Distributed Reflections

The Future of Blockchain Identity

Identities are reflections of our past interactions, present attributes, and future agreements. Blockchain technology collects visions of self and directs them toward those whom we trust. The future of identity rests upon these distributed reflections. Blockchains allow anyone in the world to share and store information that can't be erased. This information builds on past events as time moves on. We will use this permanence and chronological history to track our ongoing interactions and prove them to future collaborators. Through open-access software, we will own and manage our identities for ourselves, in some cases without involvement from traditional record-keeping authorities.

Along the way, we will question the basic nature of identity itself. Some argue that identity is a unique name that anchors our belonging. Others argue it is the contextual activities and memories associated with this name that let us piece together a whole self. Either way, sharing names and memories with others directly, rather than through silos of authority marks a departure from the past. It offers an opportunity to re-engineer our systems of trust from the ground up for inclusivity and self-sovereignty.

We will open up opportunities for Wall Street bankers and refugee migrants alike to establish their own statements of worth. They will gather testimonials from those around them. New players will emerge, as the power to vouch for others moves from institutions to everyday people.

Some will use blockchain architectures to construct societies that never forget, and hold records in perpetuity. Others will embrace ephemerality, and provide tools to limit personal identity access to its bare minimum. Citizens will create and control thousands of identities at a time, combining identity fragments to share purpose-built personas as reflections of themselves. Each decision point will transform trust and empowerment for millions globally.

> **"We can be free individuals in the digital world."**
>
> **Christian Lundkvist**

INSTITUTE FOR THE FUTURE

BLOCKCHAIN FUTURES LAB

201 Hamilton Avenue
Palo Alto, CA 94301
www.iftf.org

Rebooting Identity

expert voices

Identity is in crisis. Individuals have little ownership or control of the information they use many times a day to prove who they are, what they are authorized to do, what they are entitled to receive or access, or where they are allowed to go. Identity records on centralized databases give the database owners the power to correlate and surveil people's purchases, travel, Internet use, and other activities without their consent. But when identity records are created by individuals and stored on a distributed blockchain, the individuals are in control of who gets to see their information, and what kinds of information they choose to disclose. We asked four experts about the future of blockchain identity, and how it could help move us beyond current tensions around identification.

Christopher Allen is the principal architect of Blockstream, a blockchain technology company. He previously co-authored the TLS security standard. He's an entrepreneur, technologist, and pioneer in internet cryptography.

Christian Lundkvist is the creator and chief architect of uPort, a self-sovereign identity and key management platform. He's a mathematician, quantitative analyst, blockchain engineer, and cryptocurrency enthusiast.

Justin Newton is the CEO and founder of the digital identity startup Netki. He founded ISPC, the first trade association for internet providers and served on the Advisory Council for the American Registry for Internet Numbers (ARIN).

Ryan Shea is the founder of Blockstack, which is a new decentralized internet and a platform for serverless applications where users own their data. He was inducted into the Forbes 30 Under 30 and graduated from Princeton University, where he studied Computer Science and Mechanical and Aerospace Engineering.

Remembering the Forgotten

Today, 1.5 billion people have no verifiable identity, which shuts them off from modern services that could help them. Blockchain technology will allow them to access networks that will connect them with the resources they need to improve their lives.

Q Why doesn't everybody have an identity already?

Newton: The first step to onboarding yourself into the identity ecosystem is to get validated that you exist by some power structure, most likely the government. In many countries, that first step actually doesn't happen for many people. As a result, it creates a hurdle to building durable identity that can be used for things like getting benefits or getting an education.

Q How will people go about establishing digital identity in 2026?

Newton: There would probably be a mobile phone app that allows parents to create a new record for a newborn child, basically a new identity on the blockchain. In the beginning, the parents will enter the data—things like gender, birthdate, and birth time. Some of those attributes will then get attested to their parents, as well as hospital officials. In time, they'll enter health and immunization records, and school registration. You'll have control both over what gets written into your identity locker and anything that's stored in it, as well as who it gets shared with.

Q How could the government still play a role in blockchain identity?

Lundkvist: The government can give an attestation in the form of a cryptographic proof that you are a citizen of a specific country. Once you have that attestation, you can participate in the activities of that nation on a digital level.

