TRANSCRIPTS

# July 2020 Videos

A complete transcript of every recorded talk from the July 2020 Videos.

| 1 | 34:44 |
| --- | --- |
| TALKS | RUNTIME |

November 26, 2026

# CONTENTS

Full transcripts of all 1 recorded sessions, in the order they appear in the archive.


| | | |
|---|---|---|
| 01 | NonconformistKeynoteWeb20200702 | 34:44 |

TALK I

# NonconformistKeynoteWeb20200702

July 2020 Videos · talks · 34:44

You know, by way of introducing Sam, for those of you who don't know Sam, you know, he was recently elected to be the chairman of the board at the Sovereign Foundation. So congratulations, Sam. In looking at Sam's background and reading, you know, some of the of his past works. I was just in awe and I felt very lucky, you know, by way of another past guest of the podcast, Phil Winley for introducing him to us. You know, he comes, you know, with the background as both an entrepreneur, a consultant, you know, very prolific in his writing, looks likes to spend time at the intersection of AI, blockchain, and decentralized identity. So, with that, I'm going to turn it over to Sam. And Sam, thank you very much for joining us from whereabouts in Utah are you from? – A little town called Lindon, which is a sub, you know, in the greater metropolitan area for Salt Lake City, Utah. You know, everybody in Utah lives in a three-county area. The rest of the state is mostly empty. – Well, I'm going to, you know, turn it over to you. Thank you so much.

And take it away. All right. Thank you. So I'm going to talk about the economics of its and bits. And that's going to cover a little bit about digital identity, freedom, privacy, control, and security. And I left security for last because it's actually the most important part of this conversation. And those that know me probably aren't surprised when I say that. So when I talk about economics, I'm really talking about value, creation and capture. And so in the environment of digital identity, what do we mean by that? Well, we talk about value extraction exchange and of course exploitation. And in order to have economics, somebody to benefit from economics has to have control over value. That's the key thing. And if you want control, then you need security. And so this cuts at the root of everything that we do in digital identity. If we don't have security, we don't have control over value and that leaves us free for exploitation by others. So, how do we get control over value? Well, this is where the its and the bits come in. When I say its, I mean atoms, physical things. So, a person is made of atoms. So, a person is a physical thing. Buildings, cars, planes, ore, minerals, all of those things are physical things. And here's the thing. It's easy to have security over physical things because physical things are not easily replicable. You have to create more atoms or you have to build or extract or get more atoms. And it costs money. Atoms are relatively scarce. Some atoms are very scarce. And you can maintain control over those atoms with what's called physical security. Just keep the atoms in place where somebody can't get to them. Now, when we talk about bits, we have a problem. Bits is digital information. The problem with bits is that it's easy to copy them. We actually use subatomic particles to transfer and store information, but those subatomic particles, electrons and photons are, you know, virtually inexhaustible. So, from a cost perspective, information wants to be free, easily copied, very difficult difficult to secure, especially if we want to control it because if somebody copies it, we lose control of it. So the question is in ITS, we have certain entities that have control over other entities or other physical bits. In information, what fills the role of a legal entity like a person or an organization or a corporation or a government? What fills that legal role that actually gives the same degree of informational security that I have in physical security. So I'm not going to answer that question right now, but I'm going to pose that question because I wanted to motivate the reason why that's so important. So if we look at 60 years of its and bits, I looked at the Fortune 20 in 1960. You can look at the companies and the Fortune 500, they always in the old days, they did it in terms of revenue. That's how they rank them. You see that all but one company on this list gets its value from capturing its, not bits. Only AT&T is primarily gets its value from capturing, storing, transmitting bits of information. If we go to 1980, well, we got IBM in there. You could maybe say that it got it from bits. It was a equipment manufacturer, but it was equipment to capture value from bits. When we get to 2000, There's a few more in there. We've got Southern Bell, Hewlett-Packard, Compact Computer, and AT&T. But still, the majority of value capture, creation capture is in the it's, not the bits.

