

Block Chain Fundamentals

Mensa Annual Gathering 2019 Phoenix

Mensa Security Special Interest Group

TLP: White



SecSIG provides 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 webpage or email us.

secsig.org
info@secsig.org

TLP: White



A QUICK BIO

Bill Weber is the Cybersecurity Sector Manager 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

secsig.org
bill@ll.mit.edu

TLP: White



WARNING

As with all of our content, we are not your lawyer. In fact, we are not lawyers and in no way is this sage advice.

You shouldn't do things that are illegal.
We're not suggesting otherwise.

For any reasonable purpose, you should assume that we don't know what we are talking about, and you should figure this stuff out on your own, or not at all.

We normally mention that our opinions are not necessarily those of anyone else, like our employers. They have no opinions. No one is paying us to talk about this stuff.

Lastly, don't call us because you ran out and bought BitCoin at its high. In case you did though, thank you. We may owe you a beer. #HODLforever

Enjoy.

TLP: White

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.



TLP: White



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.



TLP: White



Technology Building Blocks



Hashes



Nodes



Blocks



TLP: White



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.



TLP: White

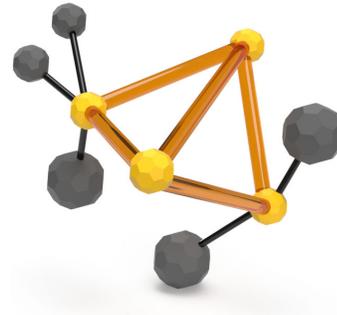


Nodes

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.



TLP: White



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.



TLP: White





A Brief Tangent Into Bitcoin

TLP: White

Characteristics of a Currency

Consistent Exchange of Value

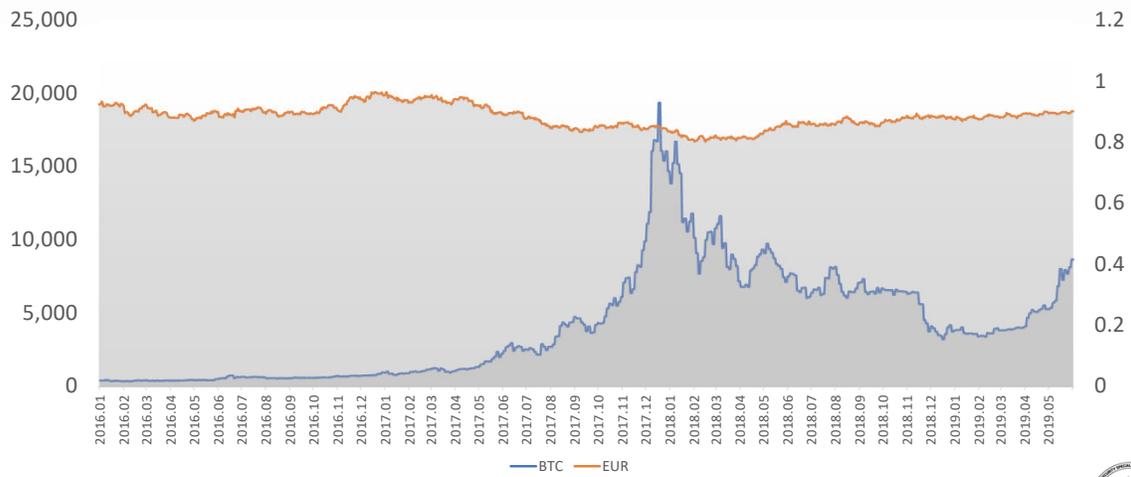
Ubiquitous Acceptance and Low Transactional Friction



