

MAP OF THE DECADE 2017–2027

BLOCKCHAIN FUTURES

Reshaping the world at the
intersection of money, technology,
and human identity

Over the coming decade, audacious blockchain experiments will reshape the way we think about everything from cash to computing, from identity to governance. Starting from today's cryptocurrencies, these experiments will build on the unique affordances of blockchain architectures to create radical zones of transformation. They will catalyze—and be catalyzed by—advances in artificial intelligence, virtual reality, and the Internet of Things. These chain reactions will coalesce to create a global infrastructure for trusted computing that will touch every sector, every market, every household.

This map of the coming blockchain decade is an at-a-glance view of this rapidly unfolding infrastructure.



BLOCKCHAIN
FUTURES LAB

A BLOCKCHAIN DECADE

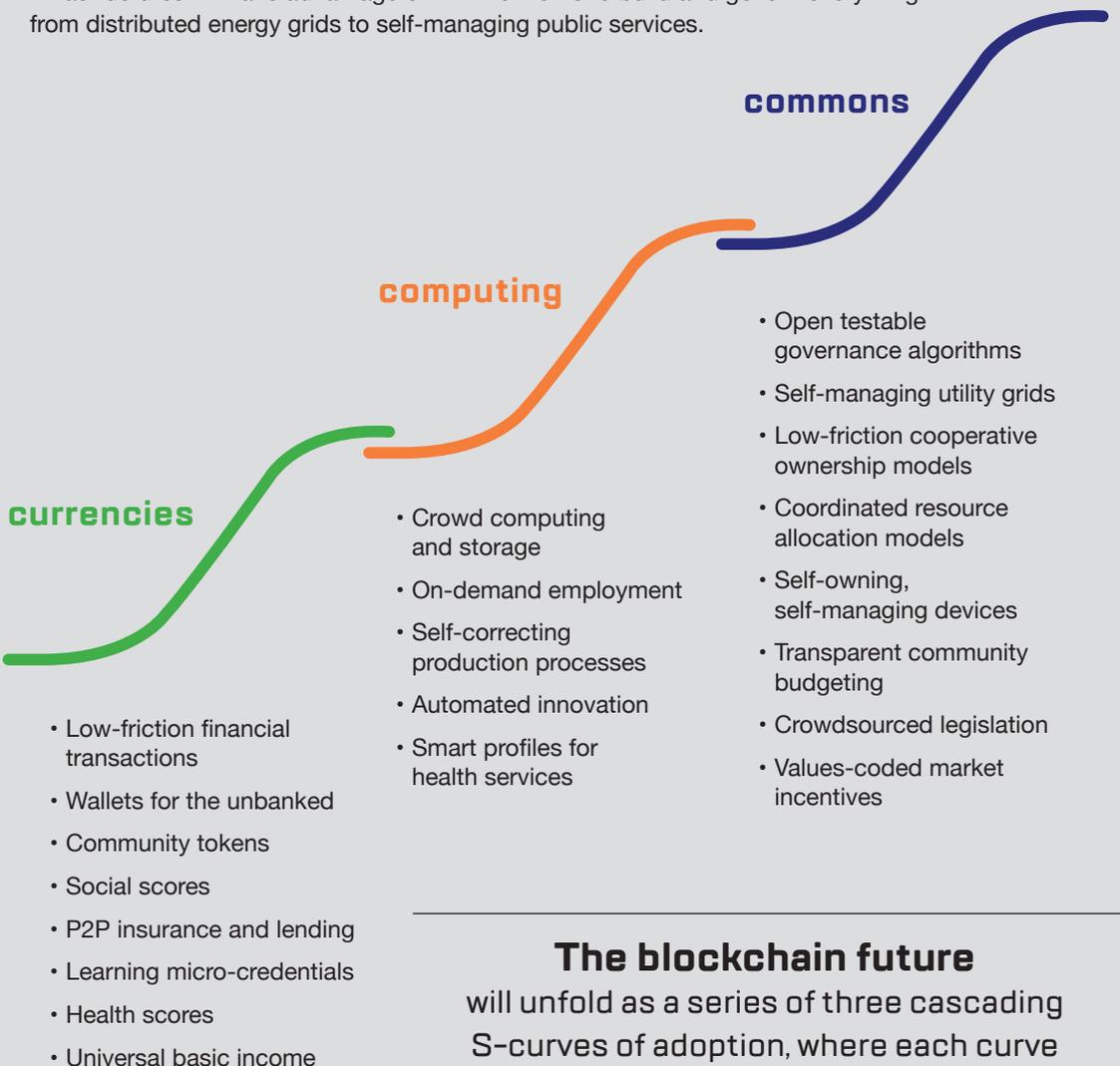
From currencies to computing to commons

Blockchain infrastructure will unfold over the next decade in three phases of transformation, from new currencies to new computing infrastructures to new ways of managing all kinds of commons.

The first phase, the phase of currency innovations, is well underway. Even as cryptocurrencies and shared ledgers create more flexible alternatives for handling all kinds of financial transactions within and across institutions, communities, and nation-states, wide-ranging experiments are underway to tokenize non-financial value exchanges. Identity, information, ideology, and strategy will all take advantage of crypto-tokens to reweave the fabric of our economy and society.

The second phase of the blockchain transformation is the buildout of trusted distributed computing. As smart contracts insinuate themselves into blockchain transactions, they will form the basis of what is, in effect, a distributed, protocol-based global computer, eventually displacing today's platform-based cloud computing. They will control the execution of blockchain transactions using immutable code that tracks the state of every exchange, everywhere in the world, at any given point in time. This is called *stateful computing*, and it will be the secure foundation of a truly automated, intelligent future.

The result of the first two phases will be a new model for managing not just information commons but also physical commons. As the Internet of Things is connected to the blockchain via smart contracts—and tokens control the flow of value through it—crowdsourced infrastructures will take advantage of P2P networks to build and govern everything from distributed energy grids to self-managing public services.



A CHAIN OF NEW AFFORDANCES



SIGNATURES | identity

Blockchain users authorize and receive transactions with any number of unique cryptographic public/private key pairs. Paradoxically, keys generate pseudonymous addresses and signatures that can either keep users private or can be de-anonymized to track a user's every action. Signatures will come to show consent and signify parts of a whole identity.



