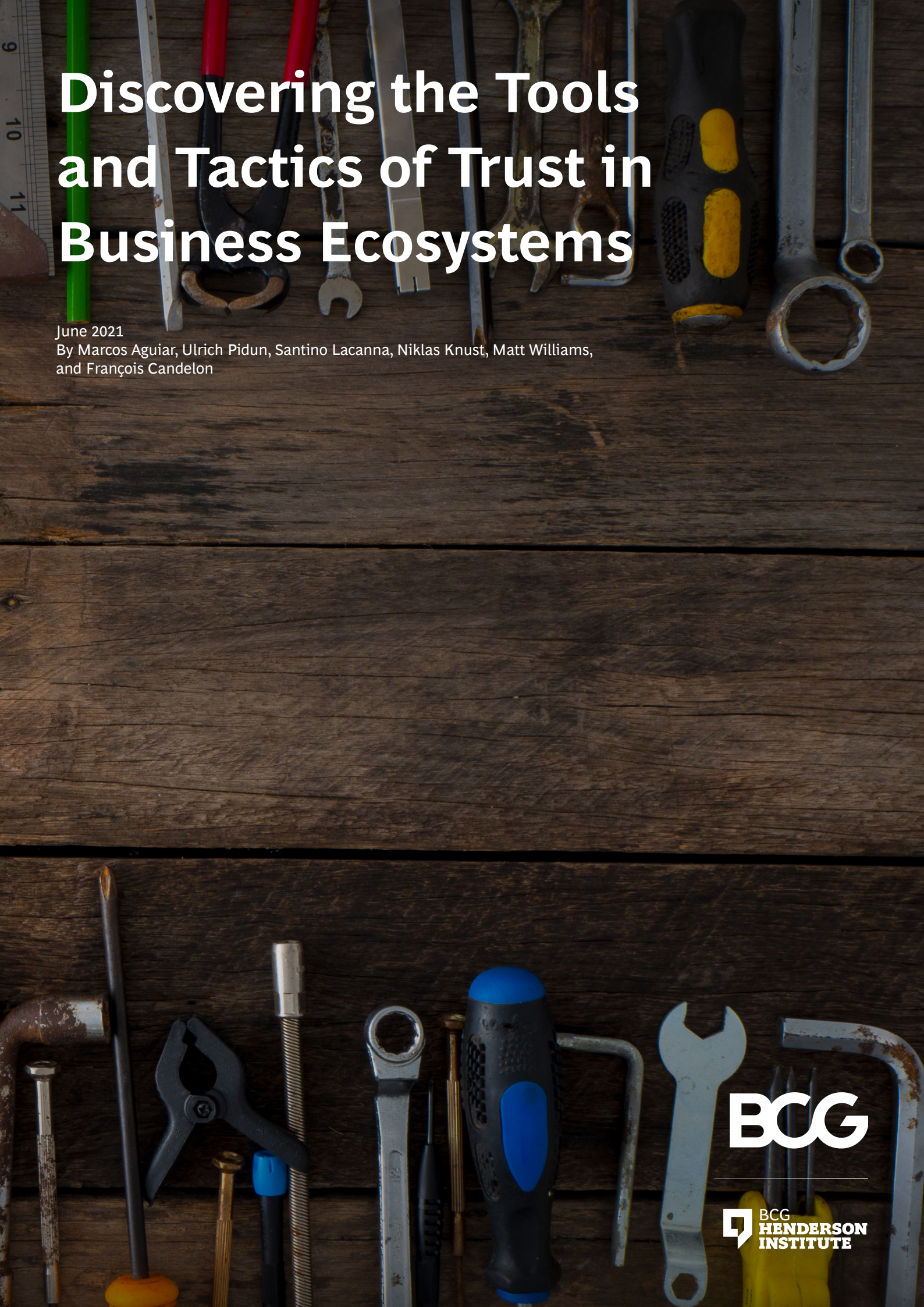


Discovering the Tools and Tactics of Trust in Business Ecosystems

June 2021

By Marcos Aguiar, Ulrich Pidun, Santino Lacanna, Niklas Knust, Matt Williams, and François Candelon

BCG

BCG HENDERSON INSTITUTE

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.

The BCG Henderson Institute is Boston Consulting Group's strategy think tank, dedicated to exploring and developing valuable new insights from business, technology, and science by embracing the powerful technology of ideas. The Institute engages leaders in provocative discussion and experimentation to expand the boundaries of business theory and practice and to translate innovative ideas from within and beyond business. For more ideas and inspiration from the Institute, please visit https://www.bcg.com/featured-insights/thought-leadership-ideas.aspx.

Discovering the Tools and Tactics of Trust in Business Ecosystems

This report is the second publication in a series on designing business ecosystems for trust. The first article explored the role of trust in business ecosystems' success or failure, demonstrating how trust can grow and how it can erode in ecosystems and identifying five key lessons (or principles) for leaders to design and manage an ecosystem that fosters trust.

As business grows ever more digital—as virtual relationships increasingly become the norm in the post-COVID reality—winning and maintaining stakeholder trust becomes as crucial to a company as ensuring product or service integrity. Nowhere is this truer than in business ecosystems, those dynamic alliances of largely independent economic entities that create products or services that constitute a coherent solution. Ecosystems depend on well-functioning networks of buyers, sellers, and various other parties in between to thrive and grow.

As business ecosystems become more commonplace, the importance of trust—between and among participants and between the end user and the platform itself—becomes a more salient issue. For example, buyers on an e-commerce marketplace need to know they will receive what they have paid for and that their data won't be abused. Participants on fundraising platforms need to be protected from fraud. Controls for bad behavior, protocols for resolving disputes, and quality assurances are essential for everything from gig economy platforms to smart, IoT-based ecosystems. For any and all kinds of ecosystems, incentives for members to cooperate are absolutely necessary in order for everyone to reap the benefits of their interactions.

Indeed, a lack of trust is one of the most important reasons why ecosystems fail. At the same time, as we argued in the first publication of this series, trust is also a core success factor in business ecosystems, a direct contributor to a company's value proposition. Therefore, watching out for weak signals of potential failure due to mistrust is one of the most important tasks ecosystem leaders perform. It's important throughout the life cycle of an ecosystem, from launch to maturity. But it is most critical in the scaling-up phase, when network effects kick in and exponential growth can make or break market leadership.

While most ecosystem members recognize that trust is important, it is often treated as a feature that arises organically, on its own, over time. And although most ecosystems adopt some mix of instruments to engender trust among their members and customers, few consciously and proactively build it into their platform. But trust doesn't happen automatically; it must be designed into an ecosystem. It can be hard to build, but it is easy to erode.

Through our in-depth analysis of both successful and failed ecosystems—B2C, C2C, and even B2B—we identified key tools and processes (herein referred to as "instruments") and their combinations for major types of ecosystems. Instead of taking a hit-or-miss approach, ecosystems can use these findings to forge and maintain trust as they launch, scale, and sustain their business.

