CS5412/LECTURE 14
BLOCKCHAINS FOR IOT (PART 2)

Ken Birman
CS5412 Spring 2019

HTTP://WWW.CS.CORNELL.EDU/COURSES/CS5412/2019SP
Let’s look at a blockchain created specifically for IoT

Cornell has a new “smart farms” research effort.

Led by Susan McCouch, Hakim Weatherspoon and Abe Strouck.

One early accomplishment: Vegvisir, a BlockChain specifically for agriculture.
A BLOCKCHAIN FOR THE FOOD SUPPLY CHAIN

Robbert van Renesse

joint work with Hakim Weatherspoon, Danny Adams, Kolbeinn Karlsson, and Stephen B. Wicker

Initiative for Crypto-Currencies and Contracts (IC3)
Cornell Digital Agriculture Initiative
BLOCKCHAIN’S PROMISE

Promises

• Global currency
• Smart contracts
• Notarization
• Accountability
• …
A REPLICATED LEDGER OF TRANSACTIONS

Jane
(owns 15 bitcoins)

Joe
(owns 1 bitcoin)

Judy
(owns 15 bitcoins)

give 10 bitcoins to Jane

give 10 bitcoins to Joe

give 3 bitcoins to Judy
SMART CONTRACTS

*Smart contracts* are executable programs on the BlockChain, take input from the BlockChain, and produce output on the BlockChain.

Main use: *automated escrow*, where disbursement depends on agreed upon conditions.

Caution: Smart Contracts have been found to be prone to (very expensive) bugs.
POTENTIAL USE CASES

Killer app: cryptocurrencies

Other potential uses:
- Reduce opaqueness of supply chains
  - One “trustless” place for all transactions along the way
  - Improvements over paper-based systems and many disjoint databases
- Eliminate middlemen
  - Why does farmer make so little and consumer pay so much?
- Reduce fraud
  - India, Russia, Sweden, Georgia… are building blockchain-based land registries to fight “land fraud” and simplify international property transactions
FOR THE FOOD SUPPLY CHAIN?

Supply chain management
- Walmart is building one for the food supply chain
- Food safety: fast identification of tainted foods
- Consumers are demanding more information about the products they buy (organic, fair trade, …)
- Simplify international transactions

Help farmers
- Want to know what happens to their products for fair pricing
- What products should they be producing?

Reduce food scandals
- illegal production, misrepresentation, loss and waste, …
INDUSTRIAL UPTAKE?

ripe.io:
- A company that is building a “blockchain of food” with IoT interfaces

Walmart:
- partnered with IBM and Tsinghua to identify sources of contaminated products and speed up recall

But today’s blockchain technology may not be appropriate for all use cases
- too dependent on availability of plentiful power, networking, and storage
DESIRED BLOCKCHAIN PROPERTIES

Performance:
- High Throughput, Low Latency
- Energy-Efficient

Security:
- Always available for reading (verifying) and appending
- Fair
- Tamperproof (Integrity)
- Possibly confidentiality as well

No Single Administrative Domain
- *no need to trust a single provider*

Open membership (or not)
OPEN MEMBERSHIP IS HARD

Traditional secure logs are based on voting
Members vote on which transactions to add to the log and in what order

Problem: “Sybil” or impersonation attacks
  ▪ a participant may try to vote multiple times
  ▪ with closed membership, cryptographic signatures can identify the source of a vote
  ▪ with open membership, anybody can create identities and that way vote many times
# Permissionless vs Permissioned Blockchains

<table>
<thead>
<tr>
<th></th>
<th>Permissionless</th>
<th>Permissioned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approach</td>
<td>Competitive</td>
<td>Cooperative</td>
</tr>
<tr>
<td>Basic technique</td>
<td>Proof-of-Resource</td>
<td>Voting</td>
</tr>
<tr>
<td>Membership</td>
<td>Open</td>
<td>Closed</td>
</tr>
<tr>
<td>Energy-efficiency</td>
<td>Often terrible</td>
<td>Excellent</td>
</tr>
<tr>
<td>Transaction rate</td>
<td>At best hundreds / sec</td>
<td>Many thousands per second</td>
</tr>
<tr>
<td>Transaction latency</td>
<td>As high as many minutes</td>
<td>Less than a second</td>
</tr>
</tbody>
</table>
Permissionless, open membership

Proof-of-Work

There are thousands of Bitcoin miners
  • they use ASIC hardware to compute SHA256 hashes
  • use about more energy than the country of Denmark

Overall rate is a few transactions per second
THE BLOCKCHAIN

Ledger

nonce

HASH( ) < target

“cryptopuzzle”
THE BLOCKCHAIN
THE BLOCKCHAIN
THE BLOCKCHAIN

Exponentially distributed rate of new blocks, with constant mean interval

target automatically adjusted every 2016 blocks so that mean interval is 10 minutes
INCENTIVES FOR MINING

Prize:
- "Minting"
- Transaction Fees

Wins proportional to computation power
Two blocks “mined” at approximately the same time by two different miners
FORK RESOLUTION

- **Longest** chain wins
- Transactions on short chain are reverted
A transaction is **confirmed** when it is **buried** “deep enough” (typically 6 blocks – i.e., one hour)
SECURITY THREAT!