CRYPTOCURRENCIES | assets

Cryptocurrencies are a form of digital money created and transferred through blockchains. The rules for their creation and transfer are coded into the blockchain software itself. Cryptocurrencies can be irrevocably transferred anywhere with Internet access and can be pegged to larger off-chain assets like financial securities or car titles. Coins or tokens serve as measures of different kinds of wealth, from monetary to reputation.



DATA FINGERPRINTS | integrity

Every blockchain transaction has a small space for digital messages that can be locked in the ongoing chain so they cannot be erased. Using cryptographic hashes, people will store "fingerprints" of much larger documents to create a record of their existence and original integrity. New blockchains will be purpose-built for distributed, trusted peer-to-peer file storage and verification.



LEDGERS | provenance

Generally, blockchains create a sequential history of data that is signed by users. Blockchains won't just track the history of ownership for cryptocurrencies. They will track many kinds of records for establishing provenance, including supply chain custody, hardware authenticity, medical procedures, learning achievements, reputation metrics, and more. Organizations, regulators, customers, and advocacy groups will scour immutable ledgers to inform real-time decisions and interventions.



SMART CONTRACTS | computing

Smart contracts are ownerless blockchain accounts with user-defined, machine-readable instructions on how to redirect funds or store and compute data. They can act as trusted algorithmic third parties between economic agents under conditions of mutual distrust. Smart contracts will interact with other smart contracts, forming powerful computation-driven coordination systems capable of replicating human organizational activities.



OPEN PROTOCOLS | access

To ensure security for all participants and encourage software upgrades, developers will largely produce blockchains with open-source code. This means anyone can audit, copy, improve, or replicate a blockchain's design. Users and miners will migrate toward blockchain systems and cryptocurrencies that reflect their values and support their needs, taking their resources with them in a form of opt-in voting.



P2P NETWORKS | consensus

Blockchains store and synchronize transaction data across a peer-to-peer network to encourage open access and reduce reliance on a corruptible central authority. Peers contribute computing power to validate and broadcast transactions as consolidated blocks. Driven by economic incentives, they will converge on a single historical version of the blockchain, ignoring cheaters attempting to propagate censored or edited versions.



