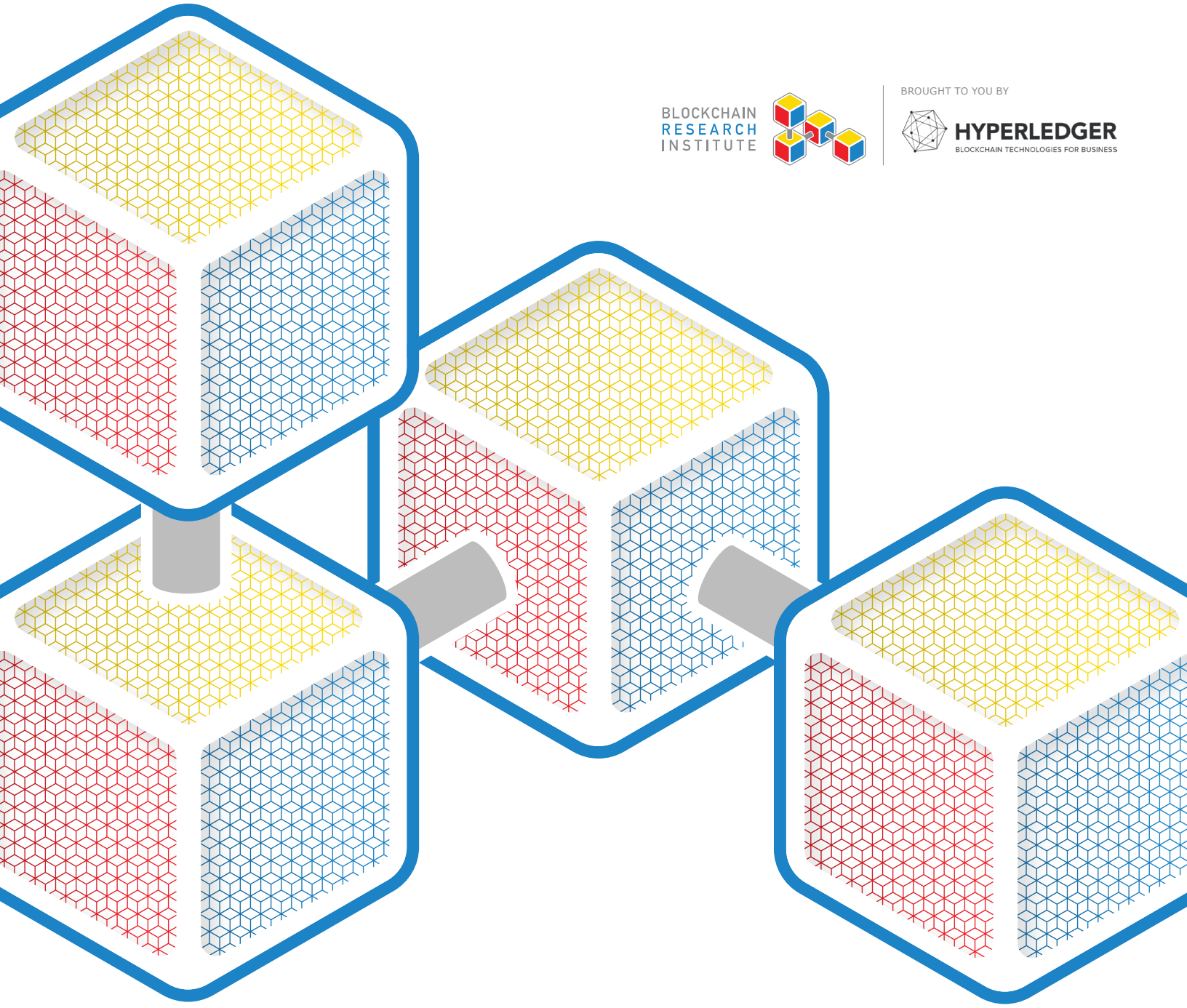
BLOCKCHAIN RESEARCH INSTITUTE

BROUGHT TO YOU BY HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS



BLOCKCHAIN AND THE FUTURE OF DIGITAL IDENTITY

Brian Behlendorf, Linux Foundation

Stephen Curran, Cloud Compass Computing Inc.

Nathan George, Kiva Microfunds

Don Tapscott, Blockchain Research Institute

May 2021

A BLOCKCHAIN RESEARCH INSTITUTE NEW DIRECTIONS FOR GOVERNMENT WEBINAR

Realizing the new promise of the digital economy

In 1994, Don Tapscott coined the phrase, "the digital economy," with his book of that title. It discussed how the Web and the Internet of information would bring important changes in business and society. Today the Internet of value creates profound new possibilities.

In 2017, Don and Alex Tapscott launched the Blockchain Research Institute to help realize the new promise of the digital economy. We research the strategic implications of blockchain technology and produce practical insights to contribute global blockchain knowledge and help our members navigate this revolution.

Our findings, conclusions, and recommendations are initially proprietary to our members and ultimately released to the public in support of our mission. To find out more, please visit www.blockchainresearchinstitute.org.

