2016 IEEE 16th International Conference on Data Mining Workshops

Data Exchange Platform to fight Insurance Fraud on Blockchain

Indranil Nath[1]
[1]Vice President, Insurance Industry Solution, IBM, United Kingdom
indranil.nath@uk.ibm.com

Abstract —**This paper introduces the concept of Blockchain and its application in sharing fraud intelligence data in Insurance marketplace.**

Keywords—**Application, Adoption, Blockchain, Bitcoin, Centralized, Claims, Decentralization, Data, Digital, Exchange, Fraud, Intelligence, Insurance, Management, Processing, Standard, Technology.**

I. THE PROBLEM

The bad guys know more than the good guys. Each insurer has a narrow lens. Criminals exploit gaps in visibility. Examples…

- Same device used to create multiple policies
- Synthetic IDs used to create multiple policies, identifiable only looking at wider dataset
- Same parties involved in multiple fraudulent claims in different roles (customer, suspect, victim, witness, provider)
- Same patterns used in multiple claims across insurers by same or different people (text phrases, rings)

Each insurer also invests heavily in similar public and subscription data to inform fraud prevention and investigation. In some jurisdictions, they are pooling resources to lower cost and improve insight.

- Derivative intelligence
- Cost considerations

Therefore clearly there is value in sharing intelligence to expand the observation space, so why hasn't this happened. Insurers have tried to share intelligence in past, but face technical, legal, and commercial challenges

- Sharing PII data
- Sharing data across borders
- Unwilling to share sensitive loss information with competitors or 3rd parties
- Who manages the shared data--trust

The free-rider problem is that bigger insurers contribute more and get less than the small insurer. So could Blockchain technology help make fraud intelligence sharing viable?

The obvious advantages in creating them will include immutability, accountability and transparent compliance. Subrogation could be a good example where this sort of feature can come very handy. If a network of insurers can collaborate to develop a Blockchain network for the ecosystem, as mentioned in the problem statement, a large number of distributed processes can be housed on the network, with no single owner and full transparency.

II. INTRODUCING BLOCKCHAIN TECHNOLOGY

What is Blockchain?

Blockchain [1] is a technology for a new generation of transactional applications that establishes trust, accountability and transparency while streamlining business processes. Think of it as an operating system for interactions. It has the potential to vastly reduce the cost and complexity of getting things done. It's essential for Blockchain technology to be developed following the open source model so a critical mass of organizations will coalesce around it—and reap its full benefits [2]. Because of the open source rules, participants can trust that the technology will fulfill their needs and conform to industry standards–assuring interoperability between Blockchain applications. Also, by sharing the foundational layer, the participants can focus their individual efforts on industry-specific applications, platforms, and hardware systems to support transactions.

It's a completely novel architecture for business–a foundation for building a new generation of transactional applications that establish trust and transparency while streamlining business processes. It has the potential to vastly reduce the cost and complexity of getting things done. Essentially, it could help bring to business processes the openness and hyper efficiency we have come to expect in the Internet Era.

Transactions are grouped together into a block and the chain is multiple blocks, linked together. Blocks are numbered in ascending order, 0 is first/oldest. The number is the 'height' of the block. It only goes from newer to older block, a block only directly links to the one immediately before it. Once the block is stored, it's read-only, which is why it doesn't link to the ones after it, which would require you to update it. Block store data, in Bitcoin, it is the transaction, but it could be any digital data. Blocks are created periodically, on average, 10mins for Bitcoin, by a process called 'mining'. A block represents a set of events that have occurred over a particular time frame, usually, since the previous block. Blocks aren't identified by their height, but by their id. Block id is the 'hash' of the data in the block. Block id is

2375-9259/16 $31.00 © 2016 IEEE
DOI 10.1109/ICDMW.2016.144

a digital fingerprint of that block. A 'magic number' (2f9c88c94d) to show it is a Bitcoin block. A size number specify how much data is coming next. All are transactions. Metadata like version number of the block format, link to previous block that came immediately before it, the root of all the transaction in the block, Time stamp of when the block was created, etc. A block is identified by their id, the hash of the metadata.

Blockchains solve specific problems, which databases cannot do yet. They are fully distributed, highly fault tolerant. It does not need centralized authority, providing 3rd party trust without trust, while reducing double spending and very low transaction costs.

The Blockchain is seen as a main technological innovation of Bitcoin, since it stands as proof of all the transactions on the network. A block is the 'current' part of a Blockchain, which records some or all the recent transactions, and once completed goes into the Blockchain as permanent database. Each time a block gets completed, a new block is generated. There is a countless number of such blocks in the Blockchain. To use conventional insurance as an analogy, Blockchain is a like a full history of insurance transactions. Bitcoin transactions are entered chronologically in a Blockchain just the way insurance transactions are. Block, meanwhile, is like individuals.