In this report, we aim to help ecosystem leaders design and ingrain trust by answering three questions: What instruments can be used to build trust in business ecosystems? How do successful ecosystems combine those instruments, and why? And what are some of the most critical considerations that ecosystem leaders should focus on when designing an ecosystem for trust?

The Difference Between Success and Failure

A stunning 85% of ecosystems—even the most promising ones—fail. By that, we mean they dissolve, shrink to insignificance, or are bought out for below investment cost. In analyzing the demise of more than 100 failed ecosystems over the past 46 years, we discovered that trust (or lack thereof) played a pivotal role in their failure. (See the sidebar "Our Methodology.") More than half of them (52%) struggled to build trust altogether. This caused friction among participants, drove up costs, and thwarted network effects, which are effectively the entire basis of ecosystems' benefits and a fundamental reason participants join them.

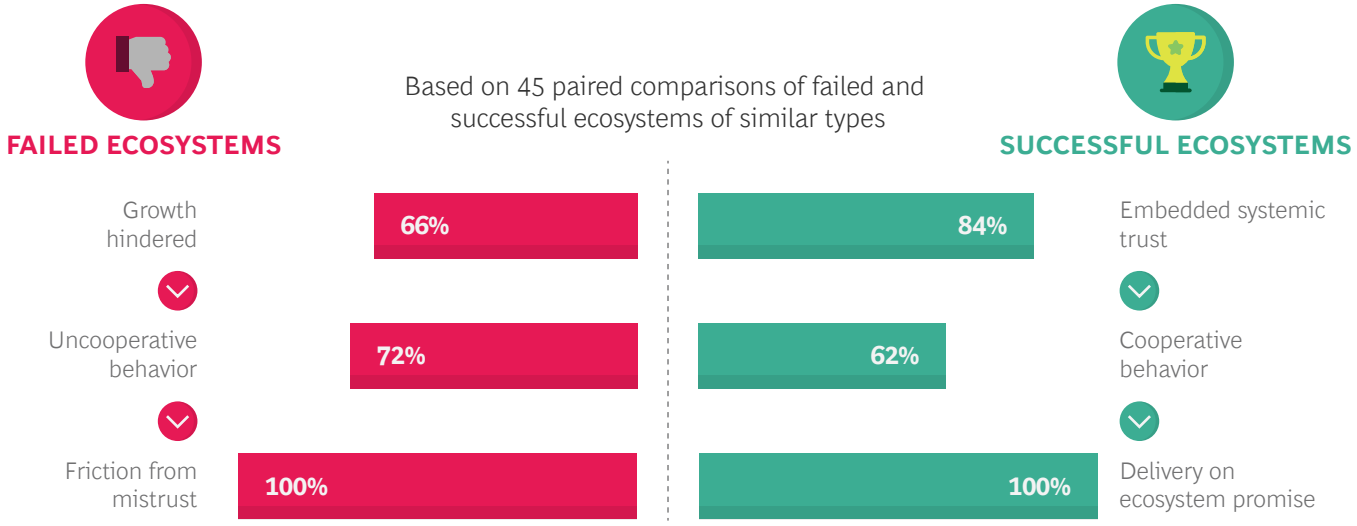
Our Methodology

To understand the role trust plays in ecosystems, we analyzed failures and successes in a two-part study. First, we examined 110 failed ecosystems—B2C, C2C, and B2B—that were born and died between 1974 and 2020. They include social networking companies; online marketplaces; software solutions companies; and payment, mobility, entertainment, and health care service providers—the average lifespan was 6.8 years and average funding was $185 million. We combed through quantitative and qualitative data such as their history, capital raised, deal sizes, industry classification, and geography, as well as a database of unstructured data that we created from public sources.

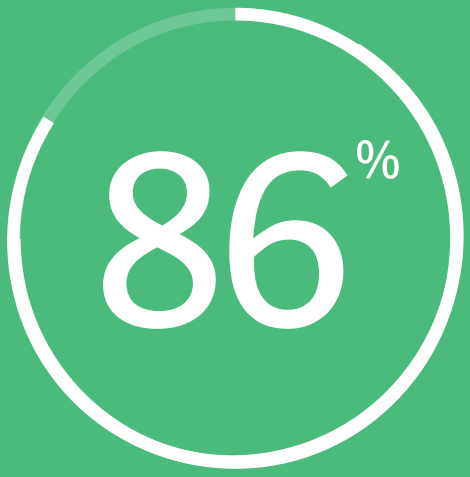
Next, we matched a failed ecosystem with a successful counterpart, chosen from 45 success stories drawn from the same period. These paired comparisons allowed us to more clearly distinguish successful trust-building efforts from unsuccessful ones.

On the flip side, trust is a cornerstone of success for thriving ecosystems, according to our study of 45 successful ecosystems across 20 industries. Among the successful ones, 86% actively embedded trust in the platform and their governance practices, achieving what we call "systemic trust." These organizations understood that trust between strangers ("relational trust") doesn't arise spontaneously; it takes cultivation. The cooperation needed to fuel success was anchored chiefly in systemic trust, and this trust is what spelled the difference between success and failure. (See Exhibit 1.) Some 88% of ecosystems used a combination of digital instruments (such as ratings and escrow models) and nondigital instruments (such as guarantees and access rules).

Exhibit 1 - How Trust Stokes or Thwarts Ecosystem Success



Source: BCG Henderson Institute analysis.



of successful ecosystems embedded systemic trust

The Trust/ Success Connection

A stunning 85% of ecosystems—even the most promising ones—fail. … More than half of them (52%) struggled to build trust altogether.