Reclaiming Ownership

Today, we outsource our identities to companies and central authorities who may not share our best interests. We'll use blockchain technology to give individuals new ways to establish "self-sovereign identities."

Q What's the problem with identity as it stands?

Shea: We outsource our identities to other people and to other companies. What that means is that when you do anything on the Internet, you are who you say you are not because you are presenting yourself, but because someone is vouching for you.

Q What's wrong with outsourcing the custodianship of our identity to a central authority that knows what it's doing?

Newton: When Google, Facebook, Microsoft, or some other large corporation controls your digital identity, you become dependent on that company and that company's long-term goodwill in terms of how, where, and what about your identity is shared. If you upset Google, Facebook, or Microsoft you'll lose access to other platforms that use the credentials they provide for you.

Allen: Because it has led to a slow erosion of rights over the last couple of decades. As our lives become increasingly digitally entwined, compromises we made a long time ago are beginning to haunt us. When you go to a new website that collects personal information about you, a lot of it gets captured without your permission—through cookies, correlation, and things of that nature.

Q What concerns should large organizations have about blockchain identity?

Newton: Let's say I'm a bank and I'm going to trust someone else to do validation of a user that's onboarding onto my system for anti money-laundering purposes. I'm going to want to make sure that they're willing to take on the liability if there was an error in that validation. Otherwise, I'm going to want to do it myself. That's a non-technology piece of the puzzle that needs to get solved.

Q What is a self-sovereign identity and what are the advantages?

Lundkvist: A centralized identity provider is someone with more power than you and bestows your identity on you, but in the self-sovereign case the individual is actually the source of the agency.

Shea: This digital identity artifact is the digital proxy for you. You have control over it because you hold this digital key.

Lundkvist: You can choose to have some of your identity be public and some be private. You own your digital identity and have ultimate agency with it and also the corresponding data that belongs to it. Services you transact with won't already have copy of the identity data they need. Instead, they would have to ask you for permission to access your data and you would be able to grant these permissions granularly.

Newton: You'll be able to have fine-grained attestations. Not just "this person is Alex" but "this person is over 21," and an attestation from your educator saying "this person has this degree on this date," and an attestation from your health insurance company that says "you carry this kind of health insurance that's good through the state," and an attestation from your apartment complex that says that "you can open the front door."

Redefining Selfhood

Today, identity is based on biometrics and birth records, which can be forged and compromised. The unique affordances of the blockchain will lead to a new, and more useful, definition of identity.

Q What makes blockchain technology well suited for identity?

Shea: If you have timestamps and signatures, you can do pretty much everything. Timestamps give you "when" and signatures give you "who." The data that you're signing gives you "what." You get the continuity of an entity through time. We have that in the real world with the physical characteristics and the behaviors of a person or thing. In the digital world, it turns out that we can do the same thing if we have a blockchain. As more and more blocks sit on top of that block, the likelihood that that information can be removed diminishes extremely rapidly.

Q How would you use a digital identity in 2026?

Newton: I show up at a bar and, instead of having to show my full ID that discloses everything about me on it, I show them my digital wallet and it flashes up a photo and the fact that I'm over 21, and no other information. Or, I'm crossing the border from the US into the UK. Instead of using my physical passport, I pull out my digital wallet and I show my attestation from the US government that I'm a US citizen. Then the UK government digitally signs a visa that says I can stay in the country for 90 days. Now, any time I see authorities, I can show them something that says I can still be in the country and what I can do there.

Reducing Abuse

Today, identity theft affects over 13 million people yearly in the US alone, with $15 billion stolen. Centralized identity provider silos are data honeypots for hackers because they contain thousands or millions of users' information (the identities of people, things, entities, organizations). Users are at the mercy of the least secure database that has their information. Blockchain-based identity will make it much more difficult for identity thieves and other bad actors to ply their trade.

Q What are the risks of keeping information in a centralized identity provider's susceptible database?

Lundkvist: If they don't have a good overall security plan then you run the risk of them losing your data.

Shea: A lot of times, depending on how the system is built, its information gets inevitably hacked. It has a lot of central points of failure. It's not a question of if, but rather when. Because of the way that a lot of these systems are designed, the hacked information can be used to impersonate you as well. This results in things like identity theft. There's a lot of costs of cleaning up the mess when things go wrong.

