Assurance of Trust: Blockchain and AI

Ashish Kundu
ACM Distinguished Speaker, ACM Distinguished Member

Keynote
Records Knowledge Conference, Sacramento
May 23, 2019
To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

Ken Thompson
Turing Award Lecture, 1984
What is trust

trust is seen as qualified reliance on received information...
Why do we need trust

Intelligence

Data  Compute
Why do we need trust

Device 1

Intelligence

Compute

Data

Communication

Intelligence

Compute

Data

Device z

Ashish Kundu - Keynote on Trust
Trends on Data

- Analogs
- 0, 1
- Bytes, words
- Arrays
- Tables, Objects
- Trees, Graphs
- Qubits
Evolution of computing

Compute
Store
Retrieve
Communicate

Trust
Compute
Store
Retrieve
Communicate
Share

5/28/19
Ashish Kundu - Keynote on Trust
Trend towards de-centralized trust
Why trust

Generation 1—Late 1980s, virus attacks on stand-alone PCs affected all businesses and drove anti-virus products.

Generation 2—Mid 1990s, attacks from the internet affected all business and drove creation of the firewall.

Generation 3—Early 2000s, exploiting vulnerabilities in applications affected most businesses and drove intrusion prevention systems (IPS) products.

Generation 4—Approx. 2010, rise of targeted, unknown, evasive, polymorphic attacks affected most businesses and drove anti-bot and sandboxing products.

Generation 5—Approx. 2017, large scale, multi-vector, mega attacks using advanced attack tools and is driving advanced threat prevention solutions.

Source - https://www.checkpoint.com/gen-v-cyber-security/
Where are we?

World's Biggest Data Breaches
Selected losses greater than 30,000 records
(updated 30 August 2020)

Table 2: Severity of Breach Patterns, Top 5 Country Targets

<table>
<thead>
<tr>
<th>Country</th>
<th>Compromised Records Per 100 People</th>
<th>Compromised Records Per 100 Internet Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>68</td>
<td>79</td>
</tr>
<tr>
<td>Greece</td>
<td>81</td>
<td>140</td>
</tr>
<tr>
<td>Netherlands</td>
<td>23</td>
<td>24</td>
</tr>
<tr>
<td>Norway</td>
<td>80</td>
<td>83</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>220</td>
<td>245</td>
</tr>
</tbody>
</table>


Industries Affected

- Healthcare: 23%
- Financial Services: 18%
- Education: 16%
- Retail: 12%
- Professional Services: 6%
- Insurance: 6%
- Government: 6%
- Restaurants/Hospitality: 9%
- Other: 2%


http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

5/28/19

Ashish Kundu - Keynote on Trust
To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

Ken Thompson
Turing Award Lecture, 1984
To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

Perhaps it is more important to trust the people and the AI/ML systems who wrote the software.
Countering Trusting Trust

Counter the “trusting trust trojan attack” using diverse double-compiling (DDC), ...

David Wheeler, 2010
Countering Trusting Trust (+ de-centralized)

Counter the “trusting trust trojan attack” using diverse double-compiling (DDC), ...

de-centralized trust among multiple compilers

Blockchain
What is a blockchain

- De-centralized Peers (untrusted)
- Consensus
- Smart contracts
- Immutable ledger for chainedhashed data items
Bitcoin & Virtual Currencies

how computers shall be compensated for their work!
Cryptocurrency Virtual/Digital Currency

• Not all bitcoin-type currency need to rely on “crypto”

• Any hard-to-compute/process, but easy to verify can act as PoW

• MIT Digital currency
  • https://dci.mit.edu/

• Ethereum Ether
  • Memory-hard
Blockchain platforms

how de-centralized trust is enabled in computing
Blockchain-based support for trust management

Consensus management enables managing trust
Each stakeholder has a smart contract that implements policies
Smart contracts verify the state of security of data and the systems
## Summary of Features of top 5 Blockchain Platforms for Enterprises

<table>
<thead>
<tr>
<th></th>
<th>Ethereum</th>
<th>Hyperledger Fabric</th>
<th>R3 Corda</th>
<th>Ripple</th>
<th>Quorum</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Industry-focus</strong></td>
<td>Cross-industry</td>
<td>Cross-industry</td>
<td>Financial Services</td>
<td>Financial Services</td>
<td>Cross-industry</td>
</tr>
<tr>
<td><strong>Governance</strong></td>
<td>Ethereum developers</td>
<td>Linux Foundation</td>
<td>R3 Consortium</td>
<td>Ripple Labs</td>
<td>Ethereum developers &amp; JP Morgan Chase</td>
</tr>
<tr>
<td><strong>Ledger type</strong></td>
<td>Permissionless</td>
<td>Permissioned</td>
<td>Permissioned</td>
<td>Permissioned</td>
<td>Permissioned</td>
</tr>
<tr>
<td><strong>Cryptocurrency</strong></td>
<td>Ether (ETH)</td>
<td>None</td>
<td>None</td>
<td>Ripple (XRP)</td>
<td>None</td>
</tr>
<tr>
<td><strong>% providers with experience</strong></td>
<td>93%</td>
<td>93%</td>
<td>60%</td>
<td>33%</td>
<td>27%</td>
</tr>
<tr>
<td><strong>% share of engagements</strong></td>
<td>52%</td>
<td>12%</td>
<td>13%</td>
<td>4%</td>
<td>10%</td>
</tr>
<tr>
<td><strong>Coin Market Cap</strong></td>
<td>$91.5 B (18%)</td>
<td>Not applicable</td>
<td>Not Applicable</td>
<td>$43.9 B (9%)</td>
<td>Not Applicable</td>
</tr>
<tr>
<td><strong>Consensus algorithm</strong></td>
<td>Proof of Work (PoW)</td>
<td>Pluggable framework</td>
<td>Pluggable framework</td>
<td>Probabilistic voting</td>
<td>Majority voting</td>
</tr>
<tr>
<td><strong>Smart contract functionality</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