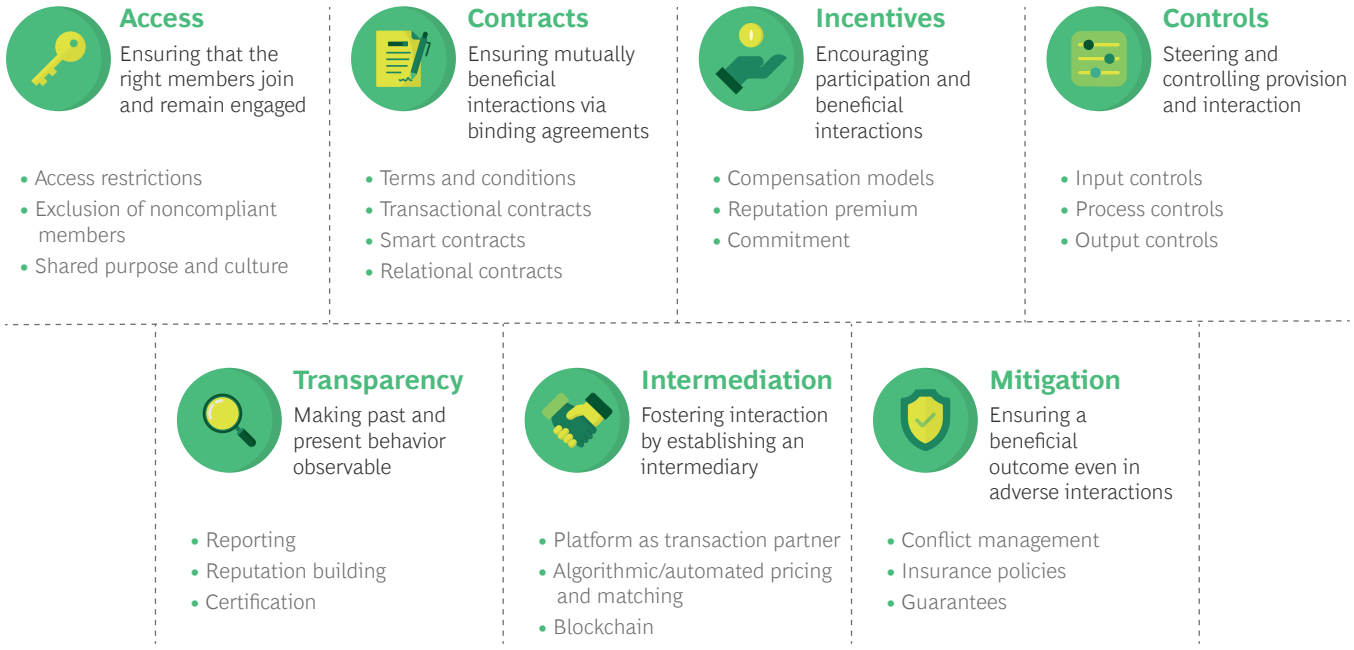
Among the successful ones, 86% actively embedded trust in the platform and their governance practices, achieving what we call “systemic trust.”

The Trust Instruments

We uncovered 22 trust instruments, which can be grouped into seven basic classes (see Exhibit 2):

- **Access,** which ensures that the right members join and remain engaged
- **Contracts,** which guarantee mutually beneficial interactions through binding agreements
- **Incentives,** which encourage participation and cooperation
- **Controls,** which guide interactions and behavior
- **Transparency,** which makes past and present behavior visible to all
- **Intermediation,** which facilitates interaction by establishing a neutral middleman
- **Mitigation,** which ensures a beneficial outcome even amid disputes or adverse situations

Exhibit 2 - The Seven Classes of Trust Instruments



Source: BCG Henderson Institute analysis.

Access. Fostering high-quality, cooperative interactions is critical for ecosystem success, and that means screening players to ensure that the right ones join and stay. Access instruments serve this purpose. Just as important, they block bad actors—those that have already demonstrated they don't play by the rules and those that are likely to be noncompliant.

Access regulation may start with a strong ecosystem culture with shared norms and a common purpose, both of which support trust by attracting and keeping desirable participants. The software platform Linux is built on the open-source community's values. Access restrictions help engender trust and prevent problems; a good example is HopSkipDrive, an "Uber for kids" that requires drivers to have certain qualifications and pass a detailed background check before they can join. Exclusion tactics include after-the-fact measures, such as Uber's policy of banning drivers whose customer ratings fall below a certain threshold, or actions such as Linux banning contributions from University of Minnesota participants after discovering that researchers knowingly submitted code with security flaws as a test. (Perceived inconsistencies in exclusion decisions and different interpretations of what constitutes bad behavior have drawn public and congressional criticism. Clearly, as a reflection of contemporary culture and attitudes, social media may, more than any other type of ecosystem, need a routine reassessment of trust instruments.)

Contracts. Building trust through contracts is more difficult in an ecosystem context than in bilateral or hierarchical relationships because the ecosystem operates on voluntary collaboration between largely independent economic players. Still, contracts can play a role in fostering trust. Various types of binding agreements formalize ecosystem participants' commitment to fulfill their obligations. One example is the Terms and Conditions agreement. Signed upon entry, Terms and Conditions agreements stipulate the various parties' rights, obligations, roles, and responsibilities. Although legally important and almost universally used, they are little more than a pro forma first step to trust building. Transactional contracts define the conditions of specific transactions, such as return policies, which are particularly important for building trust with consumers in used-goods marketplaces.

Smart contracts are computer programs that automate the execution of an agreement without third-party involvement. Created automatically from the standardized data buyers and sellers provide, they are fast, encrypted, and secure, so they ensure trust and transparency. Smart contracts may be particularly applicable to digital ecosystems. Ant Group's Trusple, an international trade and financial service platform, relies on smart contracts to automate the otherwise intensive and time-consuming processes that banks use to track and verify trading (particularly cross-border) orders. Such contracts also enable small and mid-sized enterprises to establish their creditworthiness and ease the financing process.

Relational contracts are flexible, principles-based (as opposed to rules-based) contracts in which parties define common goals, dependencies, or roles and obligations to the platform itself and among themselves. Relational contracts can be useful in establishing a general framework for collaboration, especially if the ecosystem is still expanding and evolving.

Incentives. Incentives prompt players to act according to the ecosystem requirements—not in direct ways but by setting conditions that are conducive to cooperation, as in game theory. A compensation model uses the prospect of value sharing to instill trust. Amazon Kindle's compensation instrument, for example, grants publishers the same payouts from e-books that they would get from print books, thus overcoming the trust concerns about cannibalization of their core business. Reputation premiums reward partners with a record of trustworthy behavior. For example, sellers on Taobao with a first-rate reputation can charge higher prices.

Commitment—in the form of coinvestment or cospecialization—is yet another incentive instrument.[1] SAP established a tiered partner network that confers extra benefits to higher-ranked partners. To obtain a higher ranking, partners must invest in the ecosystem. Doing so signals both their heightened commitment and their dedication to quality—which, in turn, enhance customer trust. HomeKit, Apple's smart home ecosystem, uses cospecialization to forge trust: Hardware manufacturers of accessories that connect to Apple devices are obligated to join the company's highly regulated MFi (made for iPhone/iPod/iPad) program to ensure quality.

Controls. While incentives influence by making specific behavior the rational choice, controls steer interactions directly and limit or impede unproductive behaviors, unacceptable inputs (for example, counterfeit items on a marketplace or nude photos on a social media site), or unintended consequences.

Formats, standards, and interfaces are common technology examples of input control instruments. For example, Spotify and Amazon's Kindle have forged trust with their partners (music studios and publishers, respectively) through their platforms' technical architecture and data format, which prevent piracy. Other ecosystems define input guidelines; Taobao, for example, determines which products are allowed on its platform, and social media platforms establish communication guidelines.

Process controls involve behavioral restrictions. Uber applies this instrument in two ways: automatically assigning the nearest driver to the customer and automatically picking the most efficient route to ensure that drivers don't take advantage of the customer.