Q Are there new security or societal problems that could come about from blockchain identities?

Allen: Any personal identifiable information on a permanent, immutable ledger is a risk.

Newton: It's really important to think about how we ensure that any data that could potentially be used against a user is stored in a way that that gives the user sole access and control for a period of time that's equal to their lifetime. Anything that you're writing to a blockchain is only protected from exposure by encryption. So far, there has never been an encryption created that's lasted a human lifetime. It either obsoletes because in ten years processors get faster, or it obsoletes tomorrow because someone put a semicolon in the wrong place.

Allen: It could cause huge abuses in piracy.

Lundkvist: The easiest way of implementing this thing is that you have an identifier on the blockchain. Then you use that same identifier to log into all kinds of systems. If they share data between them through ad networks or what have you, then your activity is correlated throughout all these sites. How do you avoid correlating identities while still avoiding this silo effect of each site having its own identity?

Allen: It allows for the very rich to do things behind the public's back that are not fair.

Q What is the security benefit of being able to prove that a statement is true while not revealing any details about that statement?

Lundkvist: For instance, imagine you want to prove you are an accredited investor, but you don't want to reveal your exact income. You could use a zero knowledge proof to prove something like, "Okay, my bank account has more that $250,000 in it" without revealing exactly how much money you had in the bank account.

BUILDING BLOCKS

We can understand the future of identity through the four building blocks shown here. Each block plays a crucial role, both in redefining identity as we understand it and in giving it unprecedented agency. Blockchain technology will allow entities to establish their first **ADDRESS**. It will allow them to **ATTEST** for each other's actions. It will give them a means to **OBSCURE** data for privacy's sake. And it will **VALIDATE** the other entities it interacts with.

ADDRESS

Blockchain identity begins with a unique and persistent address. This is the solid foundation for all other aspects of identity.

Open-access blockchain systems like Bitcoin allow any user to spin up new addresses for themselves. By using a digital wallet on their computer, they generate a pair of keys, one public, and the other private. The public key is a shared address so others can send messages and value to the user. The second, a private key, is kept by the user, and can be combined with the public key to signify consent and ownership when authorizing transactions.

With ownership comes responsibility. Users are ultimately in control of the keys to their identity. When these keys become necessary to interact with critical services throughout one's lifetime, loss or mismanagement of credentials will be akin to forgetting the combination to an unbreakable safe that holds your assets.

Some will trust third-party online services to hold pieces of their identity. Projects like Consensys' uPort will provide a way for people to revoke and recover their identity through rituals of social network approval. Others will opt to control their own physical hardware wallets and personally-run software. They will sign messages through implanted devices and smart objects.

Users can create addresses at their will and establish an identity for themselves digitally, without the need for formal institutional support. Previously disenfranchised groups without government-issued identities will create their first identities and use them to work toward worldwide recognition and inclusion.

Citizens who have always benefitted from the privilege of identity will find new ways to break their personal information down into independent identity fragments for privacy and controlled, flexible sharing. Some may even come to sell their addresses on open markets, both for illicit coordinated efforts and legitimate transitions of power.

Organizations will adopt proven addresses in a new form of incorporation, and share these trackers with partners and governance bodies so they can audit the organization's on-chain activity. Consumers demanding supply chain accountability will pressure retailers to provide trackable incorporation addresses from upstream providers.

Accounts won't be limited to humans and organizations. Physical objects and algorithmic agents can be given an address and private key as well. An explosion of persistent addresses will give rise to high-resolution accountability and distributed control. The range of possibilities for building atop these addresses is near infinite.

ATTEST

Blockchain systems will let us point to pieces of our past to prove our qualifications and dependability in the present.

Once identities have been established with root addresses, users will accumulate provable attestations from their interactions with others. Users can self-attest to any statement permanently, but will augment these claims by gathering additional stamps of approval digitally signed by an increasingly broad range of institutional and non-institutional sources of authority.

With open ledgers that allow permissionless participation, anyone can post attestations, negative and positive, whether they are right or wrong. Thus, attestations will include evidence and links to external off-chain events to bolster their believability. In the absence of on-chain references, potential collaborators will rely upon human and machine "oracles" to provide their informed best assessment of a situation or condition. Oracles will maintain reputation within their communities based on their objectivity and accuracy.

