SANDIA (think TED) talk 2018, by Nick Pattengale[1]

I know the title of my talk emphasizes the word blockchain, but this talk is really about trust.

Here's a hypothetical.

Imagine it is 2008 and one of your friends tries to tell you - next year someone is going to write a research paper describing a network protocol, just a network protocol, that in turn will in a few short years

1. completely redefine global perception on the definition of what it means to be a currency
2. spawn a true renaissance in cryptography research, and
3. create, out of thin air, hundreds of billions of dollars of value

You'd probably tell your friend to keep dreaming! But this is in fact what has happened. How on earth does this arise out of a network protocol definition?

It has arisen because normal people around the world have decided to run open source software containing implementations of these network protocols, it's really that simple. But what that has amounted is also staggering.

The amount of compute power that people bring to this global network is measured in zetta flops. Zetta is an order of magnitude more than exa, and humans

[1]Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of EnergyâĂŹs National Nuclear Security Administration under contract DE-NA-0003525.

have

have yet to achieve an exascale supercomputer. That is to say that the computing power of this global decentralized network is tens of thousands the compute of all the world's supercomputers combined.

The reason this is important is that in order to compromise the integrity of the data in these systems requires controlling a majority of the compute, and that's just to rewrite the data bouncing around in the network now, rewriting history requires exponentially more compute than that.

And so that's what I mean when I say this talk is really about trust. Both the strength of the integrity of data, and new constructs for verifying that integrity afforded by this system, completely redefine what it means to have trust in information.

CLICK - bitcoin paper screenshot

I first ran across that paper in 2011.

I remember it like it was yesterday. My team and I were participating, as Sandians with expertise in cyber, in Terminal Fury, which was then an annual US Pacific Command tier 1 military exercise. I remember that exercise not for what transpired, but because I snuck away during every free chance I could get, to read and reread that bitcoin paper. I knew at that point that this had a game-changing potential, and that I'd like to make it part of my research agenda.

Of course it wasn't clear back then how, or even if, this was national lab relevant. We did challenge ourselves to estimate its potential for tech surprise, and pondered the implications of large numbers of people in the developing world embracing the technology to address corruption, bribery, and currency instability. That is still a relevant area, but it has turned out that there

is

is so much more, and I'm excited to be here today to share with you other reasons why this is a national lab relevant area.

In the past three years our funded work in this area has gone from roughly zero to approximately 6 FTEs, and I wouldn't be surprised if that increased to 10 FTE in the next year or two. In just the past year, I've had the privilege of briefing chief information officers of municipal governments, senior science advisors to cabinet secretaries, and US Senate staff, on this topic.

Some of these folks are worried about the technology, some of them are excited by the technology, and they look to Sandia to be unbiased tellers of technical truth, one of my favorite roles as a Sandian.

So what is the truth on this technology? First off, most of the urban legends are misleading or outright wrong, for example that bitcoin is anonymous and only good for buying drugs.

CLICK - shady connotation slide

That myth has been throughly busted, and has actually been quite to the contrary. Law enforcement has been quite successful at correlating incriminating information to effectively deanonymize key bitcoin transactions in many high profile cases, such as with the Silk Road, Alphabay, and Hansa darkweb takedowns. And, yes, there is illicit usage of bitcoin, although the data says that legitimate usage outweighs illicit usage 4 or 5 to 1. But more importantly, the invention of bitcoin stimulated an earth-shattering wave of subsequent innovation. By saying this myth is busted, I am not saying that we should dismiss the dark side of this technology's application space. There are serious policy and technical issues here.

Make no mistake about it, bitcoin was an attempt to create a digital cash with privacy properties that make government oversight impossible, and while it didn't achieve this goal, there will be a community of developers that will keep trying, and probably succeed, and we have the opportunity now to figure out what that should mean from a policy and law enforcement perspective, and we should not waste that chance

But my take on this tech landscape is that it is poised to make more profound nationally relevant impact in at least two key ways:

1. it provides more explicit control over where trust, remember I said this talk is really about trust, more explicit control over where trust is placed in information systems, which could play a vital role in, for example, improving design surety of high consequence digital systems, a problem which has been surprisingly difficult to solve

2. it has let the cat out of the bag with decentralized systems, which even if the currently deployed systems like bitcoin, ethereum, and monero, don't last, will permeate the next generations of software developers and system architects with options they previously didn't realize could work. A push toward true decentralization will have policy and technology impacts for decades to come. Systems with true decentralization change the calculus on whether those systems can be 'shut down.' This is good for resiliency and fault tolerance in systems where you want that, but presents enforcement challenges when decentralized systems are being used for illicit purposes.

Let's take a step back and establish some technical definitions, so we're all on the same page.

We'll begin by busting another myth. Specifically, that bitcoin and blockchain are the same thing. They're not. Blockchain is a technology that underlies bitcoin, but which has far wider applications than cryptocurrency. You may have also heard the term 'decentralized ledger technology,' which like blockchain is another generalization in this concept space.

