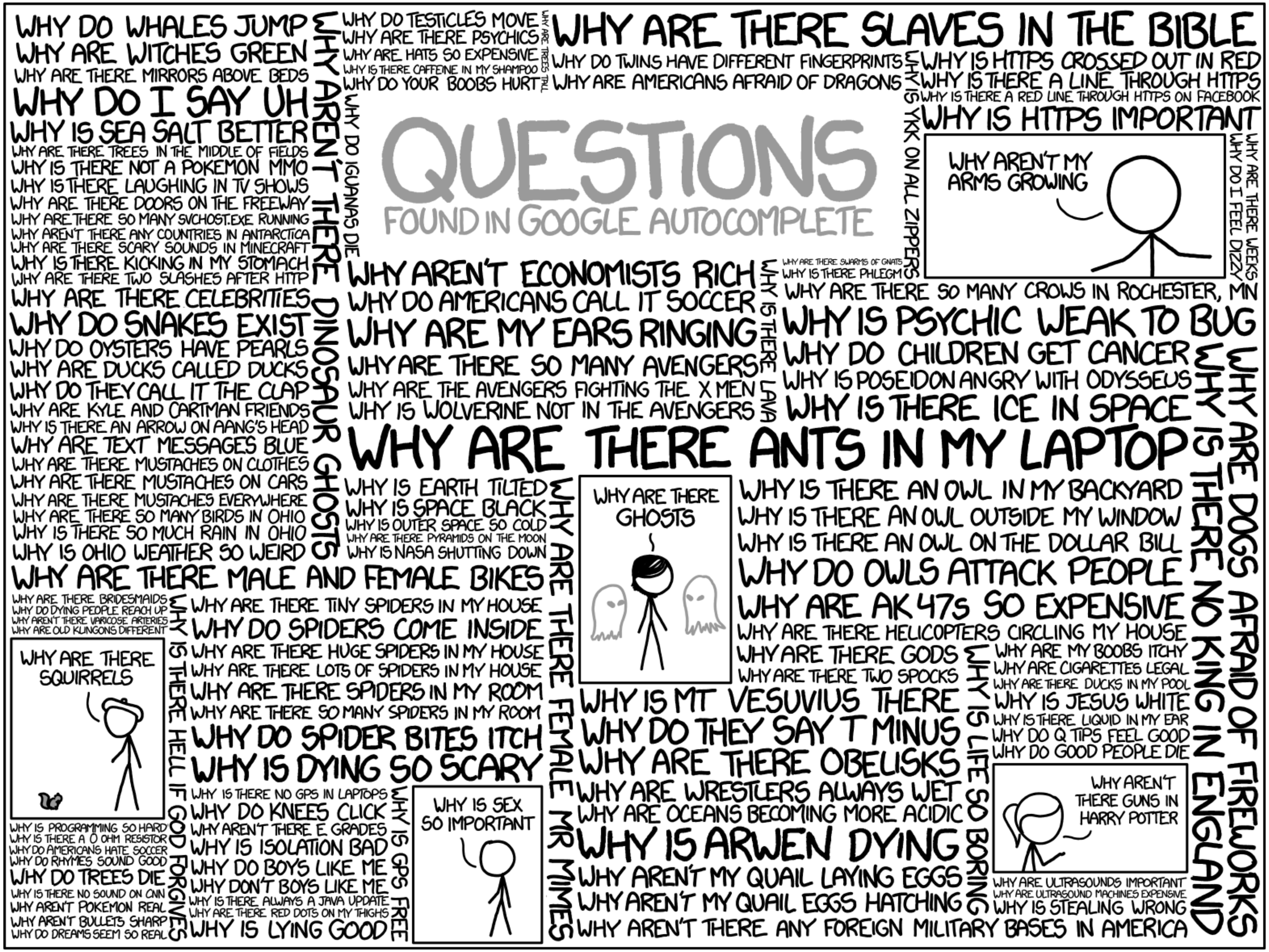
If you don't believe it or don't get it, I don't have the time to try to convince you, sorry.