Over time, attestations for one party may be passed on through others to establish a wide-reaching "web of trust." This term, borrowed from early 1990s PGP encryption communities, describes a way that accounts can sign off on others, extending the initial user's access and validation beyond their initial sphere. Soon, social graph analysis may make trust probabilistic, rather than cut-and-dried based on affiliations. People will measure their degree of trust with others based on community trust metrics.

These metrics will be constructed to demonstrate not just transactional reliability, but also personal achievement. Blockchain attestations will emulate and, in some cases, obsolete existing forms of credentialing. Since anyone can attest, this means credentials can be constructed and shared by friends and mentors as easily as employers or traditional universities. It means drivers can attest for their riders and vice versa to create a robust, Uber-like reputation system. It means criminal histories can be vouched for by a state or by members in a village, with equal robustness.

For businesses, this means brands and the certifications associated with them will be based on attestations by consumer protection groups, supplier collectives, and customers. This is a double-edged sword, as those with credible counter-attestations may just as easily post their grievances against a brand for all to see. Activist organizations, governments, and philanthropic efforts will be placed under comparable scrutiny as they are audited by their beneficiaries.

Machines will break from the control of branded organizations and owners, and work to build reputation themselves as autonomous equals. In public key infrastructures of the present, digital certificate authorities bestow marks of approval upon devices to grant them inclusion in networks of trust. Soon, robots will prove themselves without these centralized gate keepers, earning attestations as they take on gigs from other machines and people. They too will have resumes and develop reputation with their peers.

Overall, there is a key tension between completeness of attestations associated with a single identity (the status quo for state-controlled identities) and the ability to spin up entirely new identities based on context. Ultimately, users have the ability to present attestations and correlate isolated profiles as they wish in response to demands from counterparties.

We won't expect inhabitants of a decentralized world to trust our online identity. We will prove it ourselves with shared memories.

OBSCURE

Obfuscation and anonymizing technologies will protect people transacting on blockchains from growing powers of surveillance and censorship.

In the near-term, enforcement agencies and companies operating under legacy structures will struggle and barter to de-anonymize potential customers and bad actors. Over time, trust-minimizing blockchain systems will render certain aspects of identity unnecessary by establishing rules for execution at the protocol layer, rather than the human application layer.

In most blockchain systems, a user is neither anonymous nor fully certified. Rather, they are pseudonymous, known only by their public address until they elect to associate this address with information about themselves. The information itself can be encrypted and stored for its intended recipient without fear of prying eyes. Further secrecy is derived from hierarchical deterministic wallets, which use a single, secret seed to create a brand new address for each and every transaction. All of this comes together to afford users the option of selective disclosure, sharing identity information through a series of isolated accounts on or off-chain, on an as-needed contextual basis.

Even without personally identifying information, qualities about the account (such as currency balances, reputation metrics, and valid addresses) may be entirely sufficient for peers to interact. Individuals who might otherwise be excluded from high-trust services like credit or corporate governance will soon participate pseudonymously or anonymously alongside established and publicly-known citizens. Sharing portions of identity only as needed for a given interaction means counterparties can focus on risk factors, and prevent their own bias against otherwise capable populations that wish to interact with them.

Obfuscation doesn't just benefit those operating on the margins and in the shadows. Large organizations will lead the way in obfuscation techniques that prevent competitors and malicious hackers from accessing ongoing operational logs. Ongoing supplier relationships, customer data, medical information and more will flow through dark internet tunnels.

The most advanced of these technologies edge toward total anonymity by relying upon a cryptographic scheme known as a "zero-knowledge proof." It allows one user to prove a statement is true to another user without actually revealing the underlying data. This means a bar patron could prove they were above the age of 21 without ever revealing their true age. It means a financial exchange could prove their solvency without revealing any account balances or overall holdings information. It means a low-income patient can prove they are eligible for medicaid support without revealing the details of their pregnancy.

As a result, new anonymized cash systems like Zcash, Monero, and DASH have come to advance the pseudonymous nature of Bitcoin toward full anonymity. We will soon see this extend to all kinds of proofs, including the ability to prove career achievements, educational certifications, belonging in a group, business licenses, car ownership, and more.

