Paul Snow
Chief Architect, Co-Founder
Factom Inc.
Disrupter Series: Digital Currency and Blockchain Technology
before
The Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade
U.S. House of Representatives
March 16, 2016

Thank you Chairman Burgess and members of the Subcommittee for the opportunity to testify before you today. I am Paul Snow, the chief Architect of Factom, a protocol focused on lowering the costs and barriers to creating new Blockchain based solutions, as well as applying Blockchain based solutions to existing systems.

Blockchain based technology has been cited as disruptive by the Brookings Institution[1], Deloitte[2], Goldman Sachs[3], and many others. The open source protocol Bitcoin Blockchain was launched into the computer ecosystem in 2009. By 2012 the disruptive nature of this protocol was becoming evident. Bitcoin the currency was just the beginning of a more general revolution in how we approach data security, settlement, business process audits, and more.

Through Cryptographic checks and distributed ledgers, we can advance financial reform, increase efficiency, reduce costs, increase privacy, and oddly enough, reduce crime and money laundering. I was quite surprised by the warm reception many three letter agencies afforded crypto currency and Blockchains.

---

[1] Beyond bitcoin: The future of blockchain and disruptive financial technologies http://www.brookings.edu/events/2016/01/14-beyond-bitcoin-blockchain-disruptive-financial-technologies

[2] Banking reimagined How disruptive forces will radically transform the industry in the decade ahead http://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-banking-industry-outlook-2016.pdf

[3] Emerging Theme Radar: What if I Told You… http://www.goldmansachs.com/our-thinking/pages/macroeconomic-insights-folder/what-if-i-told-you/report.pdf

at the Department of Justice's Digital Currency Conference held at the Federal Reserve in San Francisco last year.

Allow me to cover a few points about the technology behind Blockchains that might not be obvious. First of all, Blockchains utilize Hash functions to link together blocks of information. A Hash is a way of taking any digital artifact, a document, picture, video, transaction, etc. and producing a short digital fingerprint. A block is a collection of transactions, and can include these fingerprints and other digital data. When a block is added to a Blockchain, the hash of the previous block is also included in the new block. That's the "Chain" part of Blockchains. Validating a Blockchain includes checking the hashes or the fingerprints, and making sure they match. Any error or change in data would "break" the chain; the hash of the changed block would no longer match the hash in the next block in the chain.

Since we can hash anything digital and produce a unique ID, we can now talk about building trees of hashes. We call these Merkle Trees. Just like a sports bracket, pairs of hashes can be hashed together, in a repeated fashion until you have only one hash, what we call the Merkle Root. Now here is the magic: Just like I could track a team through a tournament bracket and only need its opponents to see it progress to the winning slot, all I need is the hashes as they are combined to reconstruct the Merkle Root from the hash of an artifact. A proof that some data has not changed can be very small, even if it is only one of billions of entries in the beginning.

Lastly, a public witness is critical to the security of a Blockchain. Bitcoin uses a system of difficult hashing problems and a global network to ensure that all nodes in the Bitcoin network have the same, validated ledger. In fact, Bitcoin's ledger is certainly the most secure data structure on the planet. Including a Merkle Root into Bitcoin allows all of Bitcoin's security to be applied to truly huge sets of data.

Factom uses these basic concepts to allow its users to create their own groups of entries. Every 10 minutes the Factom Protocol writes one of these Merkle Roots of all the data collected into Bitcoin. This serves to "Anchor" Factom to Bitcoin. As a result, any modification to any part of Factom would "break" the

Factom Anchor. Factom will place anchors in many Blockchains, both public and private. Doing so makes the same Merkle Root available in many contexts. Syncing two systems based on different Blockchain or traditional systems only requires matching the latest hash. This allows an application running on a Private Chain to be able to run the same cryptographic proof as an application running on a different Private Chain.

Effectively applications can share process histories, transactions, market data, sensor data, product tracking, or any other data of interest.

It may seem very complex, these "Blockchains" and "Merkel Roots" and "Hashed Artifacts". One might ask, "What does a Blockchain solution bring to a problem that is radically new and different from existing solutions?"

The surprising answer is nothing new and different. But a much better solution.

Blockchains provide three things, accountability for the data entered, notification services of new data, and algorithms for ensuring all systems have the same data, i.e. consensus between systems.

We have solutions for accountability, notification, and consensus today. However, the older solutions are more error prone, more expensive, and complex to maintain. Blockchain based solutions hold the promise of deploying faster, accountable, lightweight solutions where the older approaches have failed.

Blockchain based systems will be able to track any manner of manifests and business processes for consumer goods, components, drugs, and food to ensure safety and quality. We will see Intellectual Property and Copyrights documented managed over Blockchain applications to streamline royalty payments and accelerate innovations. Increasingly mortgages are traded and move across different systems. Blockchain based solutions can and will ensure that such transfers do not lose data and result in the kinds of errors and mismanagement we saw in 2008 to 2010. Blockchain solutions promise to address

issues in all sectors public and private, and address pain points in all industries. While we have had solutions in the past that sort of worked, Blockchain based solutions promise very disruptive changes that will bring greater efficiencies, transparency, privacy, and most importantly, accountability to all parties.