Frequently Asked Questions

Version 1.0
November 17, 2014

In a nutshell, what is Factom?
Factom is a way to record entries in a way that makes the list unique (everyone gets the same copy) and allows anyone to add to the list, but does not allow anyone to change entries once they are in the list.

As a designer of business applications, why should I consider using Factom?
Factom is a method of creating an immutable audit trail. It is also a mechanism to communicate changes in a system. If your application needs a central server to coordinate processes, you might be able to eliminate the central server in favor of using Factom.

Does Factom use a cryptocurrency?
Yes. You can use Factoids (the Factom currency) to purchase Entry Credits with a simple transaction. The protocol does the conversion, so you effectively purchase the Entry Credits from the protocol. You assign those Entry Credits to a public key.

Who controls Factom?
Factom is a distributed, decentralized protocol running on top of Bitcoin. That means nobody controls it, but that it is software that people all over the world run to make the protocol work.

Factom.org is releasing and maintaining the software. But the software is open source, and anyone is free to use it for any purpose.

Will there be a crowd sale of Factoids?
Yes. We have a crowd sale scheduled for early in 2015.

Are Entry Credits recycled or burnt?
Entry Credits are burned.

What is the origin of the Factom Name?
Factom comes from the Latin Factum for "Anything stated and made certain."

Where can I find out more about Factom?
You can go to the website at http://Factom.org, where you can read the whitepaper,. Also, find us on Github, Facebook, Twitter, Linkedin, and local Meetups.

Who are likely to be the first users of Factom?
We are working with a number of parties to use Factom technology in their applications. We should see Factom in 2015r supporting applications for asset trading and management, security applications, coordinating systems of record, simple proof of publishing, and more.

Who runs the Factom Servers?

Individuals wishing to run Factom Servers will set up a profile in Factom (to be specified), and recruit user support. The top servers ranked by user support will be the Federated Servers, followed by the Audit Servers (that stand by to step in were a Federated Server to lose support or is offline).

How can I help make Factom Successful?

You can join the community to give us feedback, work on the infrastructure, build applications using Factom, get involved in the community, spread the world via social media, … Really any number of ways. Talking to the Factom team is a good idea, as we are working to document and acknowledige everyone in the community that is part of the effort.

Is Factom an Open Source project?

Yes.

Will Factoids have their own blockchain?

Ultimately Factoids will be implemented on their own Chain in Factom. For the crowd sale, other options are possible.

How are Factoids created?

Two ways. Factoids will be created as a part of the crowd sale. Secondly, Factoids will be created at a fixed rate and paid to the Factom Servers and Audit Servers for their work running the system, and to pay other incentives.

Can Factom store all of my business process data on the blockchain?

No. Factom puts very little data on the blockchain. Instead, Factom places data in its own structures, which are shared and secured over a distributed hash table (much like torrent files).

How will Factom pay for Bitcoin transactions?

The individuals running the Factom Servers pay those transaction fees. In turn, they are rewarded with Factoids.

Is Factom primarily about proof of publication, proof of process, or proof of audit?

Factom is about all three.

We prove the existence of each entry in a Chain. This is proof of publication.

We group all the entries in a Chain which allows them to be enumerated, the order examined, and the validity of each to be determined. This is proof of process.

Lastly, a Chain is immutable, so it can be presented at any time. The documents behind the Chain can be provided by the client application's organization, and independently validated against the chain. This is proof of audit

Will data I send to Factom be secured forever?
Nothing is forever. That said...

Factom will hold the data as long as the protocol and Bitcon are running. Even if Factom went away, the data can be validated as long as the user kept a copy of their data, and has access to the Bitcoin blockchain.

How does a person use Factom?
Factom is a technology used by applications. We will have some sample applications that provide proof of publishing, journaling, and other features useful to people.

How does Factom make syncing multiple systems of record easier?
In today's world, a system of record holds the definitive answer to questions within its purview. Factom can allow such a system to post the hashes of information as (for example) an individual's case changes. That would allow another entity to request the update, validate it, and use it. The Factom Chain not only allows validation of records, but provides notification of changes to records.

What if Factom is being used to record a series of events, and an event is recorded incorrectly? How do I fix that?
Factom reflects the way the real world works. An incorrect record can be updated with a new entry in the same chain. Pretty much any mitigation technique for errors used today would work in Factom…. That is, except for changing historical journals. Factom doesn't support denial -- a denial that an error occurred or a denial that an error was fixed.

