kbr

KAUFMAN BORGEEST & RYAN LLP

Bitcoin/Blockchain & Professional Liability Insurance

October 3, 2017

Scott A. Schechter, Esq.
Kaufman Borgeest & Ryan LLP
George Kimmel, Esq.

PLUS

PROFESSIONAL LIABILITY

bitcoin

Introduction

- In this presentation we will introduce you to the intertwined concept of bitcoin and Blockchain. We will give you some of the background for this interesting development which draws from the fields of cryptography, computer science, information technology and finance.
- We will explain why it is attracting so much interest from Venture Capitalists, financial regulators, investors, payments and settlements experts, futurists, libertarians and other assorted people and speculate why it has potential impact on markets, our insureds and our customers.
- We will also discuss the insurance marketplace as respects bitcoin and Blockchain, including the types of insurance available to cover insureds in the space, the types of claims that have been made to date, and potential coverage issues that might arise in connection with claims.

What is Virtual Currency?

- Bitcoin and blockchain generically refer to 3 different interrelated, interconnected things:
  - Blockchain Platform: architecture which overlays the internet
  - Blockchain Protocol: operating system or instructions for how to execute transactions
  - Bitcoin: the cryptographic key denoting an individual user on the platform ("user x"), the cryptographic instrument of value to be transmitted over the system ("the Bitcoin") and the instructions for routing that key and that instrument to another cryptographic key holder on the system ("user y") such that upon contacting the target key holder the instructions will say "transfer me from the custody of user x to user y."
  - One bitcoin trades for approximately $666 as of July 2016.
  - When a person wants to participate in bitcoin/blockchain, all they need to do is download the software off of the *bitcoin.org* website and click on the "get started with bitcoin" tab.

What is Virtual Currency?

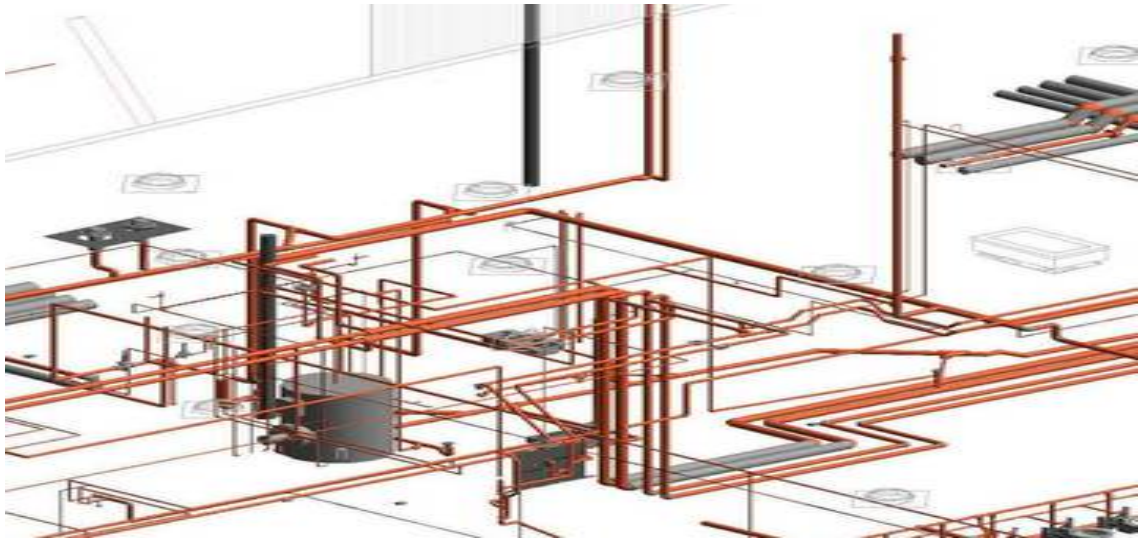
- Once the bitcoin software is installed on a person's computer, that person can obtain a bitwallet and a personal key necessary to obtain and trade bitcoin.