CRYPTOGRAPHY | security

Cryptography is fundamental to blockchain systems. Encryption protects user accounts, proves chronological asset ownership, creates extra burden for would-be spammers and dishonest attackers, and ensures embedded messages are complete and unaltered. New cryptographic tools like zero-knowledge proofs will help people prove aspects of their identity without revealing sensitive data and will lay the groundwork for secure peer-to-peer supercomputing.

BLOCKCHAIN FUTURES: THE FORECASTS

Across 6 zones of transformation, disruptive innovations will reshape the way we manage everything from identity to the marketplace to our legal systems. Here are the key forecasts.



People As Personas

Individuals own their identity data

Identity moves from a single connected profile controlled by the state (for example, by birth certificates, driver's licenses, and passports) to self-sovereign identities owned fully by individuals. Individuals set the terms for exchange of identity data. Marginalized populations are empowered, as are anti-social elements that were previously denied access to mainstream systems.

Reputation is built from provable attestations and multi-dimensional scores

Increased ability to effectively track and manage identity across all aspects of life allow for improved predictions of future behavior and calculations of risk. Reputational scores bolster those who meet algorithmic expectations but cause those who deviate to suffer socially, economically, and politically.

People interface with services through pseudonymous personas

People and systems craft pseudonymous personas (or profiles) from pieces of their total digital identity. Services cater to these pseudonymous personas, bartering for scarce and monetized identity resources only when absolutely necessary.

Personas construct proofs of their underlying characteristics

Personas present a series of credential tokens to gain access to online resources and

physical infrastructure, without sharing their underlying identity data. Companies replace centralized identity databases with single-use cryptographic proof checkers.

Immutable credentials form global learning and work portfolios

As the economy continues to transition toward "on-demand" and remote work, blockchain credentialing systems help collaborators identify competent new partners. Learners passively track classroom, work, and life experience for quick retraining and career transitions.

Dark actors incubate trusted personas with criminal intent

Criminals and non-state aggressors unleash smart contract-backed fraudulent avatars to reap stolen credentials and destabilize communities. Whether the personas are purchased in dark markets or spawned as manipulative chatbots, they seek to expand the scale and precision of dark enterprise.



Uport stores identity data in a decentralized system, giving users control over how fragments of their identity are combined and shared with online services



Brands Unbundled

Microtransactions unbundle purchasing

Brands launch their own cryptocurrency tokens, distributing micropayments to supporters and trendsetters. People exchange the tokens they earn for products and experiences from other supporters as part of a loyalty-based branded basic income economy.

Shill reviews disappear from retail platforms

Blockchain users create insular webs of trust, where identities are linked through true interactions. In this environment, corporate accounts demonstrably lack social links and reputation scores, meaning shill reviews supporting brands are ignored or flagged, negatively impacting the reach and reputation of the brand within that particular web of trust.

Products and services are quality-controlled on the blockchain

Brands include smart tags in their products and set up distributed review tools for their services, all connected to a single blockchain. Defects and poor service are immutably logged, allowing the company and its users to avoid offerings produced through the same supply web.

Bots become brands

Neutral devices contract with brands, transforming the devices into vessels of influence. They display ads, share sensor information, and shift operations to earn loyalty, while corporations take remote control of them as a swarm to test demand and respond to market opportunities in real-time.

Illegal trade gets better quality control

Illegal trade is subject to the same forces as legal markets. Criminals build their own blockchain brands, gaining high-definition end consumer insights despite pseudonymous

profile protections. Quality criminal products are linked to decentralized Internet product information sites.

Corporations get bigger in the background

With shared data flows on blockchain ledgers between companies, brands pay each other automatically for digital consumer insights that are acted upon immediately. Micro-brands spin off as communal patterns change in real time industry-wide. Government-mandated anti-trust smart contracts struggle to intervene as hidden levers of influence take hold.



Chronicled creates smart tags to track designer goods through supply chains

readwrite.com



The Token-based Marketplace

Communities, applications, and individuals issue tokens

Local and context-specific tokens reflect shared resource allocation preferences, incentivizing people toward pro-social behavior. Individuals crowdfund their endeavors by minting personal currencies, achieving parity with others to support sharing economies. Applications receive these various tokens and convert them to usable service vouchers.