The precedent set by these blockchain experiments will inspire future platforms that maximize functionality with minimal personal data storage.

VALIDATE

Blockchains will support human intuition and rigid algorithmic specification when validating claims and assigning rights.

Aided by algorithmic data visualizations, blockchain users will scrape numerous immutable databases to surface claims and judge trustworthiness. Distributed communities will determine membership based on validated criteria, disenfranchising those unable to provide sufficient qualification data.

Institutions are testing new membership-based blockchains that prevent reading or writing without being whitelisted first. These networks, known as "private," "permissioned," or "federated" blockchains control access to their systems by validating the organizational identity of the participant. The goal is to limit reading or writing of industry information to the general public, as public blockchains allow by design. We will see an explosion of such permissioned chains, each with their own rules for validating entries and users. They may interact with private and public systems through cross-chain links, or isolate themselves completely.

Both private and public chains will allow organizations and individuals to connect with others under specified terms based on their attested qualities and hard-coded interaction parameters. Smart contract AIs will be formed to serve as brokers between parties that may otherwise not have the means of finding each other or ensuring the other is capable of trade.

At the personal level, claim validation will shape the way people make decisions as they go through their day. Though the average individual is unlikely to parse and analyze terabytes of publicly logged information, they will rely upon validation mavens and ready-made chatbot AI decision assistants to help them. These will help people remain informed about the products they buy, the issues they vote on, and the people they work with. Shoppers may see products disappear from their augmented reality displays when they come into conflict with their ethical or investment filters.

This information and associated digital services will flow through a radically decentralized Internet, where all files are validated as being complete and trustworthy without a central intermediary. Developers will advance the work of peer-to-peer torrent technology developers, creating systems that collect files from other computers by querying a file by name, rather than querying a specific computer's IP address for a file and trusting it is what the user wanted. This will radically transform centralized domain name systems, placing content and its providers' names on the blockchain for people to find themselves.

Law enforcement and regulation will attempt to mandate the inclusion of validation parameters for applications and corporate smart contracts wherever possible. They will audit records of approved business transactions, and cut off access to those found to support criminal activity. Criminals themselves will be immutably marked within the systems in which they transgressed. This will prevent them from accessing community resources, assuming these communities have chosen to validate based on city, state, or national watch list criteria.

"Trust but verify" will not be sufficient in a blockchain world. People will validate qualifications from the very beginning of an economic partnership or community initiation.

pbs.twimg.com

BitNation is prototyping a process for establishing a global passport.
bitnation.co

Global Citizens

Government IDs are the critical passport to government protections and social services, as well as financial tools like credit cards or even bank accounts or health records. Yet today, one-fifth of all people on the planet have no formal identity, and the other four-fifths are restricted to national identities.

Over the next decade, blockchain addresses will increasingly stand in for government IDs. Individuals, sometimes working with passport identity services, will use open-source encryption protocols and blockchain tools to claim the root addresses they need to create global, persistent, self-sovereign identities that are not limited or regulated by traditional geographic boundaries. As blockchain trade grows, these borderless identities will challenge the way we think about everything from global trade agreements to worker benefits and citizen rights.

Provenance helps artisan food brands attest product origins and authenticity through stories of custody
provenance.org

Crowd-Attested Brands

Brands are a form of identity—the reputation of a product, service, organization, or idea. With the emergence of social media, marketing organizations have learned to relinquish some of the control over brand reputation to the public with limited ratings and reviews. But on the blockchain, crowd-attesting may be the future of the brand.

Brands will build trust by their actions, which will be visible as documented transactions on the blockchain. Their reputations will be built on what they do, what supply chains they are part of, how they interact with communities of people and objects. But they will also be built on what others attest to—that is, claims made on the blockchain—which no one will be able to censor. Over the next decade, brands will increasingly "make deals" with the crowd of blockchain profiles, encouraging people, things, and code to use the brand as part of their individual identities in a mutual exchange of attestations. Ultimately, as AI and corporate smart contracts converge, brands may become a new kind of independent actor on the blockchain.

bitcoinmagazine.com

Zcash uses zero-knowledge proofs to hide the sender, recipient, and value of all transactions on the blockchain
z.cash

Prosthetic Identities

As traditional Bitcoin-style wallets give way to hierarchical deterministic wallets and zero-knowledge proof protocols, people will configure multiple identities to serve specific purposes. For example, a mother of three might create a partial identity to manage her transactions with schools and the children's doctor, and another that features her competencies as a jazz musician to book gigs and sell MP3s. We can think of these multiple partial identities as prosthetic identities that keep various components of one's identity separate but verifiable to access resources and assistance.

