BLOCKCHAIN FUNDAMENTALS

SECSIG

SecSIG provides Information Security related content to, for and by members of Mensa.

While our SIG membership is limited to members of Mensa, our content is freely available and usually published on our web site.

For any members of American or International Mensa who want to join us, come to our Facebook page or email us.

https://facebook.com/groups/secsig
info@secsig.org

WARNING

As with all of our content, we are not your financial advisor and this isn't investment advice.

You have a better chance making a profit by having a deadly herpes monkey fling shit at Sears stock than listen to our presentation.

Really.

Enjoy.

BLOCKCHAIN FUNDAMENTALS

(AT MENSA SPEED)

IT'S A CHANGE IN MINDSET

- **Data as a Public Commons**
  Data exist without ownership, application, or location.
  Data that is meant to be public should not rely on centralized custodianship in order to be made available.
- **Data is Immutable**
  Known data should be protected from corruption.
  Data that is meant to be public should maintain integrity and be resistant to attack by those who would seek to interfere.
- **Data is Direct**
  Individuals should be able to transact value without interference.
  Data conveys value. Data must be directly transactional in a secure way without facilitation or interference by another.

IT'S A CHANGE IN TECHNOLOGY

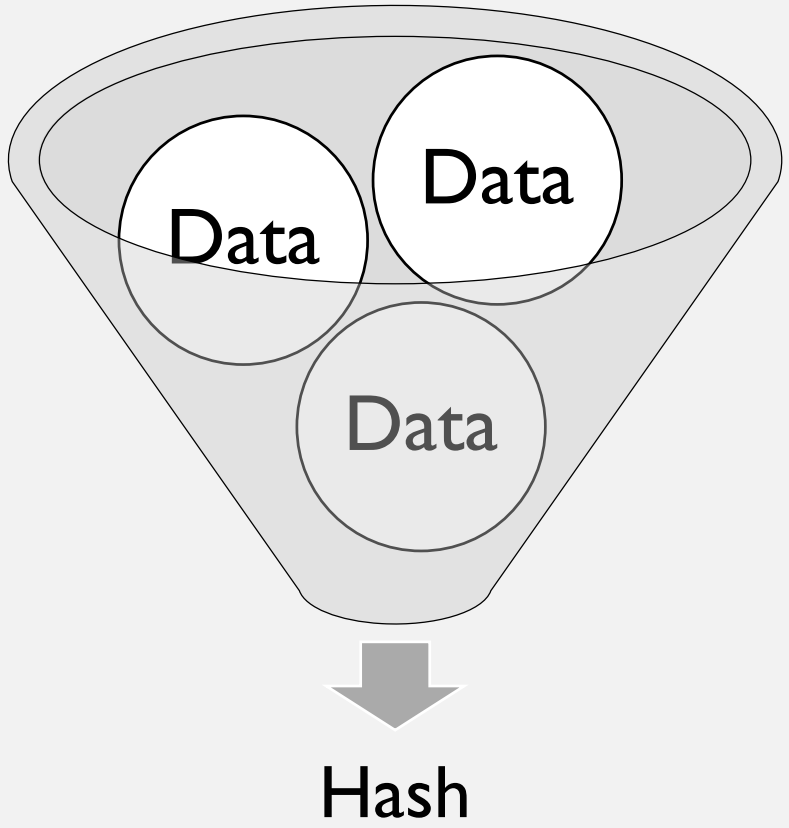
- **Distributed Ledger**
  Everyone knows what is public and has a way of maintaining consensus as new data is created.
- **Identity Assured**
  There are secure methods for identifying people and data.
- **Everyone Is Welcome**
  Anyone can fully participate, which is a core principal in everyone can validate data.
- **It's Messy**
  This is very new and is built without centralized standards.
  It takes awhile to refine and make it ready for widespread use.

HASH

A Hash Algorithm (like SHA-256) takes unlimited input and creates a fixed length output.

The output is relatively unique in that the same output from two different inputs is unlikely, but not impossible.

The value of this is that a Hash performs like a signature of the source data, but at a much smaller size.



NODE

A Node can be either a full (participating) node or a lite nodes. The primary difference is that full nodes keep a copy of the block chain and are responsible for creating and sharing new blocks.

Lite nodes must request the services of full nodes when they want to interact with the block chain.

To support the efforts of full nodes, the block chain creates and pays rewards for successfully creating new blocks to full nodes.

CREATING BLOCKS

A full node collects potential transactions from other full and lite nodes and assembles them into part of what will become a new block.