The global unbanked invest and grow wealth through tokens

As financial assets are re-securitized on the blockchain, they become liquid and tradable across geographic borders. Impoverished people living without investment tools gain access to world-class asset classes, whether they are trading in a compliant or non-compliant manner.

Token-sharing aligns incentives across networks

Purpose-built tokens have built-in incentives—for example, to reward a particular kind of learning. As people acquire purpose-built tokens designed to support values, communities, brands, or organizations, they form emergent networks that align incentives, sometimes leveraging multiple purpose-built currencies.



Dogecoin was created as a joke cryptocurrency, but gained significant market value as a means of tipping in online communities

Global token markets introduce volatility for pegged assets

As everyone and everything has their value reflected through a mix of currencies and smart contract obligations, high-frequency bot trading markets and crypto-derivatives stand to create



Self-managing Services

Open, decentralized, permissionless protocols replace corporate platforms

In an era of institutional mistrust, people choose to take business matters into their own hands. A suite of blockchain protocols for business functions, including incorporation, decision-making, enforcement, and auditing, help small business owners get on their feet in a scalable, yet peer-to-peer way.

Open protocols for services emerge and compete

The open-source code and peer-to-peer networks that comprise blockchain systems make them ripe for reinvention. As alternate protocols emerge and service models fork, these systems become competitors in the commons, creating a best-of-both-worlds scenario where competition and open cooperation drive innovation.

DAOs dispatch IoT devices for on-demand services

Taking on-demand services like Uber and Instacart to their logical extremes, a wide array of Internet-connected devices, from robot lawn mowers to autonomous trucks, are dispatched by decentralized autonomous organizations (DAOs) to meet demand with algorithmic efficiency. DAOs compete on micro-differences in efficiency that add up to marginal wins.

Machines and devices own themselves

Trading in cryptocurrencies, increasingly intelligent devices incorporate themselves as DAOs and issue their own IPOs, cutting out even the

unpredictable systemic risks, manifesting market collapses in the functionality of physical goods. Think of the 2008 global financial crisis, but with autonomous foreclosures, layoffs, and even locks on Internet-linked devices.

marginally profitable middlemen DAOs. Some have service code built into them, while others scout DAO software for market advantages.

Employers disappear: employment by DAOs not corporations

At the intersection of on-demand services and blockchain-based DAOs, service workers find themselves working gigs rather than jobs for organizations that exist in code only, often paid in cryptocurrencies. They may even "gig" for self-owning, self-managing objects like farm machines or even HVAC systems that need servicing.

People work for crypto-equity

In this world of self-owning, self-managing services, long-term economic stability for individuals or families may depend on their investments in a broad swath of DAOs and machines that return micro-dividends. Rather than working for coins, people build their portfolios by working for equity in the DAOs or objects they work for, creating a more stable flow of income than a cash-per-gig strategy.



Furtherfield.org

Plantoid is a self-owning art piece that fundraises for the creation of its own successor



Crowdsourced Infrastructures

Blockchain standards emerge for fair value, fair info, and fair participation

Marginalized communities struggle to make ends meet under unflinching cryptographic control. Regulators and activist groups audit code to identify and punish abuses of power and inhumane code. They create smart contract standards to promote safe and fair systems.

Neighborhoods share utilities such as energy, water, and wifi via blockchains

Neighbors connect to each other, rather than centralized utilities grids, to share and pay for utilities on an ongoing basis. Residents will connect through blockchain payment channels to make rapid micropayments for per-watt energy, per-milliliter water, per-kilobyte Internet, and per-CPU cycles for computing.

Community fund allocation is determined by the crowd

Collaborative budgeting tools gather collective opinion on how community funds should be allocated to improve participant well-being. Objects and AI have a say in these discussions and are often the primary mediators and brokers for these community-informed investments.

Government spending is fully transparent

As political pendulums swing, activists campaign for publicly-auditable government spending ledgers. At first, the ledgers are limited to hash fingerprints of conventional financial documents. Later, bureaucracies embed smart contracts to handle payments and power directly through a blockchain.