If you lose your document, can you get it back from a hash stored in Factom?
No. A hash isn't reversible, so while having a document means you can get the hash, and the hash is for all practical purposes unique to a document, there is no way to get the document from the hash.

If someone is using a Factom Chain to track ownership of an asset like gold or silver, could a malicious Factom server steal my gold?
No. Transactions have to be signed to be valid. The server can't sign for you because they don't have your private key (unless you gave it to them, had it stolen, etc.). They only thing they can do is delay a transaction. But you immediately know that they are doing that if they do. Once you get your confirmation, the order of transactions cannot be altered. Validate your chain, and if that checks out, you are good.

Could someone double spend an asset trade recorded on a Factom Chain?
No. Not if you have the Chain, and validate the transaction. Once a transaction is entered into a chain, the order is fixed, and will never change.

With Bitcoin, a transaction can be trusted with more levels of confirmation. Is that true with Factom as well?
Yes.

When you reveal your transaction on a chain, you get a receipt. That is level **one**.

After a few seconds, if none of the servers have issued a Server Fault Message (SFM), and you have three more messages from the server handling your Chain. That is level **two**.

The Directory Block is issued. That is level **three**.

The Anchor is submitted. That is level **four**.

The Anchor makes it into a Bitcoin Block. That is level **five**.

From here, you can wait for as many Bitcoin confirmations as you like.

What if someone posts something obnoxious to a Chain I am using, like links to porn in my Chain?
If the chain does not validate according to the rules of your application, you can note the entry as invalid, and ignore it, and remove it from your system.

Is there a security mechanism for the period of time between bitcoin blocks?
Factom uses consensus between the Factom Servers for the 10 minutes until an anchor is set, and then the Bitcoin blockchain forever after.

Is there a notion of a fork or blockheight for this period, for example if multiple servers send competing entries to bitcoin network?
Factom uses a deterministic selection to select the server to post the anchor to the Bitcoin network. No other server can validly post an entry without causing a Server Fault and being booted from the active Federated Server pool. If the server responsible for setting the anchor posts the wrong one, this too causes a Server Fault. In this case, the server will be removed, and a majority of the remaining servers will post a fault notice to the Bitcoin blockchain (so that it will be noted there), and the next server in line will post the correct anchor. This process repeats until a proper Anchor is set. As long as most of the Factom servers are honest, the correct anchor will be posted.

If there is a security/consensus mechanism, then what is the purpose of using bitcoin blockhain?
Factom's consensus mechanism is designed to ensure in real time all actors are acting properly. But to be unique, we need a publishing mechanism that cannot be altered. This allows audits over time in a way that the Factom consensus algorithm does not allow.

Is Factom secure simply because of the fact the content of the reveal is unknown to the servers?

No. The commit/reveal commitment scheme provides an anti-censorship mechanism that prevents servers from denying the recording of otherwise valid entries, for reasons based on content or chains. Validly paid entries are to be recorded. On the other hand, there is nothing that prevents a concerned group from creating their own chain that documents offensive entries (in their view) so that users that subscribe to that idea can avoid ever downloading those offensive entries. This can actually be done quite effectively (with many references within a single entry) so that the removal of spam and such is much cheaper and easier than it is to post it.

How is a server chosen to send the bitcoin transaction?

Through a deterministic ranking of the servers based on hashes closing the Directory Blocks. The Federated Servers, and Audit Servers and the users looking at the Directory Blocks can determine which server must post.

Can Factoid be traded externally like an alt-coin?

Yes.

Is there a separate Proof of Work or other consensus mechanism for factoids, independent of factom?

No. That said, the Factom chain and the Entry chain are managed by the Factom Servers (they are the application using these chains) so they validate them in real time. No invalid entries can be placed in these chains.

How do factoids get sent back to the protocol? Is it a kind of burn?

No. The Entry Credits are burned. Entry Credits are non-transferable. They can only be used to buy entries. But when they DO buy entries, the Factoid in the protocol that was used to buy the Entry Credits is released. The amount of Factoids varies since the price of Entry Credits per Factoid varies.

The Factoid paid out is calculated by dividing the total number of Factoid in the protocol by the number of outstanding Entry Credits.

The number of Factoids in the protocol and the number of outstanding Entry Credits are all computable from the Entry Chain and the Factoid Chain.