1. Based on responses from 15 leading blockchain service providers
2. Based on a random sample of set of 50 enterprise blockchain engagements across multiple industries
3. Coinmarketcap.com as of Feb 20, 2018, 6:20 PM UTC

Source: HFS Research, 2018
Some of the industry applications

**Banking & Financial Markets**
Bring trust, simplicity & enhanced customer experience to financial services.

**Insurance**
Revolutionize the trust that powers insurance with an immutable foundation of transparency and shared purpose.

**Retail & Consumer Goods**
Harness blockchain to reinvent the product authenticity, operational excellence and consumer experience.

https://www.ibm.com/blockchain/industries
Ethereum

https://www.zastrin.com/courses/ethereum-primer/lessons/1-5
## Bitcoin Vulnerabilities

### Common Vulnerabilities and Exposures

<table>
<thead>
<tr>
<th>CVE</th>
<th>Announced</th>
<th>Affects</th>
<th>Severity</th>
<th>Attack is...</th>
<th>Flaw</th>
<th>Net</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-BIP protocol changes</td>
<td>n/a</td>
<td>All Bitcoin clients</td>
<td>Netsplit[1]</td>
<td>Implicit[2]</td>
<td>Various hardforks and softforks</td>
<td>100%</td>
</tr>
<tr>
<td>CVE-2010-5141</td>
<td>2010-07-28</td>
<td>wxBitcoin and bitcoind</td>
<td>Theft[4]</td>
<td>Easy</td>
<td>OP_RETURN could be used to spend any output.</td>
<td>100%</td>
</tr>
<tr>
<td>CVE-2010-5139</td>
<td>2010-08-15</td>
<td>wxBitcoin and bitcoind</td>
<td>Inflation[5]</td>
<td>Easy</td>
<td>Combined output overflow</td>
<td>100%</td>
</tr>
<tr>
<td>CVE-2010-5140</td>
<td>2010-09-29</td>
<td>wxBitcoin and bitcoind</td>
<td>DoS[3]</td>
<td>Easy</td>
<td>Never confirming transactions</td>
<td>100%</td>
</tr>
<tr>
<td>CVE-2012-1909</td>
<td>2012-03-07</td>
<td>Bitcoin protocol and all clients</td>
<td>Netsplit[1]</td>
<td>Very hard</td>
<td>Transaction overwriting</td>
<td>100%</td>
</tr>
<tr>
<td>CVE-2012-2459</td>
<td>2012-05-14</td>
<td>bitcoind and Bitcoin-Qt</td>
<td>Netsplit[1]</td>
<td>Easy</td>
<td>Block hash collision (via merkle root)</td>
<td>100%</td>
</tr>
<tr>
<td>CVE-2012-3789</td>
<td>2012-06-20</td>
<td>bitcoind and Bitcoin-Qt</td>
<td>DoS[3]</td>
<td>Easy</td>
<td>(Lack of) orphan txn resource limits</td>
<td>100%</td>
</tr>
<tr>
<td>CVE-2012-4682</td>
<td></td>
<td>bitcoind and Bitcoin-Qt</td>
<td>DoS[3]</td>
<td>Easy</td>
<td></td>
<td>100%</td>
</tr>
<tr>
<td>CVE-2012-4683</td>
<td>2012-08-23</td>
<td>bitcoind and Bitcoin-Qt</td>
<td>DoS[3]</td>
<td>Easy</td>
<td>Targeted DoS by CPU exhaustion using alerts</td>
<td>100%</td>
</tr>
</tbody>
</table>

---

https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures
Conclusions

• De-centralized trust – easy to achieve but hard to maintain

• Security risks and threat model

• Privacy and confidentiality challenges
About ACM

- ACM, the Association for Computing Machinery (www.acm.org), is the premier global community of computing professionals and students with nearly 100,000 members in more than 170 countries interacting with more than 2 million computing professionals worldwide.

- OUR MISSION: We help computing professionals to be their best and most creative. We connect them to their peers, to what the latest developments, and inspire them to advance the profession and make a positive impact on society.

- OUR VISION: We see a world where computing helps solve tomorrow’s problems – where we use our knowledge and skills to advance the computing profession and make a positive social impact throughout the world.
The Distinguished Speakers Program
is made possible by

Association for Computing Machinery

Advancing Computing as a Science & Profession

For additional information, please visit http://dsp.acm.org/
Thanks and Questions!