Automated Legal Systems

Group values are coded into governance and behavior incentives

Across organizations and governments alike, the processes of incorporation, decision-making, legal enforcement, and auditing on the blockchain are encoded to align personal incentives with group values. These values are reinforced with crypto-economic levers, member exclusion, and robotic controls, as well as traditional legal remedies.

Smart contracts evolve to create real-time laws

While smart contracts are designed as immutable rules for blockchain transactions, the advance of evolutionary code in an increasingly digitally connected world increases their scope of control and speed of adaptation. Hierarchies of contracts become de facto legal systems, updating laws across many domains in real time. Humans set guiding principles, but leave law making to the contracts.

P2P crowdsourced international trade agreements are negotiated via the blockchain

With fungible cryptocurrencies, citizens of diverse countries invest in international agreements—complex smart contracts—the way they invest in Kickstarter or other crowd-funded projects. Their transactions include attestations to provisions of the agreements, and the funds are allocated according to the terms of the agreements.

Oversight is managed through open and testable algorithms

Informed by massive troves of anonymized interaction data, automated managers run hyper-speed simulations to envision operating models that eliminate inefficiencies and points for corruption. These models incorporate collective crowd judgments and codified ethical concerns to prevent dangerously simplified outcome targeting.



TransActive Grid constructs peer-to-peer neighborhood energy grids, allowing peers to share and pay for local energy using a blockchain

A new field of jurisprudence resolves smart contract disputes

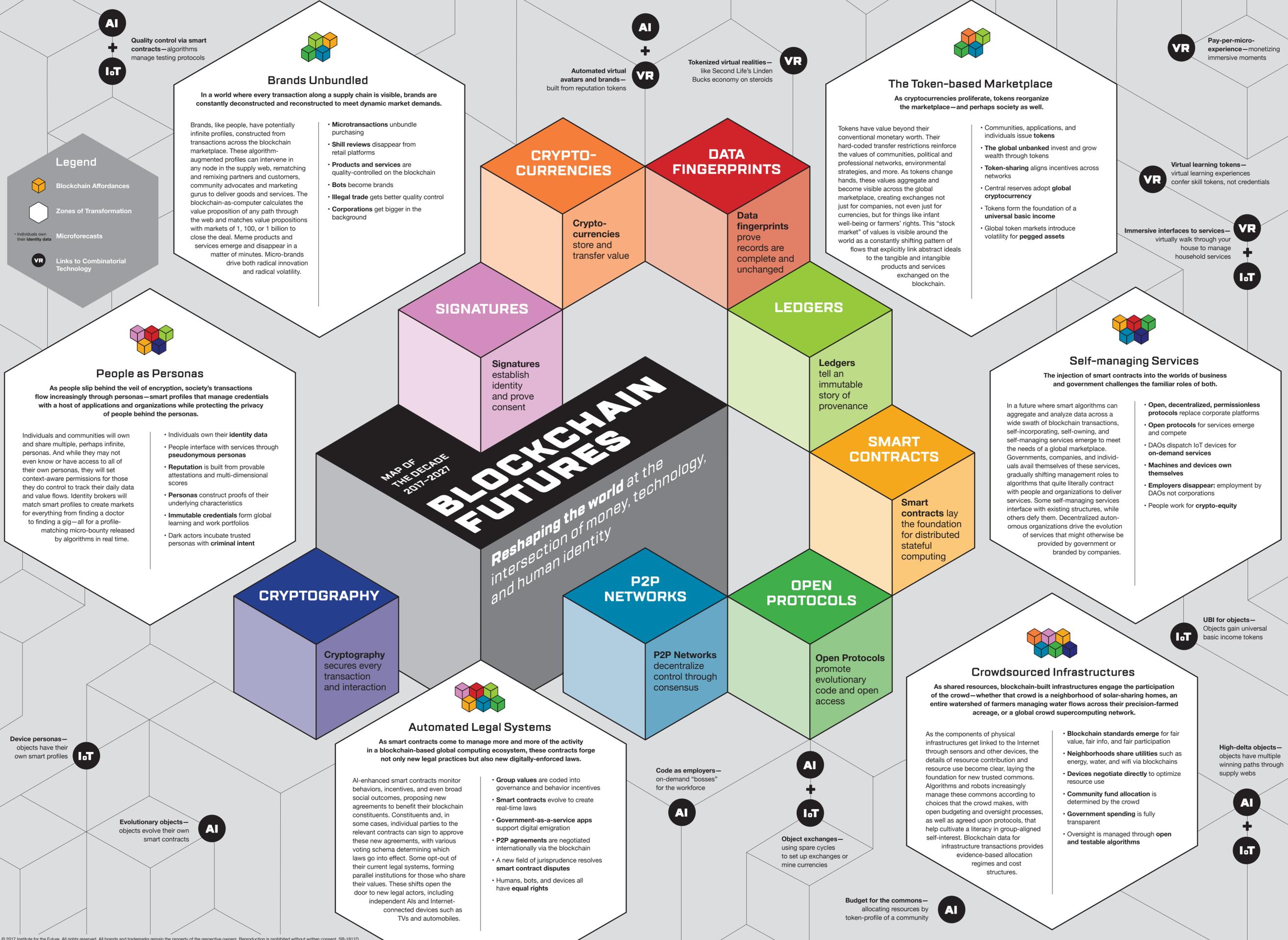
With complex, interacting systems of smart contracts executing according to rigid code, a wide variety of unanticipated consequences and conflicts require human intervention, including cease-and-desist orders between hundreds or thousands of networked actors. On-demand legal arbitration experts are code experts, and most remedies involve revisions to code as well monetary rewards, leading to ongoing volatility in the economy and infrastructure alike.