– Satoshi Nakmoto

Summary

- □ Blockchain not a perfect solution,
- □ Blockchain's distributed security model has potential for SCADA and IoT,
- □ Modifications of smart contracts good for avoiding small intrusions and some insider threats,
- □ Distributed audit trail is a great application. We are working with a medical school on this.
- □ Side-chains can make more efficient. Provide right amount of transparency.

Questions?


WHY DO WHALES JUMP
WHY ARE WITCHES GREEN
WHY ARE THERE MIRRORS ABOVE BEDS
WHY DO I SAY UH
WHY IS SEA SALT BETTER
WHY ARE THERE TREES IN THE MIDDLE OF FIELDS
WHY IS THERE NOT A POKEMON MMO
WHY IS THERE LAUGHING IN TV SHOWS
WHY ARE THERE DOORS ON THE FREEWAY
WHY ARE THERE SO MANY SVCHOST.EXE RUNNING
WHY AREN'T THERE ANY COUNTRIES IN ANTARCTICA
WHY ARE THERE SCARY SOUNDS IN MINECRAFT
WHY IS THERE KICKING IN MY STOMACH
WHY ARE THERE TWO SLASHES AFTER HTTP
WHY ARE THERE CELEBRITIES
WHY DO SNAKES EXIST
WHY DO OYSTERS HAVE PEARLS
WHY ARE DUCKS CALLED DUCKS
WHY DO THEY CALL IT THE CLAP
WHY ARE KYLE AND CARTMAN FRIENDS
WHY IS THERE AN ARROW ON AANG'S HEAD
WHY ARE TEXT MESSAGES BLUE
WHY ARE THERE MUSTACHES ON CLOTHES
WHY ARE THERE MUSTACHES ON CARS
WHY ARE THERE MUSTACHES EVERYWHERE
WHY ARE THERE SO MANY BIRDS IN OHIO
WHY IS THERE SO MUCH RAIN IN OHIO
WHY IS OHIO WEATHER SO WEIRD
WHY AREN'T THERE DINOSAUR GHOSTS
WHY DO IGUANAS DIE
WHY DO TESTICLES MOVE
WHY ARE THERE PSYCHICS
WHY ARE HATS SO EXPENSIVE
WHY IS THERE CAFFEINE IN MY SHAMPOO
WHY DO YOUR BOOBS HURT
WHY ARE TREES TALL
WHY ARE THERE SLAVES IN THE BIBLE
WHY DO TWINS HAVE DIFFERENT FINGERPRINTS
WHY ARE AMERICANS AFRAID OF DRAGONS
QUESTIONS
FOUND IN GOOGLE AUTOCOMPLETE
WHY IS YKK ON ALL ZIPPERS
WHY IS HTTPS CROSSED OUT IN RED
WHY IS THERE A LINE THROUGH HTTPS
WHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK
WHY IS HTTPS IMPORTANT
WHY AREN'T MY ARMS GROWING
WHY ARE THERE WEEKS
WHY DO I FEEL DIZZY
WHY AREN'T ECONOMISTS RICH
WHY DO AMERICANS CALL IT SOCCER
WHY ARE MY EARS RINGING
WHY ARE THERE SO MANY AVENGERS
WHY ARE THE AVENGERS FIGHTING THE X MEN
WHY IS WOLVERINE NOT IN THE AVENGERS
WHY IS THERE LAVA
WHY ARE THERE SWARMS OF GNATS
WHY IS THERE PHLEGM
WHY ARE THERE SO MANY CROWS IN ROCHESTER, MN
WHY IS PSYCHIC WEAK TO BUG