- Bitcoin can be obtained by:
    - Mining it
    - Exchanging other currency for bitcoin either through an exchange or through a Bitcoin ATM
    - Trading goods and services for bitcoin

- Anyone with the bitcoin software can be a miner. Mining is part of the process of spending a bitcoin and will be described in the hypothetical on page 8.

When and Why did it Come About?

- The current process is cumbersome, costly & attendant to fraud.
- “Payments and Settlements” is the underlying system for settling all monetary transactions all over the world.
- It is like the world’s financial plumbing system.



When and Why did it Come About?

- With a swipe of a credit card, one initiates a whole series of actions, by a whole series of people, to verify identity and ability to pay.
- This system costs significant amounts of money (3 percentage points of the transaction for credit cards) and takes days to process. Also, all parties must constantly look out for fraud.
- Between large financial institutions, when settling transfers of stocks, bonds or swaps, there is a similarly cumbersome settlement process that takes typically 3 days, referred to as “T+3.”
- On the Blockchain, such transactions can be settled in 10 minutes without worrying about fraud.
  - Is it hack proof?

How does it Work? (Hypothetical)

- Rob owes George $10.
- Rob obtains his bitcoin from a bitcoin ATM and stores it in his Bitwallet.
- Rob then goes onto his smartphone and uses his Bitwallet app to arrange a transfer of $10 worth of bitcoin to George's bitcoin ID. He hits "enter."
- The transfer message emanates over the bitcoin network to all the users who have downloaded the bitcoin software onto their computers.
- Those users who have chosen to become miners begin to work on validating the transfer (in an analogous way that Visa or Paypal would have to validate the transaction, had Rob chosen that method of payment).
- Miners validate a payment by solving an SHA 256 cryptographic hash function generated by the transfer request.

Processing & Validation

- The miner who calculates the minimum value to the cryptographic hash function validates the transaction and the solution is broadcast over the network. Any other miner will be locked out from processing the transaction because their solution will be equal to or greater than the first miner's minimum value. This method of validating a transaction is called the "proof of work method." The successful miner will be rewarded by being paid bitcoin from the bitcoin Treasury within the software. When Satoshi Nakamoto created the software, he/she created a Treasury of 21 million bitcoin to be released every 10 minutes to successful miners until the year 2140.
- After the transaction is validated, it is then attached as a Block of data with that same minimum value onto the last Block of data that was validated 10 minutes previously onto the chain of Blocks that began in 2009. That chain is called the Blockchain. Each value of each block is then added together to create one unique number.

Who is using it?

Early Adopters

- Cross Border Transactions
  - For the last 30 years, transactions have been settled using the electronic settlement system know as: SWIFT
    - Society for Worldwide Interbank Telecommunication
      - $81M stolen from Bangladesh Central Bank
      - JP Morgan clamping down on who can access SWIFT
  - The largest financial centers are seeking to replace SWIFT with the Blockchain.
- Tri-Lateral Repo Market
  - The Tri-Lateral Repo Market provides overnight liquidity to the largest financial institutions on earth. The DTCC, which is the settlement agent for the repo market, is seeking to run the market on the Blockchain.

Who is Using it?

- JP Morgan already has a private Blockchain up and running for select clients.
- Mizuho Bank is using the Blockchain for cross-border transactions.
- R3CEV has signed up 40 major international financial institutions.
- B of A has over 55 patents on Blockchain technology at this time.
- VC money from Silicon Valley and Silicon Alley is pouring into Blockchain startups everyday.

PLUS

Hack proof Results?

- If anyone tries to hack the Blockchain, tamper with a Block, or insert a new unauthorized Block, that unique number would theoretically be changed. But the system would not recognize, but would rather reject, any new number, thus making it impossible to tamper with the block. The Blockchain is rendered tamper-proof.
- In this way, the Blockchain then becomes a permanent ledger of every bitcoin transaction ever recorded.