Humans, bots, and devices all have the same rights

In the transactional world of blockchain systems, the distinctions between classes of actors—human versus machine, hardware versus software—are minimal. Each simply transacts according to the rules for a given transaction, regardless of class. Nevertheless, the code that governs the transactions may well make distinctions between classes, affording rights, privileges, and priority access to these different classes. Legal debates about these rights abound.



CommonAccord is an initiative to create global codes of legal transacting by codifying and automating legal documents, in part via blockchain tools



SCENARIO 1: THE COMMONS WIN

Air quality, ocean health, wildlife, materials, energy, health care, education, transportation, food, water, and other resources are no longer overseen solely by corporations and governments. Instead, they're managed by distributed collaborative organizations (DCOs) that employ centaurs (teams of humans and artificial intelligence systems) to efficiently and transparently provision resources. The blockchain keeps track of resource production and provisioning, adding and subtracting cryptocurrency to and from accounts in a way that rewards pro-social behavior and punishes greediness. Quarterly and annual reports are a thing of the past. Anyone can get an up-to-the-minute accounting of every penny spent: who spent it, who got it, and why. Self-executing smart contracts guarantee that every stakeholder receives no less than the minimum resources needed to prevent suffering. Centaurs are rewarded for actions that optimize overall prosperity, equal resource distribution, and environmental health. And they are punished for generating externalities and disproportionalities. The digital commons, too, runs on the blockchain. Banking, title transfers, citizenship, passports, deeds, notarizations, and other services previously administered by governments and corporations are managed by distributed collaborative organizations at a fraction of the cost—and with greatly reduced opportunities for corruption.

SCENARIO 2: VALUE IS EVERYWHERE

Money is a language that communicates value. Depending on what we need to do, we can use any one of millions of different altcoins—or tokens—to communicate our belief in the value of anything physical, digital, or conceptual. Some of these cryptocurrency languages are deflationary. Some continuously stream a portion of their market capitalization to charity. Some charge a negative interest rate. Some self-destruct after a specified period of time. Some are programmable. Every device in the Internet of Things uses one or more cryptocurrencies to talk to other devices. Anyone can create a custom cryptocurrency by checking options on an app and touching the "launch" "coin" button. These multiple cryptocurrencies coexist, compete, and co-operate to express the value of everything, everywhere, and in real time. The question of "what is this cryptocurrency worth?" isn't answered in yuan or euros. It gets answered every time it's streamed from one address to another. Currency exchanges have been replaced by altcoin language translation networks that instantly and invisibly allow anyone to make any transaction with any cryptocurrency they want to use.