> Brian Behlendorf, Stephen Curran, and Nathan George, "Blockchain and the Future of Digital Identity," panel moderated by Don Tapscott, *New Directions for Government* webinar series, Blockchain Research Institute and Hyperledger, 11 May 2021.

Contents

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Message from Hyperledger's Executive Director

First, I'd like to thank the Blockchain Research Institute and Don Tapscott for inviting me, and the other panelists for a conversation on the future of digital identity innovation. It is always good to see these types of conversations happening in the community. While decentralized identity technology has already evolved dramatically in just a few years, it's still in the early stages. Discussions like this one are key to continuing to advance a technology that has the potential to bring a new era of personal digital privacy.

Privacy is fundamental in the design and implementation of systems that address digital identity. It is why decentralized identity has gained such traction in the blockchain community. The world is moving toward more self-managed, self-sovereign distributed digital identity, which would be possible without distributed ledger technology. We can get both optionality and interoperability when we weave global identity and credentialing systems together in a decentralized way.

Next, I'd like to point out the value of community discussions like this one. The good faith sharing of expertise is the most direct path to putting applications directly in people's hands. In the pandemic-era we live in today, health and safety are paramount to the everyday experience across industries and borders. Technology is what will help us return to traveling and reopening schools and workplaces in a safe and equitable way.

Development of urgently needed solutions and systems, ranging from education to finance to public health, is happening quickly. Future implementations should work together to solve problems of privacy, ethics, and portability. My hope is that readers will continue to engage in these types of public discussions and help support the growth and adoption of open source identity solutions.

BRIAN BEHLENDORF
Executive Director
Hyperledger
General Manager
Blockchain, Healthcare, and Identity
The Linux Foundation

On 28 April 2020, the Blockchain Research Institute co-hosted a webinar, "The Future of Digital Identity," with Hyperledger. It was the third webinar in our *New Directions for Government* series. Our guests were Brian Behlendorf, general manager for blockchain, healthcare, and identity at the Linux Foundation and executive director of Hyperledger; Stephen Curran, a principal of Cloud Compass Computing and a software developer and DevOps veteran; and Nathan George, senior director of engineering for the protocol team at Kiva Microfunds. Don Tapscott, executive chairman of the Blockchain Research Institute, introduced the topic and moderated the conversation. This is an edited transcript of the proceedings.

Introduction

Don Tapscott Welcome, everyone. Our topic today is digital identity. This is a big deal. If we don't turn back the tide on climate change, then we don't continue to exist as a species. If we don't turn back the tide on the ownership of data, then I don't think we continue to exist as a civilization, because owning our own identities is the foundation of prosperity, of our individual autonomy, privacy, and security, and of our ability as societies to use large scale data in tackling big social problems like pandemics.

Digital identity is bigger than the identification of an individual. It's about the data we create in the digital world that is associated with our identity. It's the data that constitutes a Virtual You. This Virtual You knows more about you than you do, in all kinds of areas, because it remembers everything you do—where you were year ago, what you bought, which medication you took. It remembers dozens of classes of data, all generated by you. But it's captured, stored, and owned by others like Facebook, Google, and other digital conglomerates.

"Digital identity is bigger than the identification of an individual. It's about the data we create in the digital world that is associated with our identity."

DON TAPSCOTT
Executive Chairman
Blockchain Research Institute

Don continued

Through their ownership of data, the top five of these conglomerates represent half the value of Nasdaq 100 and 20 percent of the S&P 500.[1] Clearly, data is the asset class of the digital age.

So, the real problem here is that the Virtual You is not owned by you; it's owned by these entities and governments. The Virtual You isn't held by you; it's stored in siloes around the world. And the Virtual You doesn't work for you; it works for any entity willing to pay the digital conglomerates for big data analytics. You have no ability to monetize your own data, the very data that driving the market cap of these digital conglomerates. Yet you are responsible if the Virtual You is hacked, stolen, or deleted. And the Virtual You runs on centralized servers of which there are two types: those that have been hacked and those that will be hacked.

So, our topic here is, how do we reclaim our digital identities and our data? We're going to introduce the idea of the *self-sovereign identity* (SSI) in practical terms and how we can move to achieve such a thing. Brian, what do you see as the problem, the current approach to our digital identities? And that can include identification or the broader concept of identity.

Our current approach to identity

Brian Behlendorf Thank you, Don. The bigger picture here is, enough of us are sick and tired of the very portal-driven view of how digital identity works, that we are defined by what some other institution knows about us and maintains in its databases.

Think about your Facebook account, your Twitter account, your account at the California Department of Motor Vehicles, or the Internal Revenue Service. All of that puts identity at an arm's length, on the other end of the name and password, which you hope you don't forget, or your e-mail address doesn't become unreachable. Otherwise, you're hosed.

Instead, I think a lot of us want to view identity as an inversion of that, where we hold these signed documents very close to us, as the digital analog of our physical wallet. We're not defined by it, but we're holding documents that are signed, that attest to certain things about us.

