From:	Grance, Tim (Fed)
To:	Kelsey, John M. (Fed); Dray Jr., James F. (Fed); Barker, Elaine B. (Fed); Barker, William C. (Assoc); Regenscheid, Andrew R. (Fed); Chen, Lily (Fed); Perlner, Ray A. (Fed)
Subject:	Re: What next on blockchain?
Date:	Monday, April 11, 2016 9:17:45 PM

I think there are many places for which pure integrity of the data with or without encryption is important where block chain could be useful. The smart contracts especially in places where rule of law/processes (Russia, china, elsewhere) is pretty suspect that this could really help US industry compete.

I think the real challenges are practical (large scale distributed development of software, government resistance to change from complex but familiar terrain of business, and tantalizing but not real large implementations.

A ton of venture money is flowing into this. On one side are the blockchainiacs who see it powerfully disintermediating central control and changing identity, rights management, voting, and then the skeptics who say beware of technical evangelists saying real human problems can be solved by technically complex schemes understood by only a few. I saw this a few weeks ago

> The hurdles these visions would have to overcome are those any blockchain-decentralization scenario faces: the challenge of finding people to begin using and moving their own assets into new, unproven systems; the "discovery problem"—figuring out how users of anonymous, crypto-secured networks can find one another to transact business; and the fear that all this crypto-secured, anonymous-transaction-based tech will simply power illegal enterprises and antisocial activities.

Nonetheless people speculate that is will

> Ethereum's creators, for example, foresee a world in which autonomous blockchain-based entities pick up where governments and corporations have failed and lead us into a glorious future. The people behind the Scotland-based Maidsafe are similarly thinking big: They aim to rebuild the whole Net along peer-to-peer lines. Under their scheme, we all store our data, encrypted of course, on one another's machines; we all share our processing power; and we pay one another for the privilege. The server farms will fall fallow, and the Internet will get back its inter-ness. (Maidsafe, to be clear, does not use a

blockchain, but its encrypt-and-decentralize approach makes it a fellow traveler with the blockchainiacs.)*

What do I think we should do?

I think as Jim Dray said knowledge, experience, and monitoring are good steps. I think writing a publication exploring the technology, having a workshop, writing about the technical challenges and opportunities, the cryptographic questions (what happens post quantum BTW), defining some terms of the debate about block chain, and noting the key technical questions would be immensely valuable.

This is not the traditional turf the crypto group takes on so yes I am suggesting something different.

My two cents.

Tim

From: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>
Date: Monday, April 11, 2016 at 5:39 PM
To: "Dray Jr., James F. (Fed)" <james.dray@nist.gov>, "Barker, Elaine B. (Fed)" <elaine.barker@nist.gov>, "Barker, William C. (Assoc)" <william.barker@nist.gov>, "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, Tim Grance <grance@nist.gov>
Subject: Re: What next on blockchain?

The big advantage of blockchains is that they let you keep a record that can't be changed (nobody can rewrite history), and the power to decide what goes into the record is distributed among many different entities, so a single entity turning evil or being subverted or national-security-lettered or bought by someone evil doesn't have the power to mess up the record. (I think the smart contract stuff falls out of that--the terms of the contract are similarly carried out by a consensus among many entities, rather than a single potentially-corruptable entity.) So if we want applications for blockchains, it seems to me that we want places where we'd like some record to be more trustworthy than any single entity.

The NIST beacon doesn't use distributed consensus, but we do use hash chains in our records, and the whole point of that is that it means that even we can't change the past. Neither someone compromising our server, nor someone at NIST taking a bribe, nor an order from the president can allow us to change our record of past beacon pulses without risking being caught.

Are there other federal applications where we might want some kind of distributed consensus, to guarantee

that even the entities mainly responsible for keeping the records can't alter them or enter fraudulent transactions? I think at least the hash-chained, signed record part of this would be useful in a lot of places. For a lot of things, though, what's needed isn't so much distributed consensus determining what can be added to the record, as distributed auditing, so that if some agency were adding fraudulent transactions to the record, some outside entity would be in a position to detect it and make that fact public.

Comments?

--John