2020, things start to change. We see now that for the first time, we've got Amazon, Apple, you know, they've moved up into the top spots, Alphabet, Verizon, But this is revenue. And if we look at something much more telling, it's not revenue, but market cap. This is people saying who is going to capture value in the future? What companies are going to capture the value? And this is a scary list. Now, in terms of market cap in 2020, we've got Microsoft, Apple, Amazon.com, Alphabet, Facebook, and we've got five, well, three, $2 trillion companies. Alphabet was, Amazon was trillion dollars for a little bit in 2019 and Facebook and then Verizon, AT&T are still there. So, the top value captures in the world are the ones that capture value from aggregating bits. They have figured it out. They have figured out how to capture value. And they're doing it through something called network effects. A network scaling law basically describes how network value scales with the number of participants. And so if we have a multi -sided network like this, then Metcalfe's law may apply. And when Metcalfe's law applies, we get this very powerful scaling. So this equation says that the value, the average value to a participant on the network V is proportional to the number of participants on the network. And the total value of the network is the average value per participant times number of participants. So, it's proportional to the number of participants squared. And any square loss scaling is going to dominate when the network gets large enough. And this can be the main value that these companies are able to aggregate is these network effects. And it's the network effects from bits of information that they're aggregating. And the primary value is reach. If you have reach, like you can reach people in Facebook ads or Google ads, or you can reach people in your Apple app on the App Store, those contribute to value that scales tremendously. And if you extract even a little bit of value from a square law network effect, you're going to be an extremely valuable company. And Met- calfe's law has been extensively validated. I wrote a paper on this some these are some of the papers from the quote. You can go look at the paper, look at them if you're not familiar with it. So the question is how do we recapture the value in our data? Because the value in our data is being captured with good effect by these super aggregators. There's two ways that we can capture it. We can leverage cooperative network effects and we can retake control of our data. And when I say retake control, I mean really take control of our data, not sort of take control of our data. So what do I mean by cooperative network effects? Well, what happens to value when two smaller networks combine? And understand, this is how we fight people that are the largest, most profitable, most powerful corporations in the world, right? How do we fight them? Because if we can't fight them, we'll always lose. Because they have more power. They are now at the state size where they are nation states in and of themselves. themselves, they can change how nation states treat them. Well, Metcalfe's law comes to the rescue. If you look at Metcalfe's square law effect and I take two networks, N1 and N2, and I combine them and I look at the square law value, I get this bigger rectangle. And so N1 by itself has this smaller rectangle. N2 by itself has a smaller rectangle. But combined, each of them gets an an added rectangle that is in N2's cases, N1's case is bigger than N1 was to start with. And so without going through the math, what you get is a bonus of an N1 times N2 proportional factor for any two networks that combine. This is essentially free just for combining, just by combining participants from two networks. So why wouldn't any two networks combine? That's a good question. Right? And this is actually the regimes in which combination makes sense. When two networks are value symmetric, that means they're of the same size value, then it's always more profitable for both to combine. And in this paper, positive demand externalities is an operational research code word for network effects. When two networks are value asymmetric, it's always more profitable for smaller networks to combine. This is lifetime value of the combination. Now, when I have two networks where one is much larger, it's not always more profitable for the larger one to combine. That's the problem. If you're large enough, you don't want to combine. But if the network size is below a threshold, then it's still more profitable for the larger one to combine. And that threshold is based on a feedback adoption

growth rate curve, which tends to follow sigmoidal adoption curve. And when you're down here close to the bottom of this curve, even if you're a much larger network, it's still to your advantage to always combine with smaller networks. If you're up here in a saturation regime, there's no advantage to combination. So, what is this? What do competing small networks do? Well, let's look at what happens if we had several competing small networks. Each of them has a value proportional to their side. They're all the same size, right? And if they're square law effect. If I now make a super network of these cooperating small networks, the value of each sub network is 10 times its value before they combine when the size of the total network is 10 times the size. So, I get a 10 times increase in value for free just by cooperating to the extent that cooperation is free. I mean, there's always some cost to cooperation if you don't have interoperable systems. But if you have interoperable systems, then that cost is pretty small. The total value of the super network is 100 times the value of the individual networks combined. This is huge. This allows a bunch of small networks to become super aggregators merely by combining. And when I say super aggregators, I mean benefit have a network whose network value benefits from the network effect. So that is a powerful force that we can use to fight the extraction and exploitation of our data value, how we can fight back. And so this is an equation that says the proportion will value for any network to join a larger network is the ratio of the size of the larger network to the size of the smaller network. So the network effect from a subnetwork joining and cooperating as a super network is the subnetwork's values increased by the ratio of the subnetwork size to the supernetwork subnetwork size. This is the advantage of cooperation. It's a huge advantage. So the small network strategy is to one strategy is to create what's called a cooperative network cascade. What that means is I've got a small network and I'm competing with the larger network. If I convince the larger network to cooperate, then the combined network can now outcompete the next larger network and so on. And so you can cascade to where you can force even the largest existing non-cooperating network to realize that it's more profitable for them to cooperate than to compete because if you're benefiting from Metcalf's network scaling effects. So, how do we remove the primary barrier to cooperation? Even with this knowledge, even with this knowledge that cooperation is more beneficial than competition when you're in the right regime, which happens a lot, but people still don't cooperate. because they're competitors. So how do we remove that barrier? Well, one way to remove that barrier is to look at different value contexts. Look at networks that aren't directly competitive. If we can find value that's transferable between contexts, then we have a way of gaining a cooperative network effect without ever forcing competitors to cooperate because they're not competitors in the first place. They just have to cooperate. And I call this transcontential value creation and capture. So if we can have value that is transitive or transferable between contexts, and context in this case would be products and services in the same market segment, then we have an opportunity to prime or bootstrap cooperative network effects. So we use transcontential value creation and capture to fuel cooperative network effects. And then that starts the cascade. So the final thing we want to do is since the question was how do we regain control of our data value is that we want these cooperative networks to be participant controlled. We want to extract the value from it, not some administrator of a network. Even a cooperative network administrator can extract value. We want the participants to be able to extract appropriate levels of value. So we want participant controlled networks and we can get participant controlled networks if we use the right tech. And what that means is that participants can then create a virtual participant-centric network. And this enables participants to amplify their own value across multiple contexts, which maximizes adoption pool and creates the fastest spin-in of cooperative network effects. That's the economics of cooperation. And another benefit of cooperation is what I call the cooperative long tail network effect. If you think about the long tail, and that's the area under the the long tail in this curve, this is a power log distribution for a market. The long tail is essentially a bunch of different contexts