To do this, the node first takes information from the previous block, the potential new transactions and a hash of all of this information to create what it hopes will become the next block.

Depending on the algorithm (we'll get there) it then tries to gain consensus that it's block should be the next in the chain.

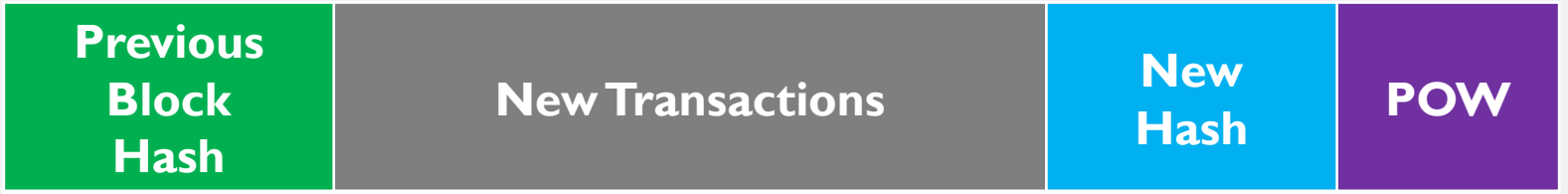
CONSENSUS

Consensus Algorithms are designed to promote the potential block of a full node into something that all of the nodes can agree upon. Conversely, they are designed to reject any information that cannot be verified.

Only information that is verifiable is adopted by full nodes as new blocks on the chain.

We will discuss Proof of Work as our sample consensus algorithm.

PROOF OF WORK



Proof of Work takes the 'New Hash' of all of the data, including the **previous block hash** and the **new transactions** along with the **new hash** as the 'seed'. This is combined with a **random value** that is used to create the **POW** hash.

The goal here is for the distributed system to create a new block every x minutes. In the case of bitcoin, it is approximately 10 minutes. But there are many nodes in a distributed system, and any node can randomly create a new block if it can solve a difficult math problem first.

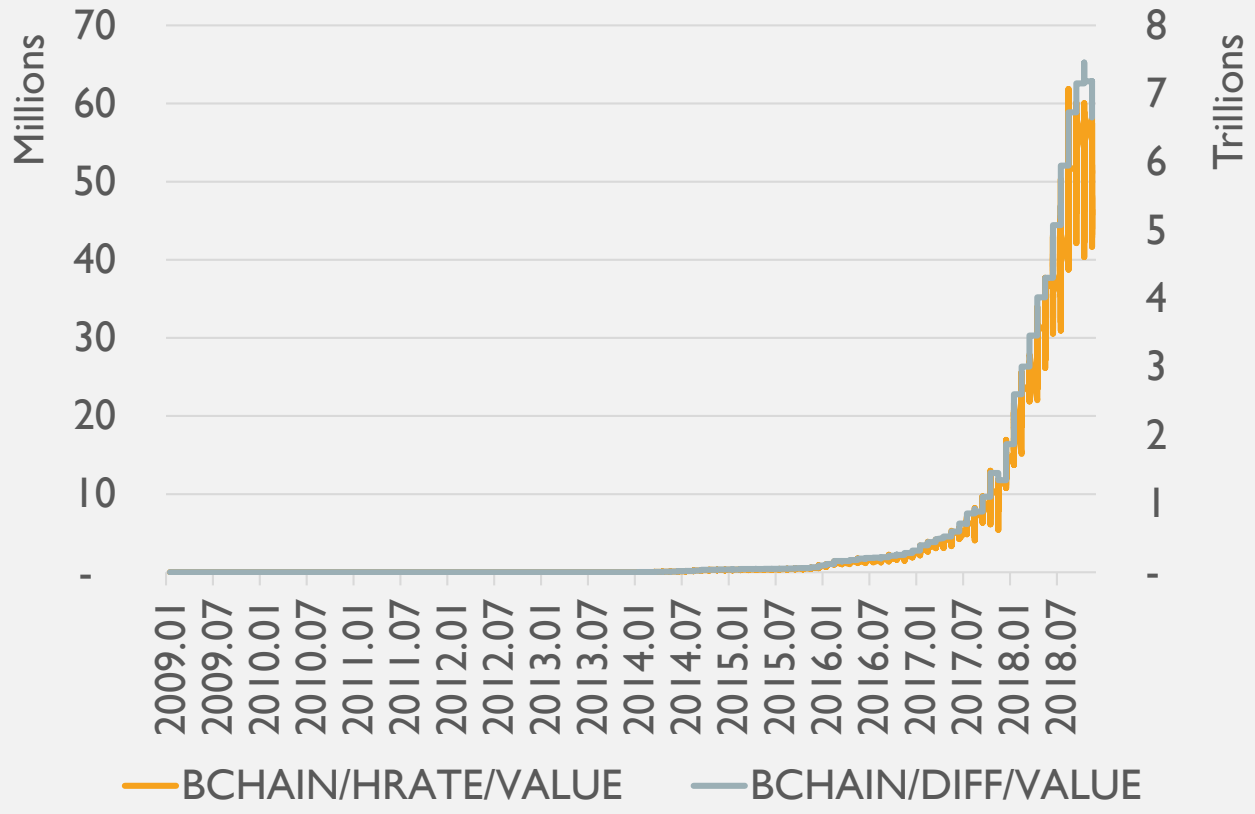
The math problem is to create the **random value** and add it to the **new hash** such that the resulting **POW** hash has a specific characteristic. Since the math function can't be forced, new **random values** have to be used until one that works is found. In the case of bitcoin, this is that the **POW** hash has leading zeros as it's value.