Output controls include the frameworks and algorithms that mobile platforms like Android and Apple iOS use to check the quality of uploaded apps. For example, every app and update on Apple's App Store platform is approved by an Apple employee at the company's App Review division. YouTube's AI algorithm checks each video's music and removes any that violate copyright. Many social networks use editorial control instruments to monitor content. Facebook uses two methods to identify bad behavior: monitoring user complaints and, through AI algorithms, flagging content that violates ecosystem guidelines. Flagged content is ultimately judged by a human compliance team and is subject to an escalated punishment system; the company created an independent oversight board in May 2020 to review its more consequential and controversial content-blocking decisions.

Transparency. By making behaviors and performance visible to ecosystem participants, transparency instruments encourage them to act honestly and in desired ways, thus engendering trust among participants as well as newcomers. Transparency can be generated through reporting instruments that allow users to flag bad behavior; social media platforms such as Facebook, Twitter, and TikTok use these. Reputation-building measures, such as ratings and customer reviews, are especially useful for marketplaces (like Amazon) and gig economy ecosystems (like DoorDash and TaskRabbit) because they help reduce information asymmetry. The prospect of negative reviews curbs bad behavior and rewards those who fulfill or exceed their promise, and the credibility of user endorsements helps attract new participants.

> **An often-overlooked but powerful trust-building instrument is certification by the platform.**

Many ecosystems confer certification on members for their high quality, whether for products (think Carvana, the used car marketplace, or eBay), projects (as in Kickstarter, the crowdfunding platform), or merchants (Google's Trusted Store program).

1. Cospecialization is a type of strategic alliance in which partners—such as a vendor and a client—bring their respective resources and expertise together to create value.

Intermediation. Intermediaries shift trust out of the direct relationships between individual participants and make it a feature of the ecosystem. By providing a buffer, intermediaries give the transaction parties confidence that the other will live up to its end of the bargain. In one model, the platform (or orchestrator) inserts itself in the transaction, typically through an escrow model. Taobao and eBay use this model to ensure that goods are transferred only after the buyer has paid and that the seller is paid only after the transaction is completed. Some marketplaces even act as direct transaction partners: They buy the goods and later sell them, decoupling trust from providers and making it a simple relationship between the platform and the end customer.

Technology provides another powerful means of intermediation to elicit trust. Many ecosystems use algorithms to automate pricing or matching to ensure quality in interactions. Uber not only matches rides through a central algorithm but also uses algorithms to centrally create prices, using a dynamic pricing model that adjusts rates based on such variables as time, distance, traffic level, and current rider-to-driver demand. Blockchain is yet another technological instrument used for intermediation between users. Interestingly, although the whole point of distributed ledgers is to disintermediate, the platform, in this case, actually becomes the intermediary. De Beers' Tracr uses blockchain to connect the diamond industry on a common digital platform and establish the provenance, authenticity, and traceability of its diamonds throughout the value chain.

Mitigation. Mitigation instruments provide troubleshooting and conflict management as a last resort. Not only do they limit the damage in case of trust failures; their mere availability fosters trust upfront by offering protections that encourage parties to participate in the ecosystem. We discovered three types of mitigation instruments: conflict management tools, insurance policies, and guarantees. Many platforms, such as Uber and Airbnb, manage conflicts between partners centrally. Payment solutions like Visa also use central conflict management to arbitrate, as in the case of fraud. Other ecosystems use decentralized or distributed conflict management processes: at Reddit, moderators arbitrate the various forums; at Wikipedia, committees of editors resolve content disputes; and at Alibaba, a dispute mediation team reviews the complaint and makes a final determination to settle the matter. Insurance policies limit losses from adverse events; Airbnb, for instance, offers members insurance to cover property damages by guests. Finally, guarantees such as those provided in auction marketplaces and payment ecosystems ensure payback in the event of fraud.

Decoding Trust Formulas

Having identified seven classes of (and 22 individual) trust instruments, we asked the next questions: How prevalent are the instruments in the 45 successful ecosystems we studied? What patterns can be observed in those ecosystems? And are there particular combinations of instruments that seem to correlate with success?

Our in-depth analysis of each case revealed that

> **most successful ecosystems use a broad set of instruments, both digital and nondigital, in a truly bionic fashion.**

In each case, we gauged each instrument's relevance to trust creation—and thus its role in enticing cooperation and spawning the network effects that fueled accelerated growth and ultimately success. This was a crucial step because, by and large, most instruments are present in every ecosystem but are not necessarily decisive for building trust or fueling performance.

What were our most significant discoveries? Access, controls, and transparency are the most common classes of trust instruments; at least one of the three is present in almost 80% of the cases. Access is the most widely used (78% of cases), and controls are used by 67% of the cases. Transparency is the most predominant digital instrument (69%) and appears to be the glue that binds participants together in an ecosystem.

Digitization enables a broader deployment of instruments—instruments that in the nondigital past would have had limited application. This is especially true for transparency (think ratings and reviews) and intermediation (for instance, where the platform acts as a transaction partner). As a result, digitization has helped fuel growth. Without it, microlending platforms—whether nonprofits like Kiva or for-profits like Ant Financial—would never have been able to reach the scale they have achieved.

These findings raised the question: Are there distinct combinations of instruments that characterize different types of ecosystems? As we delved deeper to look for such patterns, we identified five more prominent ecosystem categories, or "clusters," that use distinct combinations of trust instruments according to the specific trust issues that they need to address: social networks, marketplaces, Internet of Things (IoT) ecosystems, financial ecosystems, and gig economy platforms. (See the sidebar "Uncovering Trust-Based Ecosystem Clusters.")

We describe the ecosystem clusters and their characteristics below, looking at the particular trust issues of each and the key instruments they typically use in combination to build trust.

Social Networks

In social networks, the quality of members' interactions and behavior are critical trust challenges. Because these platforms are inherently open, they cannot directly control what each participant does.

Key instruments: Successful social networks consistently leverage a combination of three classes of trust-based instruments: access, control, and transparency. The degree of influence each class exerts depends on the ecosystem's maturity level.

Consider Clubhouse, the recently launched audio-only social network. It strictly regulates access, allowing new members only through invitations by current members. This approach is designed to ensure trust in the quality of interactions while fostering growth. More mature social networks still regulate access, but mainly in a reactive way; most platforms kick out poorly behaving individuals. It's worth noting that, amid the highly charged political atmosphere of the past several years, the exclusion policies and practices of leading networks have been put to the test and have come under fire for what some say is bias or lack of transparency (or both) in their exclusion policies. This situation demonstrates that trust instruments must keep pace with a changing culture; in recent years, Facebook and Twitter, two of the world's biggest social networks, outgrew the policy guidelines that served them well in the sites' early days. It also shows that success today is no guarantee of future success.

As social networks grow, their entry requirements typically diminish in order to capture larger portions of the market. (Clubhouse has publicly vowed that it will eventually be open to all.)