How is Blockchain related to Bitcoin?

Blockchain makes the popular crypto currency, Bitcoin, possible, ensuring that 'coins' passed between parties are cash-like: unique, immutable and final. The way Bitcoin implements Blockchain makes Bitcoins an unregulated, censorship-resistant shadow currency. IBM has no interest, and does not support, unregulated currencies that operate outside regulated financial markets.

The Blockchain is seen as a main technological innovation of Bitcoin, since it stands as proof of all the transactions on the network. A block is the 'current' part of a Blockchain, which records some or all the recent transactions, and once completed goes into the Blockchain as permanent database. Each time a block gets completed, a new block is generated. There is a countless number of such blocks in the Blockchain. To use conventional insurance as an analogy, Blockchain is a like a full history of insurance transactions. Bitcoin transactions are entered chronologically in a Blockchain just the way insurance transactions are. Block, meanwhile, is like individuals.

III. WHAT DOES BLOCKCHAIN TECHNOLOGY OFFER FOR INSURERS

Blockchain-based systems could help radically improve the insurance industry. But its impact could be much broader. Insurance claims processing and settlement are areas where a customer buys a policy and the policy sets out rules under which one gets coverage. The level of expertise required for claim adjusters or the investigators, who investigate, negotiate and settle claims, varies directly with the nature of loss, under the jurisdiction whose law applies to the contract creation, interpretation and enforcement, one of principal consumer protection issues within the insurance pricing, underwriting, and claim settlement process, the rules, aka the rules-based claims processing or otherwise a voting based claims processing, mostly followed by mutual insurers (peer-to-peer). In the claim process a person insured and other parties need to send several documents, aka data, some of which may not be available in digital format. The settlements are also subject to interpretation of the rules that apply to the product and policyholder situation. This leads claim processor to apply rules and make decisions and apply before being paid out. This goes into building incentive models to enable groups to decide which claims should be paid out and which claims should not be paid out. Further, in lines of insurance where losses require onsite examination; claims adjusters or an investigator may be sent out into the public to conduct an investigation. Today growing numbers of companies specialize in offering claims investigation services for insurance companies. Such decentralization of the insurance production cycle is becoming increasingly common, creating a market place, through the lowering of the risk and cost, enabling a breaking of existing monolithic structures, where a decentralized model has become predominant. First this creates the obvious question of mutual trust between parties - the insurers and their network to be able to collaborate within the ecosystem in a transparent way to prevent any fraud. Blockchain may be able to prevent fraud because the transactions are transparent and there will be less forgeries or manipulation of policies and contract. Second, if these features could be built into the existing market infrastructure, allowing the auto-execution of coded logic embedded into smart claims.

All transactions written to Blockchain are visible to all, shared cross multiple locations and impossible to alter or delete. As the basis for establishing consensus and enabling contract between multiple insurers with intermediary will be very useful as it creates a permanent audit trail. Mutual consensus verification protocols allow a network to agree updates to the database collectively, with a certainty that the overall dataset remains correct at all times without the need for a central governing authority.

Blockchain transactions can already be "reverse engineered" to allow a pretty good guess at the transactor. Another Blockchain virtue is decentralization of customer databases and with a federated identity infrastructure that

allows individual to identify them online without having to supply personal information, e.g. driving license number to multiple insurers. Rather than being held in any number of central databases, sensitive data is encrypted and distributed and a Blockchain is used as an audit ledger to re-authenticate the user.

IV. CAN BLOCKCHAIN REDUCE FRAUD DIRECTLY?

Blockchain may be useful in reducing fraud related to the integrity of a policy or claim or vehicle (any asset). By maintaining the integrity of the asset through various owners, Blockchain will minimize counterfeiting, double booking, document or contract alterations. It has the potential in future to be used for identity management, though this concept has a number of issues that need to be worked out. However, use of the Blockchain does not mitigate the risk associated with the majority of first party and third party frauds. Fraud detection and investigation systems will still be required. This would be true whether the Blockchain were managed by an individual financial institution, group of financial institutions operating a network or utility, 3rd party processor, or even IBM itself. You would need to run something like IBM Counter Fraud Management [4] on top:

Identity and relationship resolution: Must know for each party "who is who" and "who knows whom"