TLP: White



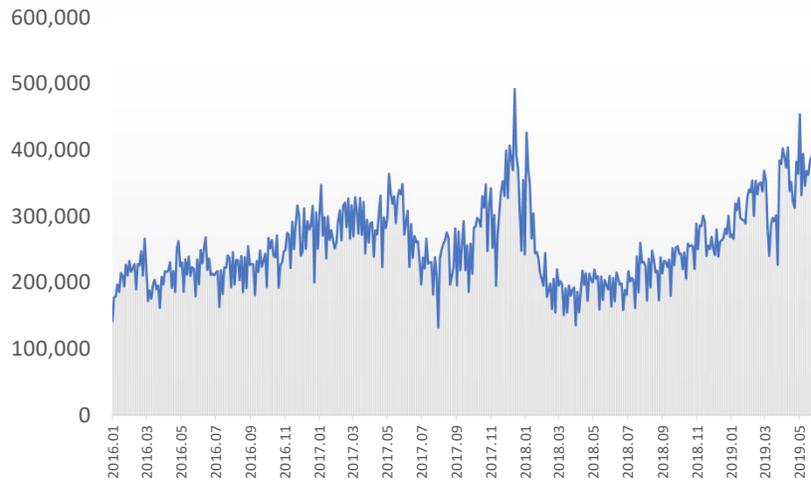
Bitcoin Price



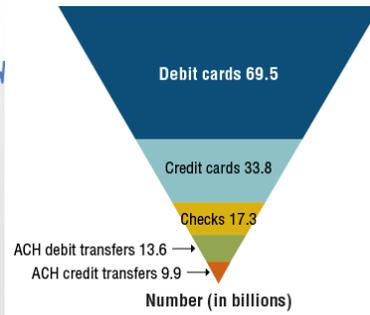
TLP: White



Bitcoin Transactions Per Day



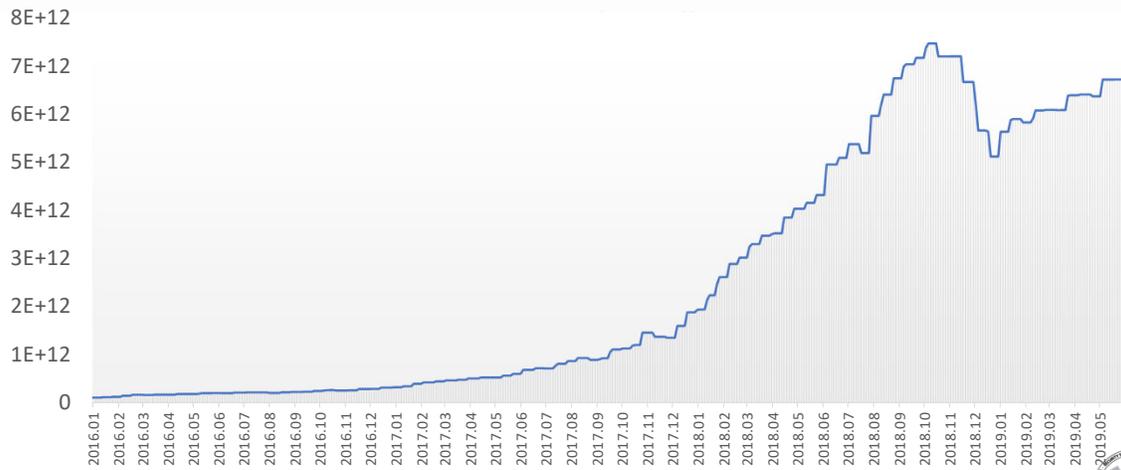
USD Non-Cash Payments for 2015



TLP: White

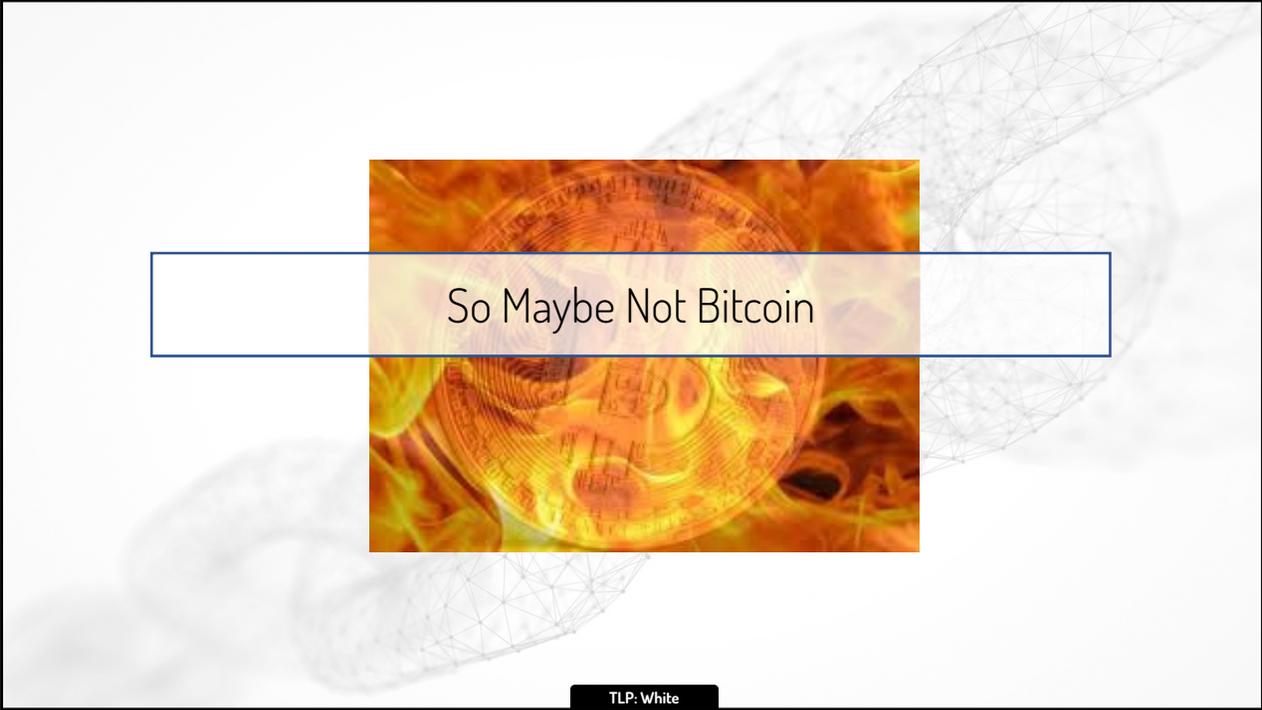


Bitcoin Difficulty



TLP: White





So Maybe Not Bitcoin

TLP: White

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.



TLP: White



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.



TLP: White



So Give Me An Example

Non-Fungible Tokens

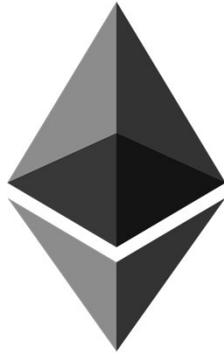
- Supply Chain Management
