THINKING OUTSIDE THE

BLOCKS

```
"hash":"f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e
_sz":1,"vout_sz":2,"lock_time":0,"size":275,"in":[{"prev_out":{"hash":
d2324359c2d0ba26006d92d856a9c20fa0241106ee5a597c9","n":0},"scriptSig":
932b8af514961a1d3a1a25fdf3f4f7732e9d624c6c61548ab5fb8cd4”}]{"hash":"f4
3783cf57adfe4c75c605f6356fbc91 0e9831e9e16","ver":1,"vin_sz":1,"ve
```

BCG PERSPECTIVES

THINKING OUTSIDE THE BLOCKS

A Strategic Perspective on Blockchain and Digital Tokens

Philip Evans
with
Lionel Aré
Patrick Forth
Nicolas Harlé
Massimo Portincaso

INTRODUCTION

Coded by an unknown hacker, germinating in the netherworld of cypherpunks, Bitcoin was not discovered by the business mainstream until 2015. Just as punk rock was repackaged as new wave, so was Bitcoin domesticated into blockchain. It burst on to the popular imagination and the conference circuit. Visionary Don Tapscott affirmed, “I’ve never seen a technology that I thought had greater potential for humanity.” CEOs pointedly asked whether this was yet another disruptive technology. Their subordinates were set to investigate how it might work. And they found that it is all rather complicated.

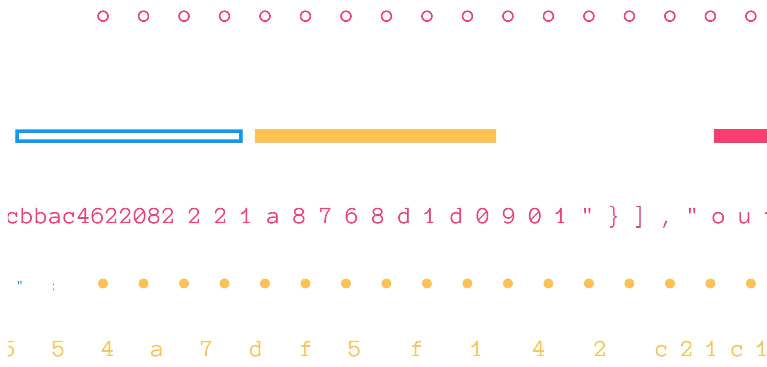
Hints of disillusion. Time, perhaps, for some strategic analysis.

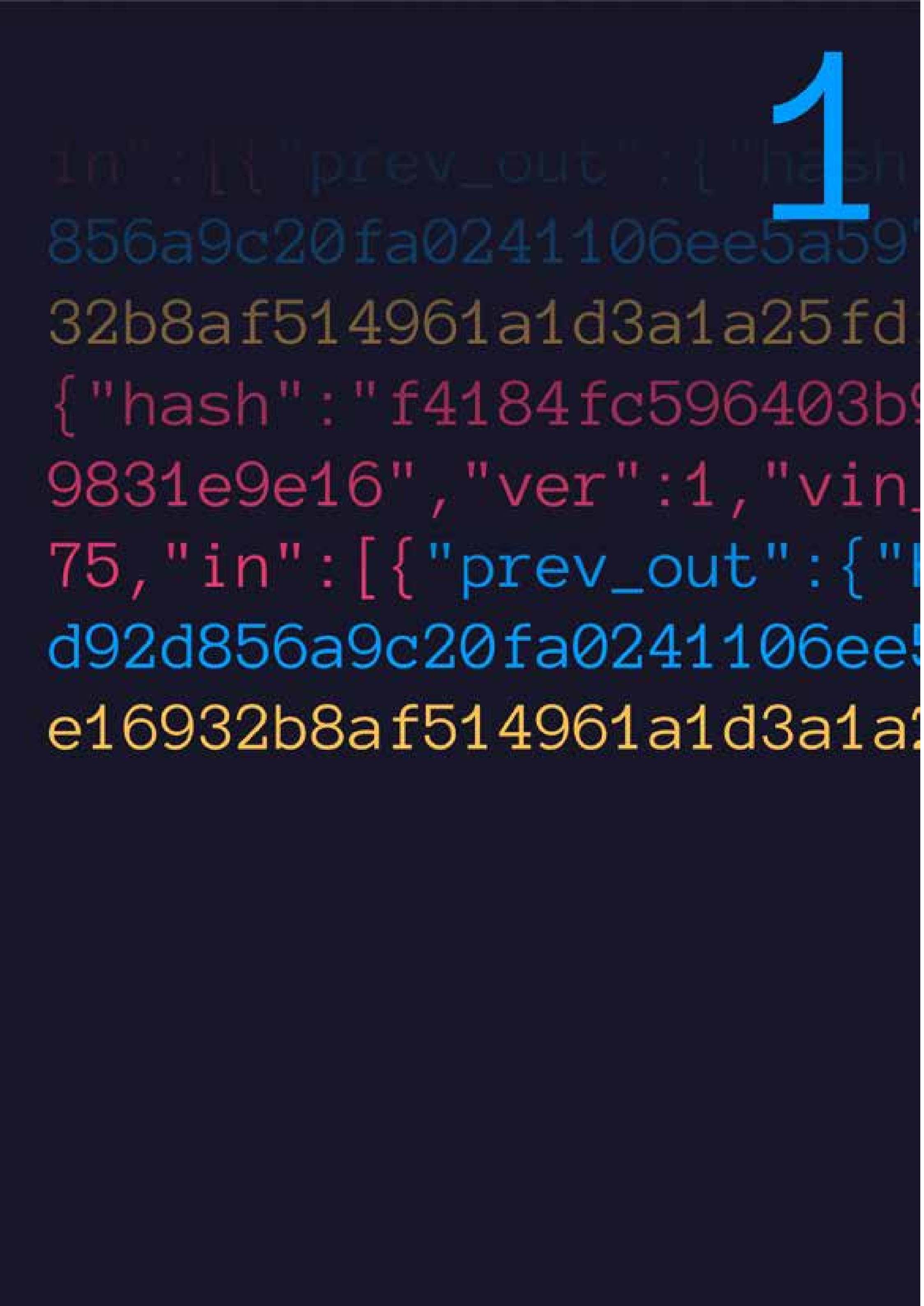
The truly disruptive technical advances of the past decades, the PC and the internet, had something in common. They wasted a newly cheap resource—computing power and bandwidth, respectively—to do something radically new. Digital tokens and blockchains, two distinct but complementary technologies, waste cheap storage to give data the continuity of real-world assets. Bitcoin is just the first application. The technologies are far from mature, but if scalability limitations are overcome, they will have long-term disruptive potential in complex transaction networks such as trade, health care, and the Internet of Things. And it is by no means obvious that traditional intermediaries will be able to control them.