WHY DO CHILDREN GET CANCER
WHY IS POSEIDON ANGRY WITH ODYSSEUS
WHY IS THERE ICE IN SPACE
WHY ARE THERE ANTS IN MY LAPTOP
WHY IS EARTH TILTED
WHY IS SPACE BLACK
WHY IS OUTER SPACE SO COLD
WHY ARE THERE PYRAMIDS ON THE MOON
WHY IS NASA SHUTTING DOWN
WHY ARE THERE MALE AND FEMALE BIKES
WHY ARE THERE FEMALE MR MIMES
WHY ARE THERE GHOSTS
WHY IS THERE AN OWL IN MY BACKYARD
WHY IS THERE AN OWL OUTSIDE MY WINDOW
WHY IS THERE AN OWL ON THE DOLLAR BILL
WHY DO OWLS ATTACK PEOPLE
WHY ARE AK 47s SO EXPENSIVE
WHY ARE THERE HELICOPTERS CIRCLING MY HOUSE
WHY ARE THERE GODS
WHY ARE THERE TWO SPOCKS
WHY IS LIFE SO BORING
WHY ARE MY BOOBS ITCHY
WHY ARE CIGARETTES LEGAL
WHY ARE THERE DUCKS IN MY POOL
WHY IS JESUS WHITE
WHY IS THERE LIQUID IN MY EAR
WHY DO Q TIPS FEEL GOOD
WHY DO GOOD PEOPLE DIE
WHY IS THERE NO KING IN ENGLAND
WHY ARE DOGS AFRAID OF FIREWORKS
WHY ARE THERE BRIDESMAIDS
WHY DO DYING PEOPLE REACH UP
WHY AREN'T THERE VARICOSE ARTERIES
WHY ARE OLD KLINGONS DIFFERENT
WHY IS THERE HELL IF GOD FORGIVES
WHY ARE THERE TINY SPIDERS IN MY HOUSE
WHY DO SPIDERS COME INSIDE
WHY ARE THERE HUGE SPIDERS IN MY HOUSE
WHY ARE THERE LOTS OF SPIDERS IN MY HOUSE
WHY ARE THERE SPIDERS IN MY ROOM
WHY ARE THERE SO MANY SPIDERS IN MY ROOM
WHY DO SPIDER BITES ITCH
WHY IS DYING SO SCARY
WHY ARE THERE SQUIRRELS
WHY IS PROGRAMMING SO HARD
WHY IS THERE A 0 OHM RESISTOR
WHY DO AMERICANS HATE SOCCER
WHY DO RHYMES SOUND GOOD
WHY DO TREES DIE
WHY IS THERE NO SOUND ON CNN
WHY AREN'T POKEMON REAL
WHY AREN'T BULLETS SHARP
WHY DO DREAMS SEEM SO REAL
WHY IS THERE NO GPS IN LAPTOPS
WHY DO KNEES CLICK
WHY AREN'T THERE E GRADES
WHY IS ISOLATION BAD
WHY DO BOYS LIKE ME
WHY DON'T BOYS LIKE ME
WHY IS THERE ALWAYS A JAVA UPDATE
WHY ARE THERE RED DOTS ON MY THIGHS
WHY IS LYING GOOD
WHY IS GPS FREE
WHY IS SEX SO IMPORTANT
WHY IS MT VESUVIUS THERE
WHY DO THEY SAY T MINUS
WHY ARE THERE OBELISKS
WHY ARE WRESTLERS ALWAYS WET
WHY ARE OCEANS BECOMING MORE ACIDIC
WHY IS ARWEN DYING
WHY AREN'T MY QUAIL LAYING EGGS
WHY AREN'T MY QUAIL EGGS HATCHING
WHY AREN'T THERE ANY FOREIGN MILITARY BASES IN AMERICA
WHY AREN'T THERE GUNS IN HARRY POTTER
WHY ARE ULTRASOUNDS IMPORTANT
WHY ARE ULTRASOUND MACHINES EXPENSIVE
WHY IS STEALING WRONG

https://xkcd.com/1256