The First Bitcoin Scandal/Failure

Mt. Gox

- The first bitcoin exchange was set up in Tokyo by an American. Mt. Gox started out as a website for users of the fantasy game *Magic: The Gathering* to trade game cards online.
- By 2013 Mt. Gox was handling 70% of all bitcoin transactions.
- In February 2014, Mt. Gox suspended trading, closed its website and exchange, and filed for a form of "bankruptcy" under Japanese law called *minji saisei*, or civil rehabilitation to allow courts to seek a buyer. By April 2014, the company was in liquidation. A scandal arose when 850,000 bitcoin belonging to customers were not accounted for. While 200,000 were recovered, the rest were likely stolen.

Does an Anonymous Marketplace Incentivize Illegal Conduct: Silk Road

- Silk Road was founded by Ross William Ullbright.
  - Was the first modern darknet market.
  - The darknet is a network that overlays the web that can only be accessed by specific software, configurations or access such as the TOR (Onion) protocol.
  - It was launched in 2011 and only accepted payment in bitcoin.
  - Silk Road primarily sold illicit drugs.
  - After a lot of searching, the FBI found Ross William Ullbright (aka Dread Pirate Roberts) sitting at a library in San Francisco and arrested him. Silk Road was unceremoniously shut down.
  - Dread Pirate Roberts has been sentenced to life in prison without chance of parole.

Silk Road
anonymous marketplace

DAO: the HACK

- As we will explain later, a DAO is a decentralized autonomous organization created of smart contracts on the blockchain. In June 2016, one company, Slock.IT decided to create a DAO that would be a self operating investment fund using not bitcoin, but the altcoin Ethereum.
- Many in the blockchain Community, including many lawyers warned that this structure was premature and had too many technological and legal bugs, but Slock.It launched DOA anyway on June 12, 2016.
- A “hacker” investor, to show the structure’s vulnerability, employed a “recursive call bug” to withdraw funds out of the structure into a child clone of the structure, effectively draining 3.6 million Ethereum coins worth $55 million of the $150 million of the notional value of the Fund.
- The Fund shut down immediately. The clone fund was frozen. No investors lost any money. But the point was made. DOA was not ready for launch.

How Can the Blockchain be Leveraged?

- Until recently, bitcoin has been transmitted over the Blockchain primarily as a currency.
- Other uses of bitcoin can leverage the Blockchain by utilizing the memo section encoded on the bitcoin that allows users to write messages which can then be transferred between parties.
- A single Bitcoin may be divided into multiple fractions, the smallest fraction of which denotes a satoshi

  - A satoshi is one hundred millionth of a Bitcoin (0.00000001 BTC).
- Notwithstanding that a satoshi is a small fraction of a Bitcoin, it has the same memo field as a full Bitcoin.
- This memo field can be used to document or program the satoshi with information or instructions in a myriad of ways at a minimal transaction cost. This leads us to the topic of smart contracts.

Smart Contracts

- One way that a satoshi may be documented could be to accept a short simplified self-executing contract between two parties. (Think of a digital yes/no type contract, almost a computer program of sorts.)
- Thus, the blockchain may be utilized to execute a contract as follows: I inscribe on my satoshi that I will pay my grandchild all of my bitcoins on her 18th birthday or my date of death. I add a program that searches registries to check to see if I am still alive and to keep account of my granddaughter's age.
- On the date that the satoshi discovers either that I have died or that my granddaughter has reached her 18th birthday, the contract self-executes.
- My satoshi would then be transferred to my granddaughter, recorded on the blockchain and placed in her Bitwallet.
- Such contracts are referred to as smart contracts. A series of smart contracts could be strung together to create a more complex agreement between the parties.

The Wave of The Future

- There are over 700 cryptocurrencies in existence at this time and quite a number of alternate blockchains (called Altchains) competing with bitcoin as a currency. Whether bitcoin or its competitors prevail as a viable currency of the future is not as important a question right now as how the blockchain architecture will be implemented in the future.

- Adam Draper of Boost VC, whose grandfather gave the VC money that started Hewlett Packard, and who has incubated more blockchain startups than anybody in Silicon Valley, states that 2016 was the year of experimentation with blockchain and 2017 was the year of implementation.