SecSIG

A BRIEF TANGENT INTO BITCOIN

DIFFICULTY

As global hash rate goes up, the difficulty algorithm creates a more difficult proof of work problem to be solved.



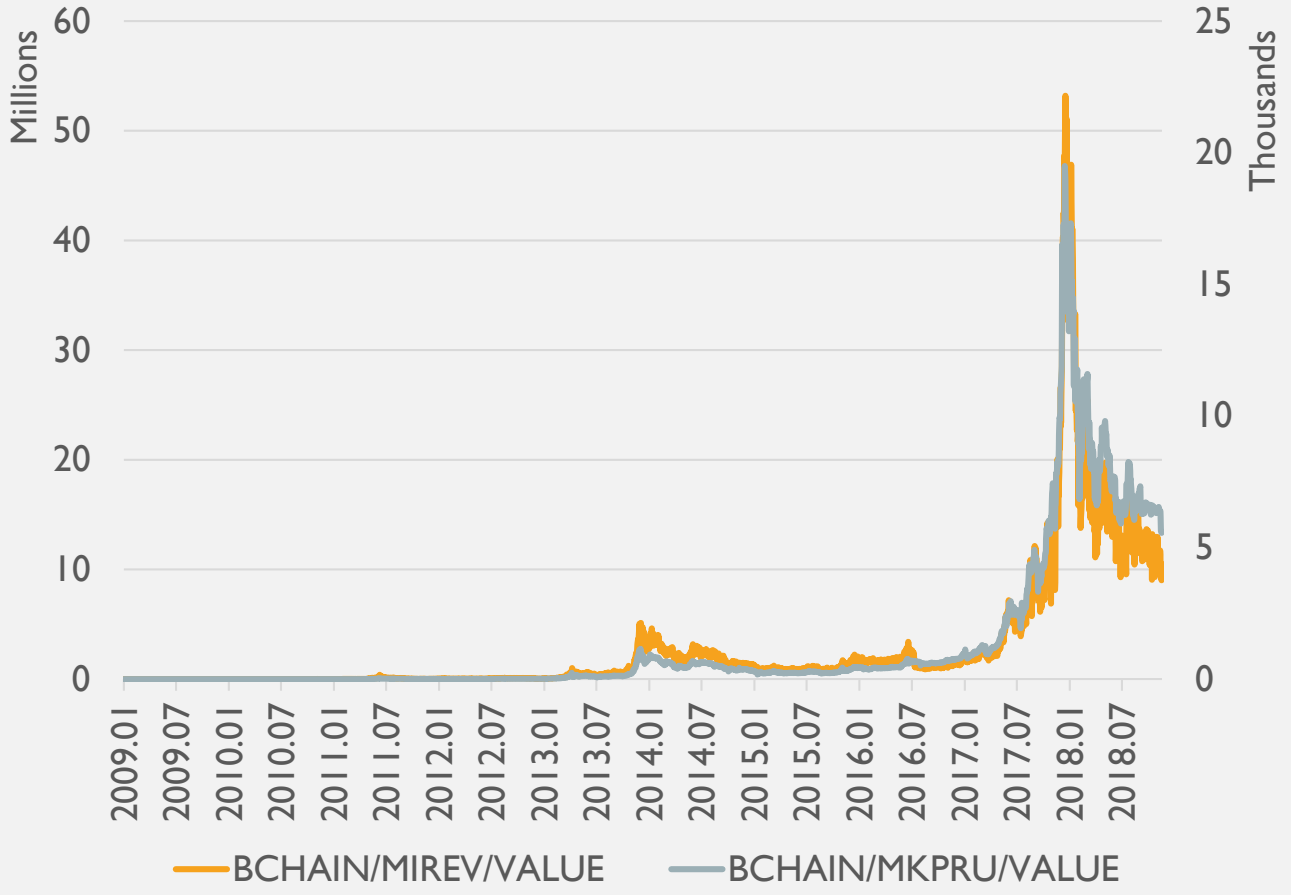
MINING PROFITABILITY

In the same way that mining difficulty is a product of global hash rate; mining profitability is a function of bitcoin price.

However; also included in this factor is the increased difficulty.

We see this as miner revenue is now trailing market price as difficulty increases.

Thus putting pressure on miners to gain technological edge to outperform market price.



ARE YOU HODL?


BTC/USD
SMA (50,0)
6,800.0000
6,700.0000
6,600.0000
6,500.0000
6,400.0000
6,300.0000
6,200.0000
6,100.0000
6,000.0000
5,900.0000
5,800.0000
5,700.0000
5,600.0000
5,500.0000
5,400.0000
5,300.0000
5,200.0000
5,070.5098
FXSTREET
RSI (14,70,30,1)
50.0000
0.0000
MOM (20)
0.0000
-1,000.0000
-2,000.0000
Aug 13 16 19 22 25 28 Sep 4 7 10 13 16 19 22 25 28 Oct 4 7 10 13 16 19 22 25 28 Nov 3 5 7 9 11 13 15 17 19

SO MAYBE NOT BITCOIN…

SecSIG

BACK TO THE BEGINNING

Data as a Public Commons
Data exist without ownership, application, or location.
Data that is meant to be public should not rely on centralized custodianship in order to be made available.

Data is Immutable
Known data should be protected from corruption.
Data that is meant to be public should maintain integrity and be resistant to attack by those who would seek to interfere.

Data is Direct
Individuals should be able to transact value without interference. Data conveys value. Data must be directly transactional in a secure way without facilitation or interference by another.

Distributed Ledger
Everyone knows what is public and has a way of maintaining consensus as new data is created.

Identity Assured
There are secure methods for identifying people and data.

Everyone Is Welcome
Anyone can fully participate, which is a core principal in everyone can validate data.

It's Messy
This is very new and is built without centralized standards.
It takes awhile to refine and make it ready for widespread use.

SecSIG