- Behavioral analytics: Must monitor behavior for parties, policies, and devices across channels and lines of business
- Descriptive and Predictive Analytics: Must be able to identify clusters, anomalies, train models
- Unstructured Data Analysis
- Link Analysis
- Alert and Case Management
- Regulatory Reporting
- Loss Reporting

V. POSSIBILITIES – USE BLOCKCHAIN TECHNOLOGY TO SHARE FRAUD INTELLIGENCE AMONG INSURERS, BROKERS, AGENTS, POLICY HOLDERS, REGULATORS, SERVICE PROVIDERS, AUDITORS AND OTHERS

Storing and agreeing datasets of financial obligations and ownership forms are the basic core of Insurance claims operations. The current methods are highly complex, utilize fragmented IT and data architectures and suffer from a lack of common standards. This creates the continual need to reconcile data with massive systems and process duplication, leading to high costs and protracted time to execute tasks. Blockchain can be used to manage shared intelligence and it could be used to drive efficiency in insurance claims processing independent of fraud, thus bringing a structural change for the industry.

If the insurers are able to record transactions on the Blockchain at each point in the transactional lifecycle from seeking a quotation to binding a policy contract, the immutable life record of that policy or the policy holder can be traced. This does bring a degree of simplicity into the underwriting process and has potential to reduce fraud. Insurance claims is a distributed process that involves many parties, insured, insurer and third parties, often with insufficient transparency to the participants. By using Blockchain and insurers can create receipts at different point in the claims process, an immutable, auditable record of all claims activities, which can be revisited by all parties including the regulators. This could lead to lower transactional cost, low transaction risk and trustless computation. Insurers and service providers compete for customer business within the market, and where large aspects of underwriting, claims and billing administration are fully automated.

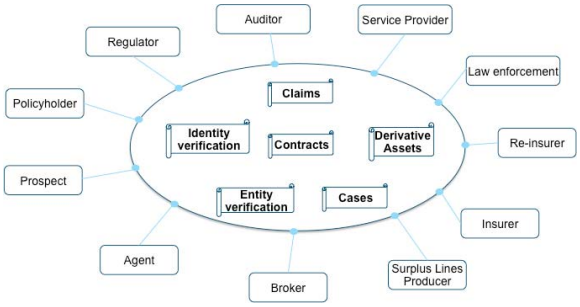

Fig 1. Several blockchainable assets across the Insurance Value Chain

These new technologies make it possible for a group of independent parties to work with universal data sources, automatically reconciling between all participants – customer, broker, insurer, co-insurer, reinsurer, all having a distributed and single view of the entire exposure data chain. In principle, any stored data record could be represented on a Blockchain, from ownership of assets to contractual obligations, credit exposures or static data. A multitude of data types can be 'hashed', encrypted and entered into the ledger to create richer datasets than today.

Example Hash: out:
2f9c88c94d860f01a17f961bf4bdfb6e0c6cd10d3fda5cc86
1e805ca1240c58553

The fingerprint (2f9c…8553) is called the SHA-256 hash of the input phrase.

{
  "size" : 43560,
  "version" : 2,
  "previousblockhash" :

"2f9c88c94d860f01a17f961bf4bdfb6e0c6cd10d3fda5cc861e805ca1240c58553",
  "merkleroot" :

"48a59f4030e0ab2debb92378f53c0a6e09548aea083f3ab25e1d94ea1155e29d",
  "time" : 1388185038,
  "difficulty" : 1180923195.25802612,
  "nonce" : 4215469401,
  "tx" : [

"d0637497fb8bc68421eb2c7b699dbab234831600e7352f0d9e6522c7cf3f6c77",

 #[... many more transactions omitted ...]

"12c5d38f6ae6aa83674cc99e4d75a1458c165b7ab84725eda41d018a09176634"
  ]
}

For example, ownership data could be entered which shows multiple levels of beneficial ownership, collapsing the hierarchies that exist in various custody arrangements. Participants store distributed records locally as their golden source of information. Many of their existing systems that are currently used to track and maintain their records of holdings and transactions could be retired. The need to interrogate centralized databases or send messages to other participants to ensure data alignment is removed.

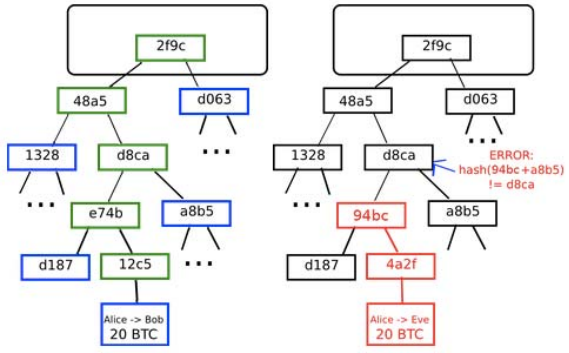

Fig 2. Datasets and Data Chain Represented on Blockchain

Some of these benefits might be achievable with existing technologies, or indeed with no actual technology at all. Adoption of Blockchain technology will be reliant upon aligning industry standards for the process, data terms, contractual documentation and so on.