- In her 2014 book, *BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY,* Melanie Swan makes the case that the blockchain is the financial underpinning the internet has been waiting for since the world wide web protocol was invented in 1989 by Tim Berners-Lee (Hypertext Transfer Protocol, “HTTP” and “HTML”).

Where Do We Go From Here?

- From replacing the payments and settlements system, to revolutionizing international settlements and payments, to modernizing the tri-lateral repo market, to smart contracts, where do we go from here?
- Overstock.com has issued stocks and bonds via the blockchain and the SEC has allowed same to be registered.
- Applications in the insurance industry: nothing is stopping the market from issuing insurance policies on the blockchain, which millennials will be able to blithely download off of their smart devices of the future, whatever they may be.
  - A technology that might replace the insurance contract?
- Blockchain is a prime candidate for regulating the Internet of Things (IoT) with self-executing smart contracts of the future.

Underwriting/Brokerage Considerations

- Is there a vibrant market for insurance coverage for bitcoin and blockchain transactions?
  - Will there be a demand for it in a soft market environment?
- Who are the potential purchasers of the coverage?
  - Banks/Investment Banks
  - Broker/Dealers
  - Alternate asset managers
  - Insurance companies
- A business that keep or maintains bitcoin (or other virtual currencies) should consider whether its current program will cover bitcoin or blockchain assets and the attendant first and third-party losses.
- Existing coverage may have explicit bitcoin exclusions; or include electronic data or new digital currency exclusions.

Underwriting/Brokerage Considerations (Cont'd)

- Stand alone policy?
- Add on to existing policy?
  - Cyber
  - D&O
  - FI (PE/Investment Adviser, etc.)
  - Insurance Company E&O
  - Fidelity/Crime(First Party Coverage)
- Crime Insurance for virtual currency
  - ISO form – door is closed to claims that a standard money and security policy covers virtual currency by adding an exclusion to its crime forms.
  - ISO has created optional endorsement: "Include Virtual Currency as Money"
- Hot topic with crime underwriters: fraudulent impersonation coverage (aka social engineering coverage). A fraudulent impersonation coverage endorsement would provide coverage for the loss of money, securities, or other property due to an employee having, in good faith, complied with a transfer or delivery instruction that an imposter fraudulently transmitted.

Underwriting/Brokerage Considerations (Cont'd)

- What are the Regulatory and price risks?
- How much coverage does the policyholder need?
- Will the new administration have any impact on bitcoin/blockchain (one way or the other); and how might this impact the insurance market in this space?
- Does it pay to be a pioneer (as a broker or underwriter) in this space?
- From an insurance perspective, is this going to be another Y2K, or does the insurance industry think that there will be significant claims that might arise as use and trading of virtual currencies increases?

Claim Considerations

- Who are the likely plaintiffs/claimants?
- What will the claims look like?
  - Identity Theft: Law360 recently reported a situation where a man is accused of identity theft and fraud after he admitted stealing from individuals who use bitcoin (man is a skilled coder with extensive knowledge of the dark web, who developed software that allowed him to steal bitcoin).
    - Possible first party claim by those whose bitcoin were stolen?
  - Bitcoin Cash: a new version of bitcoin hit the market on August 1st, Bitcoin Cash, and on its second day of trading it tripled in price and its market cap is now third biggest of all digital currencies. The new currency arrived via a so-called "fork" in which a faction of people who run the software that controls the bitcoin started a breakaway version.
    - The creation of the "fork" in bitcoin's blockchain – the software ledger that permanently records all transactions – by a minority of bitcoin operators followed a period of infighting in the bitcoin community.

Claim Considerations (Cont'd)

- There are now two bitcoin blockchains, each with its own currency.
- Upon creation of the new chain, the breakaway faction chose to award Bitcoin Cash on a one-for-one ratio to every owner of bitcoin – so if a person owns five bitcoins, they are entitled to five units of Bitcoin Cash.
- The scheme has been complicated by the decision of the biggest bitcoin exchange, Coinbase, not to support Bitcoin Cash. This essentially means that the millions of people who maintain a wallet on Coinbase did not receive the new "Cash" and, as of now, there is no way for them to do so.
- Coinbase has stated that the company is not taking customers Bitcoin Cash for themselves, but its decision to withhold the new currency looks like it will lead to a lawsuit.
- There is apparently an activist group, which claims that Coinbase's decision is akin to a brokerage withholding new shares from its investors and has warned that it will file a class action lawsuit if the company does not release the Bitcoin Cash.
- An attorney has also told *Fortune* magazine that she intends to file a lawsuit with allegations of negligence, breach of fiduciary duty and unjust enrichment.