> **Mature social networks need instruments beyond access control to ensure the quality of interactions.**

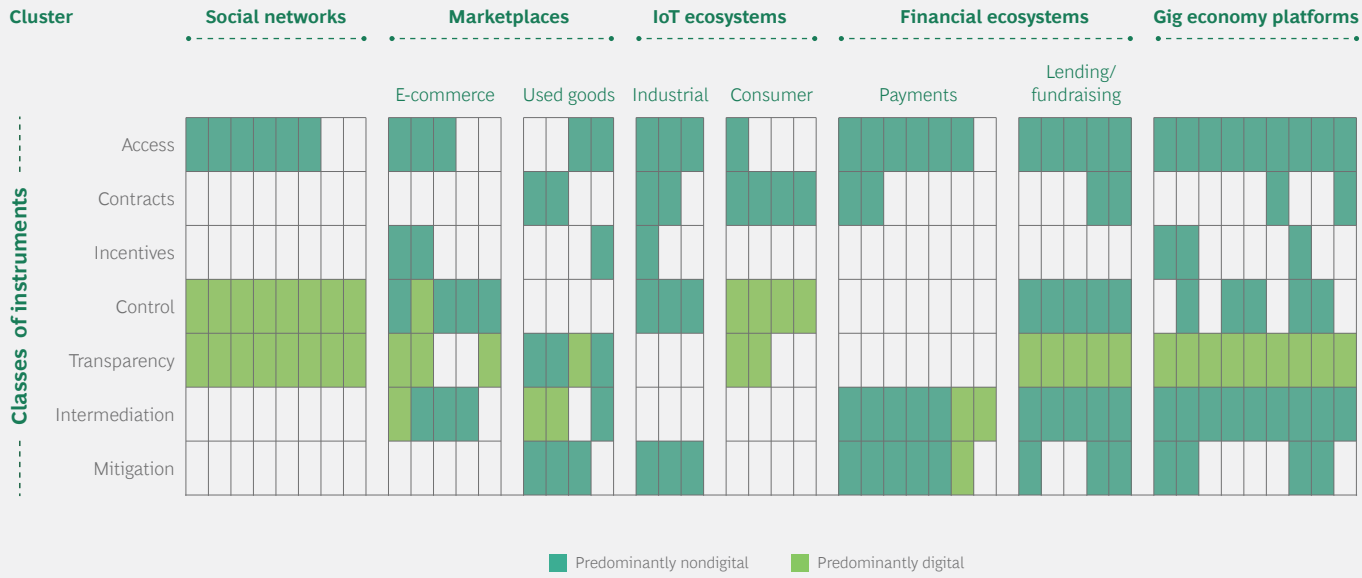
Most use behavior-shaping instruments (such as input controls, curation protocols, and communication guidelines) to ensure that participants behave appropriately. Twitter, for example, clearly states what content is allowed and actively engages in fact-checking and blocking content that violates its guidelines. Here again, digital instruments such as algorithms can play to those ecosystems' strengths. Yet having an instrument in place doesn't mean that it is the right instrument or that it is effectively designed or deployed. Finally, transparency (usually through feedback and reputation instruments) makes behavior broadly observable and users accountable, enabling judgment calls from members on relational and systemic trust. Using instruments such as "likes" for specific content or for following specific members, social networks empower members to build their own trusted networks or feeds.

Uncovering Trust-Based Ecosystem Clusters

To ensure complete objectivity, we began by looking for patterns agnostically, without regard to industry or business model. In a blind and mechanical fashion, without identifying the actual ecosystems, we grouped them into clusters based on similarly recurrent patterns of instrument relevance. Then, and only then, did we identify the actual ecosystems in each cluster to cross-check the consistency of emerging clusters.

To our surprise, we discovered that our mechanical grouping of ecosystems into clusters based on the relevance of similar trust instruments overwhelmingly matched reality. The exhibit shows the "real-world clusters" that we arrived at in our hunt for patterns. Each of the 45 columns represents a single successful ecosystem case. For example, the eight columns under social networks represent eight successful ecosystems. Each cell corresponds to a class of trust instrument: dark green indicates a predominantly nondigital instrument; light green indicates a predominantly digitally enabled instrument. The highlighted cells indicate relevance, not simply presence.

The Characteristic Combinations of Trust Instruments, by Ecosystem Cluster



Source: BCG Henderson Institute analysis.

Note: Each column represents an individual ecosystem case, and each cell corresponds to a relevant class of trust instrument. For example, we studied eight social networks and they used only three types of instruments. Six used access instruments, and all eight used control and transparency instruments.

For example, only three classes of instruments were relevant for social networks. Six of the eight ecosystems used predominantly nondigital access instruments, and all eight used predominantly digitally enabled control and transparency instruments.

For the sake of simplicity, we characterized instruments as predominantly digital or nondigital, based on the origin of the instrument. For example, for access, a background check with a fingerprint was classified as nondigital, whereas rating systems (transparency) are managed by an algorithm and were thus classified as digital. We use the qualifier "predominantly" for a few reasons. First, each class of instruments contains a mix: there are smart contracts (clearly digital) and traditional terms and conditions agreements, which are inherently nondigital (even if provided in digital format). Moreover, to an extent, everything today is digital, and at the same time, everything is human; most ecosystems are built on digital platforms that rely heavily on code, yet that code is written by a human with the inevitable human bias, unwittingly or not.

Finally, most instruments are digitally enabled, and formerly nondigital elements (such as governance and policy-related instruments) are increasingly being digitized. Indeed, our classification reflects a point in time, but it's worth noting that, over time, the instruments (like the interactions themselves) will only become more digital. The remaining nondigital elements are typically the "manned last mile" elements, such as the orchestrator's dispute escalation mechanisms for mitigation.

This is not to say that digital will ultimately supersede most human intervention. Digital has its limits, in three contexts: where the ecosystem touches the physical world (as in gig economy ecosystems, in which the product itself comes through manned delivery); where a judgment call is necessary; and where the system encounters a new situation for which code doesn't yet exist. Nonetheless, this digital/nondigital spectrum reflects the true bionic nature of business ecosystems. Knitting the digital and nondigital together in a synergistic way is what good design for trust is all about.

Marketplaces (E-Commerce and Used Goods)

Along with gig economy platforms, marketplaces use the most trust instruments.

E-Commerce. For e-commerce and digital marketplaces, the key trust concerns revolve around three issues: whether the platform lives up to its value proposition, whether providers deliver on their promise (in quality and timeliness, thus offsetting the inherent information asymmetry between seller and buyer), and potential misbehavior (for example, counterfeiting) among sellers.