The way they relate is as follows - bitcoin is an example of a blockchain, and blockchain is an example of a decentralized ledger.

CLICK - bitcoin ⊆ blockchain ⊆ DLT slide

I'm now going to use one of my valuable minutes in this talk to explain how all blockchain systems work, because people make it much more complicated than it needs to be. Users cryptographically sign data, basically any kind of data, and send that data to the volunteer peer to peer network we've already discussed. The network gossips that data around and ultimately appends it to this history data structure, the so-called chain, such that if I can see the data in the chain, I can be confident that you can see it too, no matter where you're using the system from, and I can also be confident that the data looks the same to both of us. That's all there is to it.

CLICK - chain depiction slide

The aspect that distinguishes platforms from each other is the logic that the network applies to decide whether any particular piece of data is allowed to be appended to the chain.

So that's blockchain, in a technically accurate form, in less than 60 seconds.

And

And all you have to do is use your imagination a little bit to see how this capability when globally deployed and open for anyone to use can be quite powerful.

If we fast-forward to a day when everyone on the globe is internet connected, a day which is closer than you might think, then the first use case of this technology I'll discuss is that

1. anyone can confidently send digital assets to anyone else, without ever having to register for any account. This use case covers cryptocurrency, but also any other digital asset. When you send a document to someone today, you are sending a copy, and as a result both parties can further disseminate at will. With blockchain, you actually transfer a digital asset, and only one of those parties will be able to further disseminate.

   The national lab relevant impacts of this use case are the obvious ones - banking and finance, remittance and wire transfers, illicit commerce, and complementarily law enforcement and financial crimes enforcement, but also extends to anti-corruptio asset management, and government record keeping.

2. probably more important than the first - trust anchors, or the ability to commit to knowledge of a piece of information at a specific time, without having to use a notary.

   Remember the old trick of sending a sealed manuscript to yourself or your lawyer to prove a copyright assertion by its postmark? This is essentially that. The national lab relevant impacts of this are in voting, intellectual property, design integrity, and

provenance tracking in supply chains, a use case that has also received a lot of popular press.

3. again perhaps more important than either use case discussed thus far, the data being added to the chain can be computer programs, which are executed by the volunteer peer to peer network, so called smart contracts, which afford mutually distrusting organizations to multilaterally run code together, and be confident that everyone sees the same execution and results.

   The national lab relevant impacts of this use case are in transactive energy markets, data peering markets, trade agreements, international safeguards, and treaty verification

CLICK - treaty/pencil slide

So I said this talk is really about trust, and I stated that an impact of this technology is 'more explicit control over where trust is placed in information systems?' I'd like to pull on that thread, and give an example.

Today, we're all forced to place trust in the controls and processes that organizations put around their data.

A problem with that is that typically anyone and anything with access to particular data can modify that data, at will, in ways that are very difficult to detect.

CLICK - keycircuit slide

One of the breakthrough features of blockchain is a practical scheme for trusting data without having to trust who produced it or who sent it to you. The data itself contains artifacts that prove its integrity and authenticity, all backed by the power of that global peer to peer zettaflop network.

Think of what that means. Digital data we can trust to have certain verifiable properties, without having to

trust who sent it to you, or necessarily who created it.

In non digital domains we always have the fall back of using micrometers, x-rays, and other measurements to independently validate physical properties of high consequence components to build trust that nothing its supply chain was subverted.

We don't have a digital analogue, and blockchain starts to give us real options in the domain of digital systems, which of course are already at the heart of many high consequence components, to independently validate integrity and authenticity in breakthrough ways in digital systems. This is a major step forward whose impact is only beginning to be felt.

And so if you've heard the blockchain community's infighting, debates about block sizes, and public versus private versus permissioned blockchain systems, and proof of work versus proof of stake versus proof of authority or proof of whatever, these all represent different tradeoffs in this trust landscape, some more powerful than others, but all more explicit and more expressive than constructs available to today's IT, and that's a big deal.

Only time will tell, but there is almost universal consensus that we are in the very early days of this technology arc, to use an analogy, the early 90's, the MySpace days, of this technology arc. What an exciting time to be taking a national lab crack at these problems.

Even with the compelling applications we know about, there are still major barriers to adoption, that don't just have to do with the technology's immaturity. For example,

CLICK - encrypted email joke

1. cryptographic key management is still an unsolved user experience problem
2. it is still an open question where humans actually prefer to have a third party in certain situations, even if it costs more, and has more inherent vulnerability, decentralization is not always the answer to every problem

And so in closing, I'd like to remind you of where I see the national lab level impact of this technology. It is in two places:

1. as a new set of tools in our tool belt to more elegantly approach trust assumptions in our information systems, so as to hopefully make breakthrough progress on perennially difficult problems like digital supply chain tampering and design trust, and
2. giving us lead time to get in front of what it means to have technology with true decentralization, which has both great promise and great peril. Great promise in resiliency, integrity, and trust, and great peril when those same properties are used by those up to no good.

The opportunity to get in front of these issues is still open, and I for one plan to take that opportunity.

Thank you