THE POWER OF BEING UNDERSTOOD

AUDIT I TAX I CONSULTING

RSM

BLOCKCHAIN: PREPARING FOR DISRUPTION

What is Blockchain and how will it impact you in the coming years

ACAMS Chicago Chapter

May 15, 2018

RSM

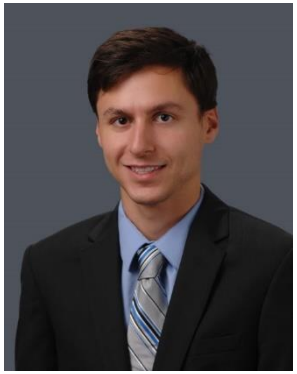
Introduction

Jay Schulman
Principal

- Lead RSM's Blockchain and Cryptocurrency Practice.
- Engaged with clients who are building new cryptocurrencies, helping companies address how to accept cryptocurrencies, how blockchain is going to disrupt a company

RSM

Presenters



Nathan Goldsmith

Associate, Risk Advisory Services

- Performs security reviews of client's blockchain projects
- Audits the largest cryptocurrency trading desks in the world
- Shares knowledge about bitcoin and blockchain tech

Nick Mustafa

Director, Risk Advisory Services

Great Lakes AML and Regulatory Compliance Leader

RSM

BITCOIN VS BLOCKCHAIN

What are we even talking about?

RSM

So what exactly is a Blockchain anyway?

A blockchain is a ledger where transactions are recorded and confirmed anonymously. It's a record of events that is shared between many parties. More importantly, once information is entered, it cannot be altered*.

RSM

Bitcoin was merely one of the first applications

Bitcoin: A Peer-to-Peer Electronic Cash System

- "Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments."
  - "Fraud is accepted as unavoidable"
  - "Merchants must be wary of their customers, hassling them for more information than they would otherwise need"
  - "These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party"
- "Chain of blocks"
- "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"
- https://bitcoin.org/bitcoin.pdf

RSM

White Paper

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the

RSM

What about other cryptocurrencies?

There are 1540 currencies tracked at https://coinmarketcap.com

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$117,348,082,175	$6,914.41	$4,368,600,000	16,971,525 BTC	1.04%	
2	Ethereum	$41,662,719,737	$421.87	$1,340,080,000	98,756,545 ETH	3.30%	
3	Ripple	$19,414,768,981	$0.496611	$178,593,000	39,094,520,623 XRP *	1.07%	
4	Bitcoin Cash	$11,155,865,061	$653.62	$246,677,000	17,067,763 BCH	0.35%	
5	Litecoin	$6,432,016,084	$114.78	$199,671,000	56,036,313 LTC	0.21%	

RSM

What is Bitcoin (and other Cryptocurrencies)

- Coins are bought and sold like stocks and commodities, exchanged for other coins, issued to raise money, and used to purchase goods
- **But….**
  - They aren't (yet) regulated
  - The IRS says they're property (like a house)
  - The SEC says if it smells like a duck (Howey Test), it's probably regulated

RSM

Blockchain

- One of the key underlying technologies behind Bitcoin (and other cryptocurrencies) is the blockchain
- A blockchain is simply a database with signatures
- Standing alone it is no more valuable than a SQL database
- There is an enormous amount of hype around the word “blockchain”

RSM

How blockchain works

- Miners compete to find the next block
- Users broadcast transactions to the network; these transactions are unconfirmed until put into a block
- Once a transaction has made it into a block it is “confirmed”
- As more blocks are placed on top, the transaction becomes solidified
- ~7 conformations = 99.9999% permanent
- Miners are financially incentivized to behave honestly

RSM

Cryptocurrency

Cryptocurrencies are good for:

- Transmitting value (Bitcoin)
- Storing information inalterably
- Smart contracts (Ethereum)

RSM

How does this apply to you?

- Storing value
  - Using “coins” to facilitate money transfers
  - Bitcoin is borderless
- Computing transactions
  - “smart contracts” – if this, then that
  - Funds are help in a contract; when the terms of the contract are met the coins are released.
- Storing Information
  - information, tracking, anything where the order of the data and integrity of the data matters
  - Different from a traditional database; the past can not be altered, no change logs

RSM

Blockchain in use today

Walmart and a group of food giants are teaming up with IBM to explore how to apply blockchain technology to their food supply chains.

The coalition includes retailers and food companies such as Unilever, Nestlé and Dole. They will be aiming to use blockchains to maintain secure digital records and improve the traceability of their foodstuffs, like chicken, chocolate and bananas.

RSM

ANTI-MONEY LAUNDERING

FinCEN guidance

An “administrator” or “exchanger” of virtual currency is considered an MSB under guidance issued by FinCEN.

Important note – a “user” of virtual currency is not classified as an MSB, and therefore, not subject to AML reporting laws

RSM

BSA/AML requirements

MSBs, including virtual currency exchangers, are required to comply with the four pillars of an AML program as follows:

- Designate AML officer
- Policies, procedures and internal controls (including monitoring of agents, if applicable)
- Training
- Independent testing

RSM

OFAC implications

OFAC may add digital currency addresses to the SDN List to alert the public of specific digital currency identifiers associated with a blocked person (March 19, 2018).

A digital currency address is associated with a digital currency wallet.

RSM

OFAC implications

Digital currency includes sovereign cryptocurrency, virtual currency (non-fiat), and a digital representation of fiat currency.

RSM

Virtual currency clients

Apply a risk-based approach to onboarding and monitoring virtual currency clients:

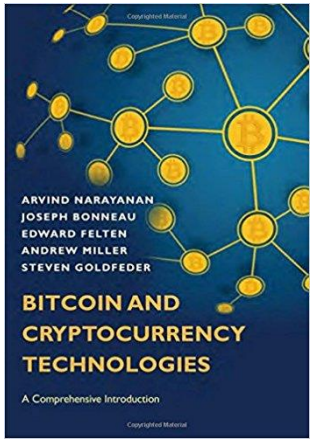
- Know Your Customer/Customer Due Diligence
- Nature and purpose
- Risk based monitoring and updating of customer information
- Expected activity
- Source of funds

It’s important to stay current on this topic, as it will effect your institution.

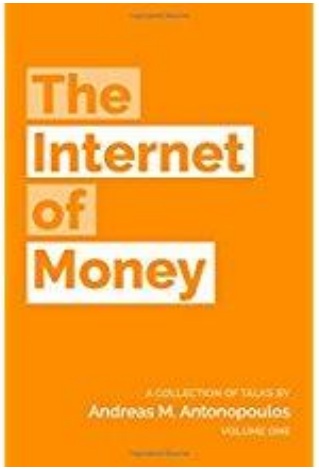
RSM

Reading Recommendations

- Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction (Princeton)
  - This is a very technical, math and computer science book



- Any Andreas Antonopoulos book
  - The Internet of Money
  - Mastering Bitcoin



RSM