Key instruments: In traditional buyer-seller marketplaces, banning repeat offenders (sellers who fail to deliver on time or buyers who fail to pay) is effective. Access, along with transparency instruments in the form of user-based feedback (such as ratings) and platform-based measures (such as certification), implicitly serve to frame the incentives to promote cooperation and trust among participants. A large number of negative ratings on a product or seller will invariably limit sales. Conversely, high ratings can earn sellers "reputation premiums"—in effect, the ability to price their wares or services at a premium because they are more trustworthy. Some e-commerce giants, like Taobao and eBay, go one step further and certify especially trustworthy sellers, directly impacting their sales.

Because, practically speaking, e-commerce marketplaces cannot entirely prevent bad behavior, control instruments can help minimize adverse outcomes and boost trust. On many e-commerce marketplaces, counterfeit products are a real risk to legitimate sellers and customers. Deploying input control measures (such as traceability policies) against copycats is a commonly used and powerful tool.

> **When there is no foundation of trust between sellers and buyers (say, because an ecosystem is new), intermediation can be a powerful tool for enabling interactions.**

When Taobao was established in China, it entered the scene as an intermediary with an escrow model. Intermediation has become more widespread among subscription model marketplaces, such as e-book platforms and music streaming platforms like Spotify. Musicians trust Spotify because it effectively prevents piracy and secures payouts, and users trust the platform because it provides a broad offering at high quality for a reasonable price.

Used Goods. In used-goods marketplaces, the picture changes somewhat. Here, information asymmetry is even greater because a product's quality is a function not only of its original manufacture but also of its prior usage. In addition, because the primary relationship is now C2C and typically transactional (often only a one-off), trust between participants becomes harder to establish.

Key instruments: Used goods marketplaces rely primarily on a set of five instruments: access, contracts (especially return policies), transparency, intermediation, and mitigation.

Access mainly involves barring bad actors. To appreciate the important role contracts play in this type of marketplace, consider Vroom and Carvana, two US-based used car retailers. Their return policies allow the customer to return the vehicle if the quality does not meet their standards. Both platforms provide transparency by inspecting every car listed on their platform, thus certifying quality and reducing information asymmetry. To further boost trust, both platforms serve as the active transaction partner—first buying and then selling the car. In this way, they make direct trust between players (relational trust) superfluous and trust in the platform (systemic trust) essential.

Others, like eBay, use traditional user ratings, which can yield hefty reputation premiums for five-star sellers. eBay's escrow model, in which payment is released to the seller only after the buyer receives the product, limits transaction risk. As in many used-goods marketplaces, these measures are not enough to ensure trust (especially when the goods in question are valuable or the potential for fraud or counterfeiting is high). Their final line of defense against trust erosion is mitigation by resolving conflicts or even compensating victims. To protect sellers from malicious bidders, LiveAuctioneers uses protection guarantees. These guarantees establish a dispute process that is triggered when a bidder fails to pay, allow sellers to contact the leading underbidder, and automatically suspend bidders with two or more disputes on their account.


Trust instruments must keep pace with a changing culture. Platforms can outgrow the policy guidelines from their early days.

IoT (Solution) Ecosystems

For IoT ecosystems, whether B2C (such as smart home systems) or B2B (like production-line devices), quality, of course, matters. But their main trust issue centers on data security. IoT devices capture and share vast amounts of often highly sensitive data, some of it destined for purposes unbeknownst to the customer or user. These can be private conversations or proprietary machine data culled in ambient data collection.

Trust in these ecosystems hinges largely on preventing misuse and maintaining security. How secure are the devices, and how safe is the stored data? Many of the devices are useless without the IoT connection, making trust issues a core concern of the service. Thus, the service's reliability is potentially addressed through product design rather than ecosystem design. These issues are relevant for both consumer and industrial IoT ecosystems.

Key instruments: Access, contracts, controls, and mitigation are the tools best suited for instilling trust in IoT ecosystems. The following two examples illustrate why.

HomeKit, Apple's smart home ecosystem, allows only trusted suppliers on the platform. The MFi program's enrollment verification process includes identity and legal entity status checks (access). It also clearly defines rights and obligations (especially those concerning data sharing) in nondisclosure agreements that providers sign upon joining. Controls also play an important role. Extensive input control (governing the kinds of products and applications allowed on the platform), as well as process control (determining how interactions and fulfillment are regulated), engender trust in the quality of the service and in data ownership structures. The smart home market leans toward more hands-off approaches than do B2B IoT solutions. Samsung's SmartThings, for example, doesn't regulate access but relies on precise use terms (contracts) and a thorough certification process (controls).

In the B2B arena, FieldView, a smart farming ecosystem, offers a good demonstration of trust instruments. Because its participant base is manageable in size, FieldView can afford to grant developers access on a case-by-case basis and allow the terms and conditions of its partnerships to be individually defined. FieldView determines who can access the platform and its data, letting farmers decide similarly on a case-by-case basis who can access their data. This instrument is defined in the terms and conditions of the ecosystem. The platform controls input and process via APIs and individual licensing agreements that regulate the solutions that software developers can offer and how data is shared. Whenever trust is threatened—as was the case in 2019 with FieldView's partnership with Tillable[2]—mitigation instruments kick in. Then, farmers feared their data would be shared without their consent and potentially used against their interests. FieldView listened to its users and terminated the partnership before any breaches could occur.

Financial Ecosystems (Payment, Lending, and Fundraising Platforms)

For financial ecosystems, designed chiefly for transferring or raising money, fraud risk, losses, and security are the main trust issues.

Key instruments: Access—allowing only trustworthy participants—is just the first level of protection for minimizing fraud and losses. Payment platforms like Visa and Mastercard use credit scores to restrict membership and adjust payment limits. In all of the financial ecosystems we analyzed, fraudulent members are excluded. But exclusion has its limits, considering that it is tough, if not impossible, to identify bad behavior up front.

The instruments of choice in such environments are intermediation and mitigation measures. PayPal, for instance, acts as the transaction partner (intermediating transactions), providing guarantees against fraud.

> **Because the range of potential interactions on lending or fundraising platforms is broader than on pure payment ecosystems—consider the greater amount of private data gathered—more can go wrong.**

So, beyond access, intermediation, and mitigation, these ecosystems need to tap other instruments. Kiva, the nonprofit microlending platform, and Kickstarter, the funding ecosystem, tightly control participants' input (the projects) and the process. For example, Kiva works only with financially excluded borrowers and is limited to projects that create social impact in their communities. Additionally, Kiva clearly defines how projects are approved, how funds are deployed, and how debtors are controlled. Both Kiva and Kickstarter also provide transparency to lenders in the form of certifications and recommendations that highlight especially trustworthy projects on the platform. Kiva, for example, features a five-star risk rating system for projects.

2. "Climate FieldView terminates platform partnership agreement with Tillable," *Successful Farming*, February 15, 2020 (https://www.agriculture.com/news/technology/climate-fieldview-terminates-platform-partnership-agreement-with-tillable)

Gig Economy Platforms

Ecosystems that focus on services provided by gig economy workers face another set of trust issues: those centered on the provider's offering, qualifications, quality, and fulfillment performance.