Claim Considerations (Cont'd)

- Problems with Initial Coin Offerings ("ICO"): There has been significant investments into ICO's – more than $100 billion. So far, the ICO's have been considered to be very positive but there are some recent challenges. Bot unlike what transpired during the dot-com IPO boom of the late 1990's, the ICO market is apparently seeing potential phantom companies that are trying to leverage the popularity of virtual currencies to make a quick buck without a real business plan. Industry publications warn of an impending ICO that goes bad, resulting in thousands of investors collectively losing millions of dollars.
  - If this happens, there will inevitably be a call for regulation of virtual currencies both domestically and internationally.
  - Pundits say that they foresee possible class-action lawsuits, not unlike those that followed the dot-com bust.
  - Recently, ICO's have strictly forbidden citizens of some countries (mainly the US) from participating in their offerings for fear of lawsuits.

Claim Considerations (Cont'd)

Insurance Coverage Disputes

- *Bitpay, Inc. v. Massachusetts Bay Insurance Company*
  - Lawsuit related to a hack at the insured company that resulted in an unauthorized transfer of bitcoin valued at more than $1.8 million.
  - Bitpay's CFO received an email from a hacker claiming to be a reporter from a digital currency publication.
  - By following instructions provided in the hacker's fake email (which appeared to be from the reporter), Bitpay's CFO ended up providing his email credentials to the hacker.
  - After having the CFO's email credentials, the hacker gained access to the CFO's computer and eventually learned how transfers were made within the company.
  - Bitcoins were transferred when Bitpay's CEO received emails that appeared to be from the CEO requesting bitcoins from customers' digital wallets.
  - On one transfer the CEO copies Bitpay's customer on the email confirming the purchase of additional bitcoins and the customer sent an email back that they did not purchase the bitcoins.

Claim Considerations (Cont'd)

- After investigating the claim, the Commercial Crime insurer denied coverage.
- The insurer cited to an Insuring Agreement, which required that the loss of use of money be the direct result of the use of any computer to fraudulently cause a transfer of that property from inside the premises to a person or place outside the premises. According to the insurer, "direct" means without any intervening step, *i.e.* without any intruding or diverting factor. According to the insurer, the Computer Fraud Insuring Agreement is only triggered by situations where an unauthorized user hacks or gains unauthorized access into your computer system and uses that access to fraudulently cause a transfer of Money to an outside person or place. The insurer took the position that the facts presented did not support a direct loss since there was not a hacking or unauthorized entry into Bitpay's computer system fraudulently causing a transfer of Money. Instead the Computer System of the reporter from the digital currency publication was compromised resulting in fictitious emails being received by Bitpay. The Policy does not afford coverage for indirect losses caused by hacking into the computer system of someone other than the insured. The insurer also noted the important distinction between fraudulently causing a transfer, as the Policy requires, and causing a fraudulent transfer, which is what occurred upon the CEO's approval of the bitcoin transactions after receiving the fictitious emails. The Loss incurred by Bitpay was not a direct loss.

Claim Considerations (Cont'd)

- The insured contends that its losses were not indirect; and further that as per its agreement with the insurer, its bitcoin holdings were subject to special consideration given the particulars of the digital currency.
- The Insured argues that the insurer agreed to add bitcoin to the Policy definition of 'money' thereby insuring Bitpay against loss of bitcoin; and unlike traditional money, bitcoin does not exist in physical form in any location or premises, and it cannot be transferred from or to any physical location." Therefore, any agreement to insure bitcoin that purportedly requires bitcoin to be on Bitpay's premises is illusory.