because they're all too small and disparate and segmented to have enough individual value to be here where people are targeting. And so if we recognize that the long tail is different context, we can create a cooperative network that aggregates the value in that long tail and and get a network effect just from the long tail. So, where do we find transcontextual value? Well, we find it in transaction costs. The theory of the firm, the theory of why any organization has value is that it reduces transaction costs to its customers. There are three ways we can group transaction costs into three buckets. There's lots of ways to do it, but this is a very useful grouping. First set are triangulation costs. These are about connection, fine filtering and matching participants. The second is transfer, facilitation, transport, delivering payment. We all know business models that are focused on one or both of these. The third one, the one that is hidden that most of us don't realize or see is trust transaction costs, security, competency, reliability, privacy, and liability. These trust costs are often hidden costs and they're often not well optimized. They're not reduced. And in many cases, people mistake the value of a network effect from their triangulation transfer and ignore the fact that they actually solved a trust transaction cost. And this is where digital identity and decentralized identity come to play because all of the technical stuff, trust over IP, right? It's about reducing trust transaction costs. So, platforms and networks sell reductions in transaction costs. To a consumer, all costs look like transaction costs. It doesn't matter if it's its or bits. All costs look like transaction costs. The principal super aggregated pull in many cases is reduced trust action costs. Your Facebook login account. You can log into Facebook.

They're going to manage all of your trust for you, all of your security so that you can interact with other participants on the platform and you don't have to worry about it. So, but the thing is trust may be highly transferable. If you think about it, reliability, credibility, accessibility, those things, an entity or an individual tend to be transferable. Those sorts of behaviors tend to be transferable. Security tends to be transferable. Digital identity is transferable. Login, onboarding, all of those things are transferable. So, a reduction in trust transaction cost is a primary network effect value from cooperation. We can leverage that. So, what we want is we want to have transitive value virtual network scaling law. What does that look like? Well, if we have a set of transcontextual cooperating networks, that means there's value that can transfer between, but they're not direct competitors, and there's some transitivity factor, average transitivity factor, then we can rewrite Metcoff scaling law this way and don't read the math, but it basically gives us down at the bottom a square law scale effect just from the value that is extractable, that is transitive. And even if T is really, really, really small because it's a square law, we get huge value just from cooperation. So, that's how we fight. And you can read the details in this paper below. Just look up meta platforms and cooperative networking network effects. So, the second strategy was retake control of our data. How do we retake control of our data? data. We have certain toolkits for controlling our data. Now, you've heard this thing that says if all you have is a hammer, everything looks like a nail. Well, the truth of the matter is if you have nails, there's different types of nails and different types of hammers work better. So, that's okay. But in this context, usually people use it to say, well, you need to get more tools in your toolbox and not just have hammers. The problem is that an information we only have one set of tools. We can do things with screws and we can use screwdrivers, but hammer is on an option. In fact, there aren't very many options. We have one set of tools for truly secure data control.

That's it. And this gets us back to answering the question because the hard question for data is secure control, right? Information security. So, we want control over value. you. Physical security, that's a solvable problem.