Key instruments: Given their multiplicity of trust issues, gig economy platforms use the greatest number of instruments. These generally include access, controls, transparency, and intermediation.

Access restrictions are vitally important. If the wrong providers are on your platform, users will lose interest, and would-be users won't even show up, thereby critically constraining your growth prospects. Belay Solutions, a virtual staffing company serving the US, hires only US-based, highly skilled, and experienced professionals—regulating access to build trust in the quality of its solution.

Behavior-shaping instruments (controls) represent another way of ensuring that the quality of interactions is sufficiently high. Uber uses process controls to determine the entire value-delivery process—rider matching, pricing, payment, routing—thus shaping drivers' behavior. Airbnb clearly stipulates what tenants are allowed to do in their rented lodging.

Transparency is an important lever for many gig economy platforms because it reduces information asymmetry and makes past behavior relevant.

HopSkipDrive uses driver ratings and safety statistics to generate trust in the platform's value proposition. Airbnb and Uber offer rating systems, not just for end customers to rate providers but also for providers to rate end customers; these systems identify participants from either side who should be barred. And intermediation, in which the orchestrator emerges as a transaction partner, is commonly used by gig economy platforms to shift trust away from individual interactions and toward the platform itself. Through an app, riders pay Uber directly, not their Uber driver; and Uber drivers need not worry about the rider lacking enough money, because Uber guarantees the transaction.

Developing the Right Trust Formula

As leaders look to embed trust into their ecosystems, the ecosystem cluster patterns we uncovered in our bottom-up analysis provide a useful initial framework. (See the sidebar "Proven Trust-Building Principles.") But there is no silver bullet or single formula; successful ecosystems combine multiple trust instruments. They should, therefore, also identify the specific trust challenges they face and pick the right instruments from the trust toolbox we've identified. Choosing at random, even if the instruments seem powerful, is ineffective. It's particularly important to consider the scope and diversity of your ecosystem's interactions; they will indicate the difficulty and complexity of your trust issues. In this way, they can guide your choice of the most appropriate instruments in the best (and most powerful) combination to foster trust in interactions, fuel cooperation, and ultimately boost the ecosystem's overall performance.

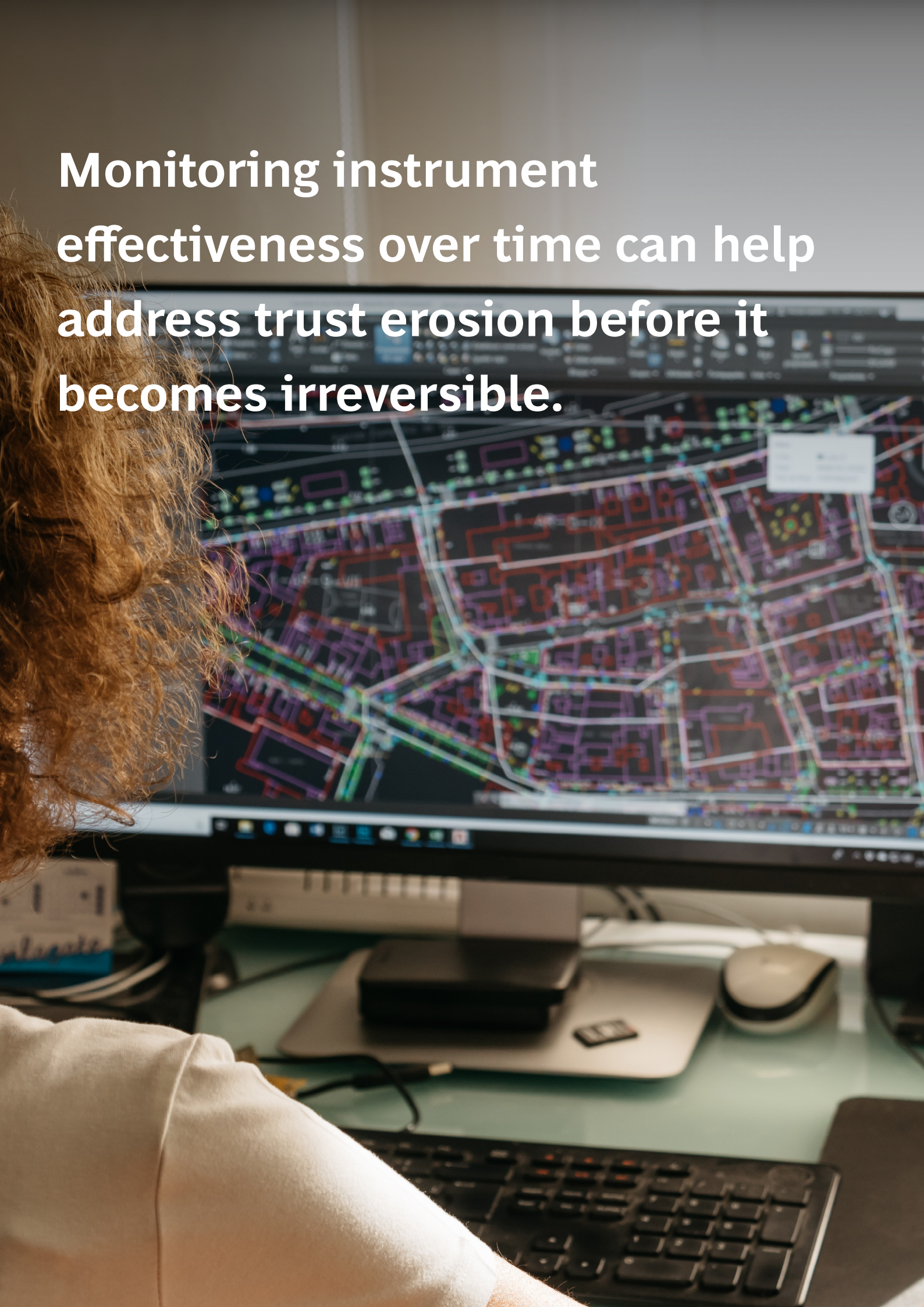
Proven Trust-Building Principles

The following principles and practices gave the success stories in our study a strong foundation of trust.

- Ecosystem orchestrators must be prepared to combine trust instruments from different classes. But they should try to keep the number of trust instruments they deploy as low as possible to avoid complexity.
- Digital plays a crucial role in enabling systemic trust and, in some cases, the very existence of business ecosystems that would otherwise not be viable. However, our analysis shows that a digital-only approach can only go so far. Digital instruments must usually be combined with nondigital ones to build trust effectively.
- Ecosystems should address trust-related issues as early as possible so that these issues don't hamper growth. Trust-related issues can be viewed as weak signals of a vicious cycle of problem and erosion that can prove difficult to revert once fully established. Rethink the entire approach if you observe early signs of trust erosion in your ecosystem.
- Refine and reassess the combination of instruments deployed as your ecosystem scales and matures (as illustrated by our sample's successful social media platforms). Current effectiveness is no guarantee of future effectiveness.
- Utilize the trust instruments to design your ecosystem for repeated interaction. By using the toolbox, you can extend what political scientist Robert Axelrod referred to as "the shadow of the future" and make cooperative behavior rational—even in inherently challenging cases like HopSkipDrive, in which parents entrust strangers with their children's safety.