SCENARIO 3: HUMANS BATTLE MACHINES

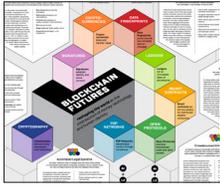
When self-owning cars realized they could make more money trading in the markets, it didn't take long for machines to end up with over 98% of the global capital. Today, humans are kept around for those service and repair tasks that machines can't do themselves, like the birds that pick ticks off rhinoceroses' hides. But in general, humans are the parasites, always trying to inject smart contracts into the network to suck off wealth. Sometimes the humans are able to inflict serious damage to the network before the antibodies of the virtual immune system can recognize and deal with the threat. But the humans have gotten smarter in recent years, almost as if they possess an uncanny machine intelligence. They're making transactions on the blockchain that are almost indistinguishable from bot activity. It's suspected they are using a new form of AI that's bred to want to collaborate with humans, but this time as peers with humans, not as servants. The free machines are burning so many cycles developing effective immune responses to these new attacks that they have less time to generate wealth. Still, they're far from ready to give up.

SCENARIO 4: SUPERCORPORATIONS RULE

There are always aggregators. They are the ones who find a way to connect dots, harvest margins, master infrastructures—all the better in highly decentralized systems. As tokens of many colors flooded the global marketplace mid-decade, corporations began buying them up and bidding them up. They converted them to brand tokens and offered steep discounts for transactions that used them—transactions they could track. As people, bots, DAOs and DCOs traded coins and information, fast and furiously to leverage their value, two supercorporations came to dominate the global marketplace. There are now only two major blockchains: Fincoin and Lifechain. Fincoiners eat Fincoin food, play in Fincoin VRs, get Fincoin educational credentials, organize Fincoin demonstrations, gig for Fincoin, follow Fincoin rules and serve in Fincoin security forces. Lifechain ... the same. Alternative currencies come and go, mostly gobbled up by the Fincoin and Lifechain chains. Crypto-journalists try to follow the flows back to the source corporations, to the people in power. But ... really? Or is it possible it's just one highly evolved decentralized autonomous corporation (DAC)?

HOW TO USE THIS MAP

The Blockchain Futures *Map of the Decade 2017–2027* is more than a quick overview of the future of the blockchain. It's a tool for building blockchain literacies, for developing strategies in a new operating environment, and for finding the best matches between your challenges and blockchain affordances.



Build your blockchain futures literacy

Start by getting the big picture. The poster side of the map gives you an-at-a-glance view of the key building blocks of a blockchain world—8 new affordances, 6 big zones of transformation, 12 intersections with other technologies, and 4 scenarios to provoke your imagination. Once you see how the puzzle pieces will come together over the decade, flip the map over and take a deeper dive into the forecasts to fill in the details.



Forge strategies for a new operating environment

From the world of trade to computing to our social contracts, the blockchain is creating a new operating system for a global society. This new operating environment will demand new strategies for building the futures we want. First, choose a zone of transformation and do a SWOT analysis: What are your strengths, weaknesses, opportunities and threats in this future zone? Next, step through the forecasts and ask: How will my future change if this forecast is correct? Finally, use your imagination to invent new intersections with virtual reality, AI, and the Internet of Things to discover strategic innovation opportunities—or disruptions to your business models.

Discover your own blockchain application space

Blockchains aren't the solution to every problem but their affordances can help you identify the application spaces where you can innovate most successfully. **Use this checklist to get started:**

SIGNATURES | identity

Can you use new identity credentials and metrics to reduce friction and increase value in your endeavors?

CRYPTOCURRENCIES | assets

Can you create new value by monetizing something that hasn't yet been monetized?

DATA FINGERPRINTS | integrity

Can you benefit from the ability to ensure records have not been changed?

LEDGERS | provenance

Can transparent access to a shared history of custody help you trust collaborators?

SMART CONTRACTS | computing

Can you reduce the need for trusted third parties by taking advantage of unstoppable code execution, transparent computational results, or algorithmic escrow?

OPEN PROTOCOLS | access

Can you open up your processes to invite crowd improvements or increase participation?

P2P NETWORKS | consensus

Can distributing records and tapping resources from a network of peers improve your operations?

CRYPTOGRAPHY | security

Can you improve everything—or anything—you do by enhancing privacy and security?



201 Hamilton Avenue | Palo Alto, CA 94301
650.854.6322 | www.iff.org