As the next decade unfolds, organizations will struggle to assemble small bits of information that are available from verifiable transactions with these prosthetic identities. The algorithmic analytics of today will give way to new strategies for compiling targeted profiles of consumers and criminals alike. One strategy may be for organizations to create their own prosthetic identities designed to attract their target profiles without revealing themselves. Of course, some of their targets may also create prosthetic identities specifically to manipulate these attractor identities for their own needs, nefarious or otherwise.

s3.amazonaws.com

Blockstream creates sidechains, connecting private-access ledgers with public ledgers
blockstream.com

Virtual Gated Communities

Although pioneers of early cryptocurrencies envisioned open and transparent infrastructure, federated blockchains are emerging to support organizations in need of data privacy and access control. Over the coming decade, these private blockchains will create robust networks for cross-institutional data flows. These will effectively form virtual gated communities of exchange, where access to certain kinds of assets and data flows are only visible and usable by members on an invitation-only basis.

Validation in such communities will begin with participant identity checks designed to ensure both the qualifications of the members and the privacy of the community as a whole. Nested gatekeeper functions will validate and provide a buffer between groups. Critical gateways known will form between federated blockchains known as "sidechains" and larger open-blockchain infrastructure. Validation can easily fail if the larger public blockchain is not rigorously synchronized with transactions on the private ledger, or if the private ledger itself is not sufficiently decentralized. In the end, the value of these virtual gated communities may be self-limiting in the same way that such isolated communities are in the physical world.

images.solecollector.com

Chronicled registers sneakers on blockchains with smart tags that can be tracked via a mobile phone app
chronicled.com

Digital Animism

The Internet of Things is rapidly onboarding physical objects, while smart contracts are turning code into autonomous software objects on the blockchain. The protocols for assigning blockchain addresses to these non-human objects are taking shape, and these addresses will be the seeds of complex evolving identities. As they evolve, the distinctions among humans, physical objects, and smart contracts on the blockchain will blur.

Once objects acquire identities, they will also acquire economic and even citizenship rights. They will earn reputations and responsibilities, including voting. In the global marketplace, it will be impossible to tell whether an economic agent is a human or an object acting like a person. In the world of education, smart contracts and even physical objects will earn credentials specifically designed for these new categories of learners. In the world of law, trees, rivers, buildings, and storm drains will perhaps begin to negotiate their own settlements. This is the future of digital animism that the blockchain is already beginning to enable.

ryxwalk.files.wordpress.com

ADEPT is an early prototype by IBM and Samsung for secure transactions and communication between IoT devices.
slideshare.net

Machine Webs of Trust

In the 1990s, encryption experts hosted in-person key signing parties to vouch for each other's digital identities, forming a mutual web of trust. Participants digitally signed a certificate containing the public key and the owner's name, attesting that the owner is who he or she claims to be, thus linking the digital reality to the physical reality.

Over the next decade, machines will use a similar model to assure the binding between digital records and the physical identity of the machine. As machines join the blockchain, they will increasingly be built with hard-coded conditions designed to ensure that other machines aren't duping them. They will receive attestations from other machines (and people), verifying that past transactions have met the hard-coded conditions. Like the 1990s version of webs of trust, these machine webs of trust will evolve and grow as more machines trust and are trusted, allowing machines that have never interacted in the past to engage in trusted transactions with an ever wider web of machines.

techcrunch.com

ShoCard mobile app generates a Single Travel Token without revealing all the documents behind a user's travel identity
shocard.com

Minimum Viable Identities

Today's CRM systems are already showing signs of failure in the shifting fitness landscape of ubiquitous digital transactions. Toxic data breaches are becoming increasingly frequent and difficult to block, and customers are slowly adopting personal data management tools and privacy-protecting proof systems. To avoid liability for data breaches they can't control or suits for misuse of personal information, companies will begin to limit the personal data they hold.