CHARACTERISTICS OF A GOOD BLOCKCHAIN APPLICATION

- The use of blockchain must provide a service that is otherwise not practical given traditional technologies.

  Primary to these are the need for public trust, distributed ownership and open design.

- The application must align the ability to scale and provide velocity with those of the blockchain technology being employed.

  Blockchain does not currently scale well. If your question is public or private blockchain, you're not addressing this question sufficiently.

SO GIVE ME AN EXAMPLE

Non-Fungible Tokens

- Supply Chain Management
  Components through end product are tracked at all points during manufacture by anyone producing, transporting, storing, modifying, transforming, retailing and ultimately consuming the product.

- Rights Management
  The use of an asset can be conveyed, managed and consumed as a matter of public record.

- Distribution Systems
  As a follow on to content distribution networks, chains can contain serialized data that act as a registry.

EXTRA CREDIT

- Ethereum
  Ethereum.org
- Ethereum ERC-721 Standard for Non-Fungible Tokens
  erc721.org

SecSIG

QUESTIONS

Visit us and download this presentation at SecSIG.org
Turn In An Evaluation and Get A Free Handout of Today's Presentation

US Mensa Security Special Interest Group Presentation

Title: Blockchain Fundamentals
Version: 2018.11.19
Time: 45 Minutes + QA
Audience: General Interest

Abstract

The audience will learn general fundamentals of blockchain technology and how the implementation has changed over the first 10 years since Bitcoin was introduced.

Speaker Biography

Bill Weber is the Director of Cybersecurity at MIT University's Lincoln Labs and a frequent speaker on personal and information security as well as cryptocurrency and blockchain technology.

With over 30 years in the field, Bill has worked with organizations like Microsoft, Electronic Data Systems, Hewlett-Packard and now MIT to provide leadership in cybersecurity to defense, financial and healthcare clients globally.

Contact Info

Email: info@secsig.org

Web: secsig.org