Components through end product are tracked at all points during manufacture by anyone producing, transporting, storing, modifying, transforming, retailing and ultimately consuming the product.
- Rights Management
The use of an asset can be conveyed, managed and consumed as a matter of public record.
- Distribution Systems
As a follow on to content distribution networks, chains can contain serialized data that act as a registry.



TLP: White



Extra Credit



Ethereum

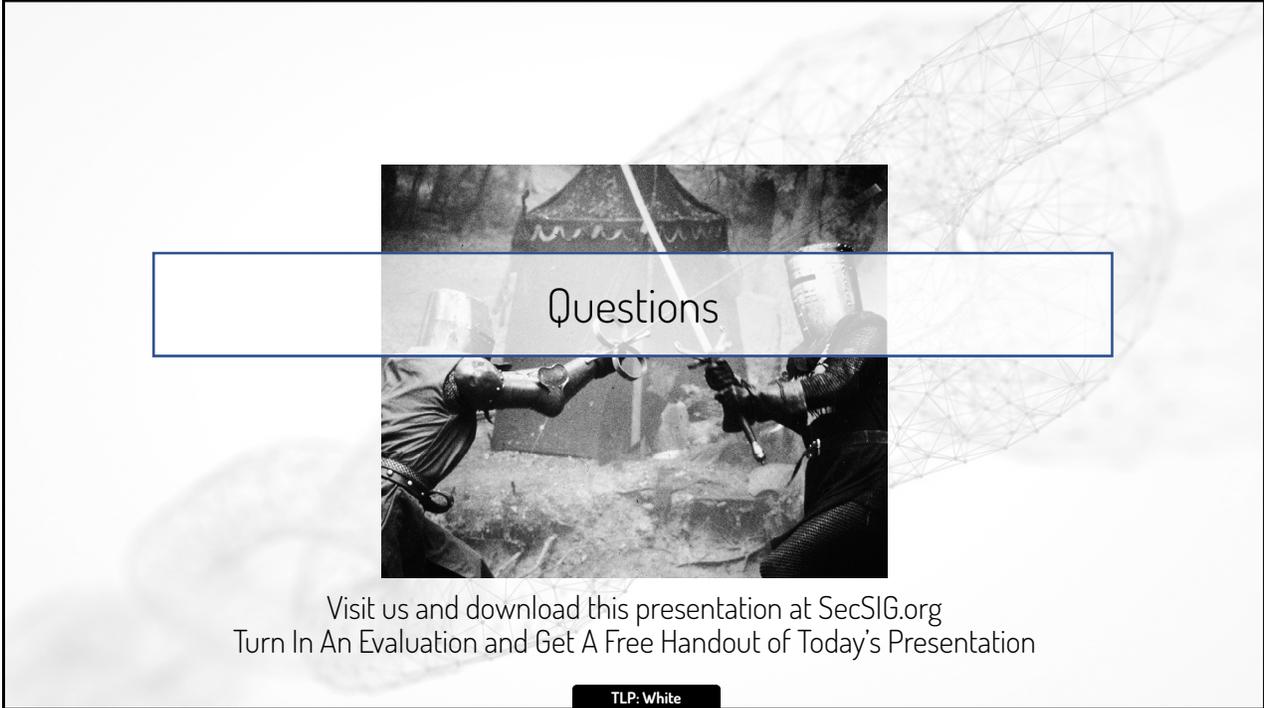
ethereum.org

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



TLP: White





Questions

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

TLP: White