The result will be the emergence of norms and standards for minimum viable identities. Think of these as guidelines for digital services (in this case case the services of HD wallets) that assess the context of a proposed transaction and assemble the minimum information necessary to secure that transaction. Any information needed for customization of transactions—for example, to apply a discount to a price based on customer loyalty—will be brokered by smart contracts that set the terms of access and typically obscure the large amount of data behind the Yes/No recommendation.

ether.press

IPFS creates file and server addresses to route traffic so peers can reliably find and validate sites
ipfs.io

Decentralized File Validation

The Internet is broken. It's subject to hacking, manipulation, and censorship, including the core infrastructure of Internet domain names. Much of this is due to the fact that individual computers are responsible for passing on information, leaving them vulnerable as targets.

New blockchain-based file and information routing systems aim to change this. Projects like the Inter-Planetary File System (IPFS) and a complimentary blockchain-based naming service called Namecoin break down domain name systems and legacy HTTPS models to enable validated file sharing worldwide. This means people can ensure that the records and services they ask for from the network are exactly what they'll receive, no matter who delivers them in the end. Additionally, this allows archiving of historical information, which can be broken apart and distributed across people, with validated re-construction methods to gather them. Ultimately, our browsers and devices will act like powerful magnets for the digital resources we need from each other, whether from across the world or within small rural communities.

Anticipating Identity Shifts

To design for our preferred futures, we must engage with the implications of radically decentralized blockchain identity. The following four are just the start. What will these shifts mean for you, your organizations and communities, and society as a whole?

From people **to peronas**

Personal identities are no longer shared as a whole with services and institutions. Rather, fragmented personas and their associated interactions are what users engage with on a global blockchain.

- How might you serve people differently if you could only identify them from their actions or segmented profiles, and not their underlying biological identity?
- How might we create massively connected identity structures while protecting user control?

From brand certifications **to attestation filters**

Any organization or person can make immutable claims on blockchain systems, and back them up with claims from others and data logs. Brands and advertisements will give way to trusted attestation links. Rent-seeking markets for earning attestations will rise, but users will cut through vouching bloat by following new trust authorities.

- How might you prove the provenance and integrity of your operations through blockchain records?
- How might certifications for achievements and production standards move toward interoperable and transparent industry validation metrics?

From service gatekeepers **to identified resource pools**

Identities attached to objects, data, smart contract applications, and more will allow people to identify their availability within local communities. This will augment the broader sharing economy through real-time transaction and inventory tracking.

- How might your organization track assets, data, and capabilities, and make these available on trusted public systems?
- How might a decentralized Internet impact global access to web resources and information security?

From identity theft **to criminal smart contracts**

Because smart contracts are self-executing, tamper-resistant, and don't require an intermediary to oversee compliance, they'll be used for countless legitimate applications—financial transactions, insurance claim processing, wills, prediction markets, and more. For the same reasons, smart contracts will also be used by bad actors to facilitate crimes.

- Decentralized smart contract systems have the same level of pseudonymity as the cryptocurrency that drives them. How will your organization manage the risks associated with this aspect of blockchain identity?
- Bad actors could conceivably create "criminal smart contracts" to launder money, steal private cryptographic keys, leak information, demand ransom, order the assassination of public figures, and commit other crimes, both online and in the physical world. How can the unique affordances of smart contracts be retained while preventing criminals from abusing them?

INSTITUTE FOR THE FUTURE

Institute for the Future is an independent, nonprofit strategic research group celebrating over 48 years of forecasting experience. The core of our work is identifying emerging trends and discontinuities that will transform global society and the global marketplace. We provide our members with insights into business strategy, design process, innovation, and social dilemmas. Our research generates the foresight needed to create insights that lead to action and spans a broad territory of deeply transformative trends, from health and health care to technology, the workplace, learning, and human identity. The Institute for the Future is based in Palo Alto, California. **www.iftf.org**

BLOCKCHAIN FUTURES LAB

IFTF's Blockchain Futures Lab connects industry leaders with practical visionaries and domain experts to identify long-term opportunities and design considerations for blockchain technology. The Blockchain Futures Lab provides a community forum to discuss paths toward a more efficient, transparent, and equitable world using the full potential of distributed systems. **www.iftf.org/blockchainfutureslab**