Information security, we continue to have hacks of computing infrastructure. We continue to have the network is not secure. We continue to have, in fact, many of the talks today were about how to how better to achieve informational security in your systems. And it's not a and it appears to not be a well-solved problem.

Well, the solution, the set of tools comes from digital uniqueness. The reason physical security is a solvable problem because we have physical uniqueness of atoms. We do not have physical uniqueness of bits. We need to somehow bootstrap to something that looks like that. That bootstrap, there's only one. It's called informational entropy. It's the only tool we have. It's like the screws in the picture before and the drivers are entropy -derived tools. These are cryptographic one-way functions. You know them as hashes, scalar multiplication, digital signatures, EKPs. That's it. That's all we've got. If we don't know how to use them well, we don't have informational security. If we use them poorly or we use them inadequately or we use them in not best practices, we fail over and over and over again. We have to do this right if we ever want to actually gain control over our data. It's like we're in la-la land if we think otherwise. And unfortunately, many people imagine that there's some magical way to get informational security that doesn't use these tools. So information uniqueness comes from captured entropy. But guess what? Anybody can capture entropy. That makes captured entropy an inherently decentralized tool. So we individuals, participants can take control of our data, but we first must retake control of our identifiers because the identifier control is what the tools give us. We can control our identifiers.

And the type of identifier that allows us to do that are called self-certifying pseudonymous identifiers. And there's a white paper I wrote that talks about the theory of self-certifying pseudonymous identifiers and why they enable us to have true decentralized roots of trust to control over our data. But obviously it's not, it's and you can go look at the paper, but it's beyond the scope of this talk. What that simplifies to are the four A's of secure data control. That's the author, authentic, authorized, and authoritative. Each data item can be imbued with these four A's. So, I call that A4 data control. That establishes that control via self-certifying pseudonymous identifiers of the data and the author and the authorization consent to all of those can be can be put in the data. And so I coined a new term called sapored data. So the term sapored means the quality and substance that affects the sense of taste, savor, flavor. So if we want data that is controllable, we need to sapored the data. And what that means is we can securely provenance the data to its authors. And if we can't securely provenance the data to the authors, we can't securely extract control. That attribution is necessary. And that means that we we build sapored data supply chains that enable consumer pull in addition to regulatory push so that we become conscious consumers of sapored data. So we go back to our diagram. We have the its that control the bits. And now I've got rid of the question mark here because this is cryptographic pseudonymous identifiers. We can control those. We can control those in a decentralized secure way and there's no there are no exploits other than you can protect it with purely key management. That means that we can have control and attribution. So we can control our data and we can get attribution back, which means we can extract value of our own data. And what we want to prevent is correlation between these identifiers and the its. That's the thing that we need to do to get privacy. But if we throw away all of this in order to get privacy, we throw away our ability to extract value and to control our own data. And that's the problem with the regulatory regime. Most regulations are throwing away all of the bits in order to prevent the correlation. They say, oh, you don't want correlation? Get rid of the bits. Then you won't have correlation because there's nothing to correlate. But then you get rid of the value as well. So it's a diseconomic incentive. So what does that mean? Privacy. You have to choose. You can have this kind

of privacy. You're a lone person on an island. Don't interact with anybody or you can have privacy where you interact with people. But if you're alone on the island, it can be strong because you're not disclosing data to anyone.

You're not extracting value from your data. You're just living on your own. If you want to interact, have commercial economic interactions, then the only privacy you can have is weak. And that sounds depressing, but it's not. So what do I mean by strong privacy? It means uncorrelated interactions over unbound in time and space. And I get in these discussions with people who want strong privacy and it's not possible because super aggregators and state actors have effectively unlimited storage and compute capacity. That means eventually all disclosed data, that means not just the third parties, the second parties will be at least statistically correlatable at some time. So all we can have is weak privacy. What does that mean? We can have uncorrelated interactive actions over bounded time and space. That's what we get. That's what we you have to work with.

And when is it weak? When the cost of correlation exceeds the value of correlation of the data, then it will be uncorrelated. Then we'll have weak privacy. So it's an economic privacy. So let's look at the economics of correlation. On this graph, I have a data life cycle. So now is data in the present.

