2022 Focus December Conference
December 1, 2022
New York, New York

Blocking Fraud with Blockchain

Panel: Jeanine D. Clark, Esquire, Margolis Edelstein,
Stephanie Glickauf, Esquire, Goodman McGuffey, LLP
Patrick Schmid – The Institutes
Susan Jakiela – The Institutes

I. What is Blockchain

What it is.

Blockchain is a different type database. Historically data has been maintained locally and discreetly. Banks and financial institutions maintained paper ledgers; think of that old passbook savings account. Businesses maintain their own paper files. More recently, even electronic records were maintained on-site. Businesses may utilize cloud solutions and proprietary yet isolated software systems. Financial transactions took place on a local basis, or involving a finite number of parties having access to data. As a result, data and information could either be manipulated, or even under the best of circumstances, becomes the subject of a dispute. The fundamental concept of Blockchain is that it is a distributed ledger system with open access, theoretically to all. By distributed, we mean that identical copies of each transaction exist throughout the system nearly on numerable servers. The distributed nature of the transactions makes it much more difficult to alter a transaction or change information. Depending upon the Blockchain system, a specified number of copies of the transaction would have to conform to the entry in order to validate it. This number is always in excess of 50%. For example, if someone wanted to change a transaction on a Blockchain system in order to either double spend a particular form of coin or clawback payment, they would need to have access to the majority of the computing power in that Blockchain to duplicate that change. Otherwise, the change would be easily discovered and would not be verified by the other copies of the chain existing elsewhere. The attempt to change the transaction would fail.

The system is generally an open or permission-less system. This means that anyone with the appropriate computing power can participate in the creation and modification of the chain. Those seeking to create the next blocks in the chain do so by a competitive process which generally requires substantial computing power. However, they are rewarded by payment either in the

form of newly "minted" native coin, or transaction is for processing the transactions of others. Blockchain utilizes cryptography to secure data.

How it works.

A transaction or information is stored on the blockchain. Owners and operators of computing power on the blockchain are known as miners. Individuals or entities seeking to have their transactions processed or information posted rely upon the miners to do so. In some cases, the miners are paid a transaction fee, and in other cases if the party is willing to wait, no transaction fee may be charged. The "block" is only permitted to be a certain size (of data) and a new block may only be created within a specified time interval. Thus, a backlog may occur and individuals seeking priority may be willing to pay transaction fees. Each time a new block is created, the operator who created the block is paid, usually in new native coin. The block is published and in order to become the next validated block in the chain, must be verified by the specified percentage of the computers on the chain. This is the part that makes it difficult to alter a transaction. Since only so many new blocks can be created within a given time, there is competition to be the one to mine the next block. Thus, the system has a competitive "tournament" which requires significant computing power to select the miner of the next block.

Many people are familiar with Bitcoin and Etherium, even Dogecoin as methods of payment. These are all blockchain based currency systems. Blockchain can be used for more than payments, however. More on that later. Blockchain systems such as Bitcoin are considered permission less as theoretically anyone with the proper computing system and power can participate in mining tournaments and submit transactions. These systems are also considered pseudo-anonymous as one's identity is not immediately apparently. Individuals need not transact as themselves.

Smart Contracts?

Smart contracts are self-executing programs. They are typically not contracts in the traditional sense. A transaction would be programmed to automatically release a payment from party A to party B upon the happening of a certain event. For example, the parties may agree that payment would be released on a specified date, upon the happening of a specific objectively verifiable event such as a football score or a weather event. The complexity of the "contract" or code impacts the transaction fee or fuel needed to process or execute the contract. An example I like to use is the EZPass. The EZPass is, of course not a smart contract or even (yet) a blockchain system. However, like a smart contract, it does not care if you meant to go through the toll, if you liked the toll, or if you fell the rate for the toll was fair. Once you have passed through the toll, your account will be debited, whether you like it or not. Once the condition precedent occurs, payment is made.

II. Permissioned Systems

How is a Permissioned System Different?

Permissioned or enterprise systems are no anonymous. Rather than an open system open to the world, a permissioned system serves either a single organization or a consortia/multiple organizations who have agreed to participate and share data. These systems are more about sharing and tracking information and traditional business applications than "crypto" currency.

How Permissioned Systems are Being Used Today.

Permissioned or enterprise systems are in use today in a variety of applications. Travel claims and travel insurance issues that are dependent on timing delays and weather are well suited to blockchain solutions. A number of insurers and in particular re-insurers are looking at how the secure exchange of information can improve underwriting and claims.
Blockchain can be used to efficiently track payments, even when the method of payment is more traditional.

III. Potential Fraud Fighting Use Cases for Blockchain.

Simple PD Claims in Auto are likely to mesh well with use of blockchain systems and handling. Repair Estimates in auto and real property losses are also likely to eventually incorporate blockchain into claim evaluation and resolution.

Weather Damage and weather CAT claims may be streamlined through use of this technology. Other use cases include health insurance, life insurance and travel insurance. Blockchain is likely to play a role not only at the claim and investigation state but in underwriting.

V. Why we Still Need Human Professionals.

Blockchain is an interesting technology that can improve the exchange of and security of information, in certain applications. It is not a one size fits all solution, however. Not All Issues are Yes/No, Cut and Dry. There are many cases where other technology or good old fashioned human evaluation are a better fit.

Human insight and evaluation is needed particularly in complex claims and litigation. The human mind is still best at evaluating gray areas and how other human minds (such as juries) will react.

Large loss cases require multi level complex handling and evaluation. There must always be human oversight at appropriate levels even in small value claims and a way for a policy holder to request a review beyond any automated evaluation. Particularly in the insurance fraud arena, claim professionals must be cognizant of avoiding extra contractual claims and the specter of automation.

New tech tools should assist in the investigative and claims handling process, not supplant the process. The informed litigator and claim professional will be most effective when skilled in the traditional tools and when aware of emerging technologies to assist in the evaluation, investigation and litigation process.