The broader the set of possible interactions, the more likely adverse events are. Generally speaking, this also means more instruments are needed. Ecosystem orchestrators must remember that the higher the stakes, the greater the potential losses—as the trust imperative grows, participants put even more stock in the trustworthiness of their transaction parties.

A good starting point is to clarify the problem to be solved and the associated trust issues. The ecosystem's lifecycle stage should also figure into your instrument choices. As ecosystems gain scale and mature, their trust challenges often change. Actively monitoring the effectiveness of trust instruments over time—and adjusting them as needed—can help avert trust erosion before it becomes irreversible. Here, again, past success is not a guarantee of future success.



Monitoring instrument effectiveness over time can help address trust erosion before it becomes irreversible.

Critical Design Questions

Clearly, there are many important design decisions to weigh. Start by studying your ecosystem's expected trust-related issues and identify the trust instruments that will help address them. We distilled a selection of key questions and specific guidelines to help orchestrators in this effort.

What must an ecosystem do to convince participants of the quality of the experience? The most effective approaches for ensuring quality are regulating access and controlling supplier input (what partners can offer on the platform). Incentivizing providers to offer high-quality products or services and enhancing transparency are also effective.

When property is the offering—residences, in Airbnb's case, or cars, in Uber's case—the potential for property damage arises, either inadvertent, through sheer use, or through abuse by poorly behaving participants. The most effective measures for instilling confidence and trust and minimizing losses are transparency and banning parties who behave badly, both preventive measures, and compensating for any asset depreciation that occurs.

What if the transaction is susceptible to fraud? Fraud is a considerable problem in many ecosystems. It comes in many forms, but the most common are transactional or financial. Ecosystems have two basic approaches at their disposal: access and mitigation. They can strive to prevent bad outcomes by banning fraudulent parties or applying process controls, and if fraud occurs, they can provide compensation.

On platforms involving the exchange of funds, participants worry about whether they will receive payment. This question arises in situations where the seller does not trust the buyer to pay (in the case of upfront delivery) and instances where money is lent. What works best in such circumstances? Screening of potential participants (for example, through credit scores), closely monitoring inputs and processes on the platform (controls), establishing the platform as the transaction partner (intermediation), or offering compensation when an adverse event occurs.

What if misbehavior leads to uncooperative interactions? Successful ecosystems ensure that partners play by the rules by being selective and, more importantly, by banning partners who misbehave or fail to deliver (access). In such situations, control instruments are the best defense against future adverse events. Transparency also helps lower risk through its deterrent effect on would-be bad actors. Finally, ecosystems with problems that can be resolved through refund can rely on mitigation instruments to earn and sustain trust.

Asymmetry of information complicates trust building. The greater a party's information advantage, the easier it is to abuse it. In ecosystems with great information asymmetries, such as used goods marketplaces, transparency tools lessen the information divide, and mitigation instruments ensure that the more knowledgeable party is held accountable for any misbehavior. Contracts are inherently imperfect because it is impossible to anticipate every kind of adversity that could arise or identify every possible contingency. Thus, most contracts contain a clause that designates intermediation through a neutral arbitrator to resolve any contractual conflicts.

What if participants question the ecosystem's security (virtual or physical)? As soon as sensitive data is involved, the risk of data misuse increases. Rigorous data governance instruments need to be in place to mitigate those risks. Successful ecosystems typically restrict access to trustworthy partners, define data usage and access rights in contracts, and closely control partners' behavior on the platform.

Many ecosystems penetrate participants' personal lives, either through social connection online or direct contact (in the case of personal services, such as ride hailing or home cleaning). The threat to a participant's personal security is, of course, one of the worst possible outcomes. Clearly, mitigation instruments are insufficient. Ecosystems must actively prevent bad behavior. Access instruments, along with control instruments that monitor platform users' behavior, are the most effective weapons in their trust arsenal.

What if participants mistrust the ecosystem orchestrator? It's not enough to build trust among participants; participants must have trust in the ecosystem orchestrator. Partners are free to engage in ecosystems and walk away from them at will. Orchestrators must internalize the fact that ecosystems compete on trust. Trust is, in effect, the lifeblood of ecosystems. An ecosystem's success is often built on the belief that the orchestrator will not misuse its platform dominance. We see this in the compact between independent software developers and large tech companies that own a platform (iOS for Apple, Windows for Microsoft). Software developers must trust that these companies will not take advantage of their dominance, that they won't change the rules for enterprise apps, and that they will honor their monetization models. Orchestrators can build this trust through contracts and transparency. But most importantly, they must consistently prove it through their behavior.

Embedding trust requires a mindset shift away from the naive belief that trust will spontaneously emerge among complete strangers. Trust cannot simply be treated as an after-the-fact consideration. As successful ecosystems demonstrate, trust must be front and center in designing ecosystems with the strength and resilience to thrive amid the challenges of the future. By fostering interaction and cooperation, trust not only helps ecosystems fulfill their value proposition but also becomes a source of competitive advantage.

The art and science of achieving this advantage reside in determining the right combination of trust instruments for an ecosystem's distinct needs and issues—in essence, designing ecosystems for systemic trust and making the enabling instruments observable and manageable in a true bionic fashion. The recommendations based on the patterns we've described represent the first step companies can take to understand trust and bolster both competitive advantage and resilience.

About the Authors

Marcos Aguiar is a managing director and senior partner in the São Paulo office of Boston Consulting Group and a fellow of the BCG Henderson Institute. You may contact him by email at aguiar.marcos@bcg.com.

Ulrich Pidun is a partner and director in BCG's Frankfurt office and a fellow of the BCG Henderson Institute. You may contact him by email at pidun.ulrich@bcg.com.

Santino Lacanna is a principal in the firm's São Paulo office and an ambassador to the BCG Henderson Institute. You may contact him by email at lacanna.santino@bcg.com.

Niklas Knust is a consultant in BCG's Cologne office and an ambassador to the BCG Henderson Institute. You may contact him by email at knust.niklas@bcg.com.

Matt Williams is a consultant in the firm's Washington, DC office and an ambassador with the BCG Henderson Institute. You may contact him by email at williams.matthew@bcg.com.

François Candelon is a managing director and senior partner in BCG's Paris office. He is the global director of the BCG Henderson Institute. You may contact him by email at candelon.francois@bcg.com.

For Further Contact

If you would like to discuss this report, please contact the authors.

BCG

BCG HENDERSON INSTITUTE