And when I'm looking at predictive value of that data, that's the primary value that aggregators get from aggregating our data is predicting. So, if I look at the blue line, this is the value of correlating my data. Notice that if I can correlate data in the future, like predicted value, it's very valuable. But the older data is, the less predictive it is, the less value it has. The brown graph is about the correlation cost. It's harder to correlate data that's present because it hasn't been shared much. You can keep it close. You can keep it relatively private. You can only share it, disclose it with certain people. Over time, it gets cheaper to correlate because data is correlatable. Now, maybe, you know, some data may just be pretty hard to correlate, but eventually it might become zero. I don't know what this curve looks like. What that means is that where these curve crosses right here tells you something. That tells you where the extractable value is. This is the value that somebody's going to go after. So if you can move this curve by making it a little bit harder to extract, you can reduce the extractable value that increases your privacy because it just won't be extracted because it's not economic. And if you can get more value out of your data, then that changes things too. So let's look at the economics of the decorrelator. That's you. You want your data to be decorrelated, right? So you have a decorrelation value. This is the value of your data when it's decorrelated because then you can extract value from it. But here is your cost to prevent people from extracting value. And guess what? Your costs go up exponentially the older the data is because now you're fighting against the super aggregators and the nation states and they're going to beat you every time. So the only place you can extract value is here. It's in the immediate past and in the future. But this can be a lot of value. And if we do things right, we can move this red curve to the left so that we can extract more value.

But we have to control. We have to be able to control our data or we can't extract our own value. And it depends on the operating regime. Those curves are operating dependent. And this is one of the problems is that when we talk about privacy and correlation, if we're talking about legitimate actors, legitimate economic actors and legitimate political actors, then regulation is a useful tool.

Contracts are a useful tool. But as soon as we're talking about illegitimate actors, illegitimate political actors, neither of those tools work. By definition, they don't keep the rules and illegitimate economic actors don't keep the rules. So if we're in an illegitimate political regime with illegitimate economic actors, the only way we can protect our data is to hide and bribe. We just never disclose our data. So we can't ever get value from it unless we bribe somebody, which means we're not getting very much

value. If we're in a legitimate political regime, but dealing with illegitimate economic actors, we might be able to hide or bribe. And if we're in a, I'm not sure what happens in a with legitimate actors and illegitimate political regime. I guess if they're just honest, then we can do business with them with contracts. If they're dishonest, then they can get away with it because they can, they're an illegitimate political regime, but doesn't enforce the rules or enforces rules that we don't have. If we don't, and the thing is, is if we build privacy preserving mechanisms that aren't recognizing the regime we're operating in, we'll build systems that won't work well.

And often things that work well down here are horrible up here because we can't get value because we're just we're throwing away our value in order to work in this regime. Because in this regime, pretty much the only thing you can do is to hide.

But in this regime, you don't want to hide. You want to extract your value. You just want to extract it securely under your control and protect yourself through contracts and regulation. So when we talk about freedom, freedom is a balancing act.

We have freedom from and freedom to. We have freedom from exploitation, intimidation, censorship. We also need the freedom to extract value of our own to build relationships to build community. The possibility of ratio of our data increases the possibility of censorship. Anonymity is the loss of value from attribution. Fairness requires data attribution. So there's trade-offs between these values of freedom and privacy. And we have to… Regulations and technology has to recognize those trade-offs. So what is a possible solution to those trade-offs?

Well, class-based A4 pseudonymity. It has the ability to have both high degrees of hiding and non-disclosure while still maintaining control and value extraction based on the class. And then we can separate our identifier trust bases so that if we have to hide, we can erase without being commingled with other trust bases that prevent erasure. And KERI allows us to do both of those. And KERI is a future technology that doesn't exist today, but is something that we're building for the future. So, that's the end of my talk.

And I'm sorry I went three minutes over. I can't hear you, Steve. Steve, I can't I can't hear you. Steve, you're on mute for everyone. Nobody can hear you. Yeah, sorry. Sorry. Yeah, my double mute is protecting me from myself.

Sam, I have to say that the that talk was epic and I've early feedback. from people on instant message and LinkedIn suggests that our minds are blown and we maybe should have you gone earlier in the day. But for everybody who likes podcasts, I assure you, Sam has promised me he'll come back and record a podcast with me because for me, that's something I need to play like over again and over again and over again and play it slowly and then play it fast. and take a transcript and it needs a little bit of repetitiveness for it to sink in. Yeah. And I'll post the slide someplace. I'm not, I guess. That was another question. Yep. Yeah. You just tell me where to just send me the link and I'll post them there. You may have already done that, but I just. If you could, you know, just email me a link or, you know, the file, I'll make sure. Yeah. I'll put them up on my GitHub page and then I'll send you a link to them. Awesome. I appreciate it. And I will be following up with you because, you know, Phil has been on a podcast. We've had Drummond, we've had Anne, quite a few folks. Good luck in your new role at Sovereign. I'm going to be watching that and looking forward to chatting again with you soon.

We'll see you next time.