"A lot of us want to view identity as an inversion of that [arm's length model], where we hold these signed documents very close to us, as the digital analog of our physical wallet."

BRIAN BEHLENDORF
Executive Director
Hyperledger

That's my driver's license, a signature thing, or a ski pass that indicates I have a right to go skiing at a certain ski resort all winter. Or a diploma or other certificate of educational achievement. These are things we hold in the real world and can show to somebody else. Even if that school goes out of business, we can still present that diploma to others, and they can verify it as a legitimate degree conferred.

We don't have that right now. If Facebook were to disappear—difficult to conceive of now, but we have only to remember AOL, Yahoo, and others to realize that these have a lifespan shorter than the average human lifespan—then maybe these [attestations] should be more indigenous to who we are.[2]

That's the bigger picture of self-sovereign identity, where we've seen a lot of work done in the Hyperledger community—in Hyperledger Indy and Aries, which Stephen and Nathan have played really core roles in helping build.[3] Associated companies like the Trust Over IP Foundation are becoming relevant now, in a world where everyone's focusing on how to reopen, how do we provide proof of vaccination or clear health status to board a plane or to enter a sporting event?[4]

Brian continued Suddenly, digital identity is becoming very real now, and the privacy issues around it are becoming very real. It's a very exciting space to be working in.

Don Tapscott Thank you, Brian. Stephen, as Brian noted, you're a regular contributor to the Hyperledger Indy and Hyperledger Aries communities and a trustee of the Sovrin Foundation, which is driving much of the work around self-sovereign identity. What's the current approach to our identities, and why is that a problem?

Stephen Curran The current approach is this: you ask other people to share data with other people, other entities. Let's say you want to log in to something, and so you ask Facebook to tell the other person who you are. You're in control of it, you're controlling when it happens, but you're actually asking Facebook to tell some other service, "Hey, that's Stephen. Let him in." We're giving that control over. That tells Facebook, "Every time we do anything, add that to Facebook's single database of everything." That's one part of it.

The other part of it is—Brian talked about his driver's license and his ski pass. These are paper things, and they're very simple to forge. As a result, there's not a lot of trust in them. That has all sorts of implications, that there's no trust in the documents you're holding.

"Paper things [are] very simple to forge. As a result, there's not a lot of trust in them. That has all sorts of implications, that there's no trust in the documents you're holding."

STEPHEN CURRAN
Software Development and DevOps Veteran
Cloud Compass Computing Inc.

And so we're trying to take the systems we've used for many years and use them for identity. Until now, we've been doing it using basic technology—scanning documents, taking pictures of them, showing them to people, and counting on them to take their validity. That has a bunch of implications, too, which get into the solutions, and so I'll stop there.

Nathan George If I can add something to that—now that we've reached this digital saturation where everything's interconnected, we're having trouble. Your healthcare data, your vaccination record, doesn't talk to your airline. Your airline data doesn't talk to the government immigration office that needs to let you in. And so, we end up in a situation where either all these systems have to merge or collectively become one, or we have to give the people involved an opportunity to move the data themselves. But that has to happen in the same way that paper credential happens, where when you get the physical credential or

Nathan continued the passport or the vaccination pass, there's some truthiness to it. Your airline can tell that it's legitimate, that it's what your airline is supposed to use.

When we talk about passports, we took forever to get to a standard that worked really well for everybody, and that's probably the simplest use case we have internationally.[5] Then we get drivers' licenses, where there are very good standards. But if I showed you a driver's license from Utah, would you know whether it was a legitimate Utah driver's license?

The hope is that we can get to where—all the way out at the edge, even for things like your social contacts or the individual line items in your résumé—when someone sees these things, they can get a sense of whether they're true. It doesn't have to come from Facebook, it doesn't have to come from your university, for someone to know it's true. You can share it with them, and they can look at it and go, "Yes, that's a legitimate university degree, that makes sense."

"The hope is that we can get to where—even for things like your social contacts or the individual line items in your résumé—when someone sees these things, they can get a sense of whether they're true."

NATHAN GEORGE
Senior Director of Engineering
Protocol Team
Kiva Microfunds

Don Tapscott To your point, Nathan, that we can't link our data, say, in a pandemic, because it's all locked in individual healthcare systems. We're not able to aggregate our data across all these siloes, for epidemiologists and government planners to analyze and to take action.

How identity differs from identification

Don continued Let's explore this idea between identification, who you are, and the broader issue of identity, what you are, how your health is, what transactions you do, what your location is, and so on. I know it's a continuum, but they're different topics in some ways.

Brian Behlendorf From a human rights point of view—which is a frame that I think we should really root ourselves in—from a humanist point of view, you are not defined by what other administrations or other organizations say you are or say about you.[6] This has been a big realization in activist circles, ever since Facebook introduced its real names policy.[7]

Drop a Comment for Full Document

SHARE
DOC
VIEW®

Free Signup at ShareDocView.com