![Diagram of connected nodes with time t]

23
SECURITY THREAT!

Threat: attacker outruns good miners
Threat: attacker outruns good miners

**Security Assumption:** good miners own >.5 of the total compute power

[blockchain.info, April 2015]
PERMISSIONLESS BLOCKCHAINS

Open membership, but inefficient
Vulnerable to 50% attacks
Examples include Bitcoin, Ethereum, IOTA
PERMISSIONED BLOCK CHAINS

Performance:
- High Throughput, Low Latency
- Energy-efficient

Security:
- No forks!

Closed membership

Examples include Ripple, Hyperledger
**BLOCKCHAIN FOR THE FARM?**

Blockchains require strong network connectivity and lots of storage

Permissionless blockchain are power-hungry

Sensors have limited resources

- Sensors for growing conditions, storage conditions, shipping conditions, …

*Blockchain for a farm will generate records in a decentralized way, and hence it *must* work in a network-partitioned or -challenged environment*
Vegvisir: tolerate branches

- Leads to DAG structure instead of linear blockchain
- Still maintains full causal history of events (respect’s Lamport’s →)
Proof-of-Witness to persist blocks securely

No more than $k$ malicious nodes in any neighborhood

At least one copy of a valid block will survive if $<k$ malicious peers
Support Blockchain reduces sensor storage needs

Support Blockchain

IoT Blockchain

Allows regular peers to discard old blocks when storage space is low
Blocks are *gossiped* over ad hoc network

Heterogeneous, opportunistic networking
CRDTs for strong semantics in partitioned world

- *Conflict-Free Replicated Datatype*
- Updates must be associative, commutative, idempotent
- Replicas can be updated independently and concurrently
- Basic CRDTs form registers, counters, sets
Transactions manipulate CRDTs

CRDT State Machine

<table>
<thead>
<tr>
<th>CRDT ID</th>
<th>Operation</th>
<th>Argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>add</td>
<td>x</td>
</tr>
<tr>
<td>A</td>
<td>add</td>
<td>y</td>
</tr>
<tr>
<td>B</td>
<td>remove</td>
<td>z</td>
</tr>
</tbody>
</table>

ID: A
CRDT Type: <crdt type>
Element type: <type>
Permissions:
<OP>: <role>, <role>, ...
<OP>: <role>, <role>, ...

ID: B
CRDT Type: <crdt type>
Element type: <type>
Permissions:
<OP>: <role>, <role>, ...
<OP>: <role>, <role>, ...

ID: C
CRDT Type: <crdt type>
Element type: <type>
Permissions:
<OP>: <role>, <role>, ...
<OP>: <role>, <role>, ...
DEMONSTRATION VIDEO

Proof of concept system
CONCLUSION

Exciting possibilities for blockchains in the food supply chain

But current blockchain designs may not be compatible with some deployment scenarios in the food supply chain

Vegvisir supports partitioned operation and has low power/networking/storage requirements
LET’S REVERT TO THE BIG PICTURE
WE DISCUSSED ISSUES IN THE LAST LECTURE

Which issues would arise on a real “smart farm”? 

Would a BlockChain solve them? What new risks would it introduce? 

What is the “speed of light” for new technology adoption?
SUMMARY OF BLOCKCHAIN CONCERNS

Permissioned or Permissionless? Energy cost of permissionless block mining.
How do I know that the sensors that Vegvisir recorded were “real”?
Cost of verifying that the BlockChain hasn’t been tampered with.
National-scale “war” scenarios that cause massive rollbacks, chaos.
Accidental loss of some chunk of the chain, making verification impossible.
Smart contracts might be too smart for their own good.
MORE CONCERNS

Most popular use cases seem to center on money laundering.

Depends on some hardness assumptions: finding a nonce, factoring RSA key. Quantum computers could shake up these assumptions.

Unresolved privacy concerns: “everything is on the table.”
What Rumsfeld called the “Unknown unknowns”.

*It ain’t what you know that’ll get you. It’s what you know that just ain’t so.*

-- Attributed to Samuel Clemens (Mark Twain)
ONE OF KEN’S “TALES OF WOE”

We take client-server computing for granted… but it was nearly on one of those gravestones!

In the earliest days, Digital Equipment Corporation invented client-server with the introduction of their VaxClusters architecture. A huge advance!

The market was exponential – DEC was on track to become the largest computer company ever. *Then it suddenly imploded and was acquired!*
WHY DID EARLY CLIENT-SERVER FAIL?

The concept was absolutely right! Yet the customers were unhappy.

The early products felt like a research prototype, not professional.

The “life cycle” of a full client-server deployment had not yet been thought through, hence there were a huge number of missing tools and features.
CROSSING THE CHASM (MOORE, 2009)

Diagram showing the progression from Early Market to Mainstream Market, with stages including Innovators, Visionaries, Pragmatists, Conservatives, and Skeptics. The Chasm is the transition point between these stages.
FACTORS THAT LIMIT UPTAKE

Early enthusiasm / bleeding edge always moves on to the next better thing, so the first adopters are certain to wander away.

Conservative customers want to be “the first to be last” and wait for the mainstream uptake to occur.

If you move too quickly, you simply overextend and fall into the chasm.
HOW TO AVOID THIS TRAP?

Technologies need to have a slow R&D process with substantial engagement with real users before they can really take off.

Setting the *detailed* concerns about BlockChain to the side, the *immaturity* of the technology space is very evident.

So BlockChain faces a chasm... as does BitCoin and other coins...
A further problem is the enormous amount of dirty cash floating around the globe.

BitCoin and similar coins have been incredibly appealing for tax evasion and money laundering, illegal activities of various kinds.

Many of the customers are large-scale criminals. This “contaminates” the products. Should we bet the farm on BlockChains dominated by their uses?