Information Protection, Distributed Ledgers and Block Chain

VARA Technology

INTRODUCTION

Computers are used to store and process information. The information changes with time based on inputs, i.e. the state of the system changes. The state machine problem has intrigued practitioners since the advent of information systems to store and maintain information. We have learnt it the hard way that accurate and consistent information state is not easy to replicate across large users across large networks and geographies. Furthermore we need to ensure confidentiality, integrity, availability, prevent masquerading and provide irrefutable evidence of transactions. Moreover there are regulatory responsibilities of large businesses that store and process information specially personal sensitive information. It is more often than not that systems fail not because of poor mathematics but because of poor implementation, lack of process and mostly lack of basic hygiene among the users. Consequently a system is as secure as the weakest link in the system.

THREAT MODEL

In the plain vanilla scenario we have Alice, Bob and Carol who are legitimate stakeholders of a system. Eve and Moriarty are outsiders and are often the bad guys. Alice, Bob and Carol asserts about their individual state of the system and everybody else assumes it to be true and acts upon. This leads to a compulsive trust relationship between Alice, Bob and Carol. Such an arrangement was fine when we had monolithic systems where the security policy was known to all the participants. However now we build systems which involve principals with mutually incompatible commitments with differing security policies and without a common minimum threat model.

Nonetheless it is impossible for either of the cooperating principals with potentially mutually incompatible commitments to achieve anything meaningful without the cooperation/participation of one another in the system. Our systems now need to collaborate with the enemy.

Insurance is one area where such collaboration manifests at a granular level. Sensitive information is shared across principals with very differing trust assumptions and needs for example the customer has very different needs and expectations from the system compared to the insurer and yet they must collaborate.

BLOCKCHAIN & INSURANCE

For better or worse the insurance industry is driven by regulators and their short term focus is getting rid of inefficiencies. The long term focus might as well be radical change. Institutions might not cease to exist but their roles may change for example the network layer, the data layer and the advice layer might evolve in different ways. Block chain will have real impact in the insurance industry but might not be in a way that will be very visible to the public.

The features of block chain that is synergic to the needs of the insurance industry and can address the conventional issues of trust and consistency, are as:

- **Trust –** When we are collaborating with principals with incompatible commitments and expectations the underlying technology gives maximum guarantee of who did what and when. There is irrefutable evidence that cannot be repudiated. Moreover individual state of the system can be ascertained in a verifiable manner without having to enter into compulsive trust relationships.
- **Decentralized Verification –** The nodes can verify data without the involvement of intermediaries or a central authority.
- **Immutability –** Data can never be tampered or modified without consent. This is also crucial with respect to the GDPR guidelines that came into effect in May 2018.

> **"We live in a world where systems are built using re-purposed components, by cooperating principals who have very different agendas, different beliefs about what is acceptable, what is possible and very different views about whom they trust and for what. There is no lowest common boss."**
>
> ***Living In An Impossible World Bruce Christianson.***

USE CASES

Claims settlement – Block chain will ensure that customers are satisfied with the fairness that is inherent to the technology. A smart contract can ensure that transfers are automated based on certain policies. We now live in a world where the internet senses thinks and acts through devices known as Things. Data collection from things and then using smart contracts to evaluate if devices are adhering to insurance conditions in a transparent in a tamper proof and transparent manner will reduce cost, fraud and ensure customer satisfaction. This will have implications in vehicle and home insurance. Moreover the transparency will ensure the principle of consent and right to access of the GDPR guidelines.

Customer On-boarding and Fraud Prevention – The costs associated with repeated customer on boarding can be eliminated by on boarding the customer once and then deploying the data in the block chain. Moreover smart contracts can also gather data from various sources and ascertain risk and/or fraudulent behavior in a tamper proof manner for example driving behavior from the vehicle.

Insurance for the marginalised – Micro-insurance has been threatened due to significant operating costs. Block chain can provide a tamper proof automated customer on boarding along with smart contracts to trigger various events based on environmental conditions. A tamper proof way of doing this was not possible with conventional systems. A related concept is pay per insurance or peer to peer insurance.

Efficient Underwriting – A insurance under writer evaluates the risk and exposure of potential clients. A block chain platform will bring transparency to the process yet guarantee confidentiality and integrity. Smart contracts will ensure adherence to policy at a granular level.

CONCLUSION

At VARA we view block chain as an opportunity to address the state machine problem with maximum security and integrity guarantees. We learn from old results in byzantine fault tolerance and adopt systems that are synergic to modern and growing organizational process and models. Our goal is minimum or negligible disruption for the users. We come with strong technical background as well as in-depth application specific domain knowledge to help you in your transition.