Regardless of technological innovation, this standardization can improve settlement times and cut costs even using existing market practices and infrastructure. A central authority could maintain a single universal source of the truth database recording asset transactions which all participants use as their golden source: in a traditional infrastructure, a central hub for sharing insurance fraud data and intelligence, using unique position at the heart of the industry and unrivalled access to data to detect and disrupt organized fraud networks and therefore the claims management process.

However, Blockchain has some drawbacks. Blockchain is a slowest of slowest instance that need to participate together. Every participant in the network saves every block – the data is not shared to divide the data into manageable chunks, which means every node has to store the entire database and then deal with every changes. Hence it needs transaction oriented computer architecture. There is a need for very high standards set for security, robustness and performance (custom computing) of Blockchain used for major industrial purpose.

Further, Industry alignment will be required on certain design points, example, whether systems are completely open, or use permissioned-base access requirements, principles for suitability in interacting with the ledger, and the interoperability between networks. Another critical requirement for Insurers to protect personable identifiable information data is Anonymity. The ability to reveal selective information to counterparties, insurers, brokers for instance, makes it extremely difficult to prevent errors that result in major data breaches.

VI. CONCLUSION

Adopting a common Blockchain could create a step-change in claims handling being more efficient and streamlined, resulting in an improved customer experience. Such an approach could also help to reduce further, if not entirely prevent, fraud if identity management was also enforced on the Blockchain – meaning that criminals could no longer crash for cash, or exploit the current challenges of sharing data unless their methods for obscuring identities became significantly more sophisticated even though many might be sceptical that anyone will let a decentralised authority manage identities, Fraught with risk. A common claims-handling platform would still make it possible for individual insurers to compete for customers, offering a range of products and prices by virtue of the smart contracts they set up. Moreover, a Blockchain could allow the industry as a whole to streamline its processing and offer a better user experience for customers who have to make a claim. Simultaneously, storing claims and customer information on a Blockchain would cut down fraudulent activity – it would certainly make it much harder for criminals to

attempt to claim more than once, if not mask their identities. Indeed, in many respects, with projects like the IFB now long-established, the general insurance industry faces a smaller cultural and organisational hill to climb than does banking and other sectors.

Any journey towards claims and/or fraud management systems based on Blockchain technology will be a step-by-step adoption rather than big bang reorganization. The system is simply too big, complex and important. This means individual use cases for the technology need to be identified and solutions developed. Initially, these use cases need to be standalone – that is, they can be adopted within or alongside today's architecture without being dependent on a critical mass of assets already being on Blockchains. Working on a concrete proof of concept or uses cases as below will be the starting point.

1: New Blockchain to share data between participants to counter fraud: The Process of a business verifies the identity of its customers. Insurers to ensure their proposed agents perform KYC, brokers or intermediaries are compliant against anti money laundering, anti-bribery, terrorist financing including the customer's integer, prevent ID thefts and fraud.

2: New Blockchain to store and trace identities for fraud prevention: Provide an inter-insurer Blockchain to support cross-border 'network linkage' analysis, also called social network analysis, has proven particularly beneficial in the fight against insurance fraud. Identity ledgers that store and trace identities of people or businesses can help reduce cost of verification and reduce fraud and identity breach costs over time

3: New Blockchain to store risk intelligence to reduce fraud: Risk ledgers that store and trace information about the risk being insured (e.g. property titles, land titles, precious gem fingerprints, high value asset fingerprints) can help reduce cost of verification and reduce fraud costs over time

4: New Blockchain to store history of supply chain: Block verify labels products and stores the history and supply chain in the Blockchain [6], allowing users to check for counterfeit products, diverted or stolen goods, or fraudulent transaction.

Other possible relevant elements that can be housed in the Blockchain are Digital Rights Management (DocuSign), Proof of Authenticity to counter fraud.

BIBLIOGRAPHY

[1] www.blockchain.com

[2] Distributed Ledger Technology: beyond Blockchain, a report by the UK Government Chief Scientific Advisor, 2016

[3] IBM Counter Fraud Management, www-03.ibm.com/security/counter-fraud/solution/

[4] Blockchain in Insurance – opporutnity or threat? McKinsey & Company, July 2016.