This essay outlines how the economics of transaction costs and trust could be reshaped by tokens and blockchains and by the stacked architecture on which they are built. The aim is not to prescribe exactly what leaders should do (every business is unique, and the devil is in the details) but to provide a strategic context to help executives frame the right questions. For example:

- Which aspects of my organization are vulnerable to disintermediation and how likely is it to happen?
- Where likely, how do I need to rethink and reshape my existing business—before others do it for me?
- Where can I take advantage of blockchain-enabled digital continuity to build new offerings and business models?
- Where blockchain-based solutions are advantageous, should I go it alone or collaborate for decisive scale?

To begin at the beginning...


cbbac4622082 2 2 1 a 8 7 6 8 d 1 d 0 9 0 1 " }] , " o u
5 5 4 a 7 d f 5 f 1 4 2 c 2 1 c 1



BITCOIN

In the winter of 2014, Ukraine was on the brink of revolution. Protesters in Kiev held signs for the television cameras asking for money. (SEE EXHIBIT 1.) The signs bore a QR code that allowed donors to send bitcoin to the protest movement. Thousands around the world pointed their cellphone cameras at the on-screen video and made donations with literally three clicks. The transactions were communicated in 20 seconds and confirmed within ten minutes at a cost of a fraction of a cent per dollar. They were anonymous: the government could not monitor them, and the recipients did not know whom to thank.

EXHIBIT 1

Exhibit 1: Paying with bitcoin is direct, anonymous, and irrevocable–highly desirable characteristics for these Ukrainian protesters.

SOURCE: OLGA BONDARCHUK. USED WITH PERMISSION.

A donor could have made the same gift through the banking system, but that would have required detailed (and politically compromising) information about the recipient's bank account, if he or she had one. It would have cost a commission of 10% or more, and taken three or four days to complete. PayPal, of course, would have been quicker and cheaper but was banned by the Ukrainian government. Paying with bitcoin was direct, anonymous, and irrevocable—like a sympathetic onlooker crossing Maidan Nezalezhnosti, the central square in Kiev, and dropping a couple of *hryvnia* into a plastic cup.

> **DIGITAL TOKENS AND BLOCKCHAINS, TWO DISTINCT BUT COMPLEMENTARY TECHNOLOGIES, WASTE CHEAP STORAGE TO GIVE DATA THE CONTINUITY OF REAL-WORLD ASSETS. BITCOIN IS JUST THE FIRST APPLICATION.**

That is not just a figure of speech. A bitcoin is a digital bearer instrument: ownership and control are the same thing.[1] There is no need for a Bitcoin "account": you simply hold bitcoins, just like the coins in your pocket. Like notes and coins, they can be lost or stolen, and transactions are irrevocable. As a medium of exchange, Bitcoin can be ten times more efficient than traditional payment methods, but when the cost of transacting in and out of fiat (government minted) currency is included, it is not obvious that it is cheaper. It offers anonymity: a nobler feature in the cause of democratic revolution than of money laundering or tax evasion.

Some libertarians see bitcoins as "digital gold": the incorruptible global currency that will ultimately replace the fiat currencies manufactured and debased at whim by central and commercial bankers. But as JPMorgan Chase CEO, Jamie Dimon, has vigorously pointed out, if Bitcoin came anywhere near to supplanting conventional currencies, central bankers would almost certainly intervene to stop it.[2] So Bitcoin as a currency is destined to fill a small niche in the payments system, a brilliant but highly circumscribed invention.

HOW BITCOIN WORKS

The phenomenon we know as Bitcoin depends on two complementary technologies—digital tokens and blockchain—that together facilitate digital identity, ownership, transactions, contracts, and trust.

To learn more, read the related article on page 60.

From a strategic point of view, Bitcoin's importance is less as a currency and more as the early manifestation of its two underlying technologies: token (in this case, bitcoin) and blockchain. A token need not be a digital coin; it can be any kind of digital asset or any digital representation of a physical asset.[3] And a blockchain (including the Bitcoin blockchain) can serve as a shared, secure, irrevocable, and trusted ledger for any kind of transaction. So although the majority of applications running today are in payments, the intriguing question is not specific to currency, or even banking; it is whether the two underlying Bitcoin technologies—token and blockchain—can serve as foundations for other applications.

The possibilities extend far beyond financial services, to supply chain documentation, land registries, health records, microtransactions, and smart contracts among billions of intelligent devices worldwide.

Venture funds and technology companies have committed over $1 billion to using these technologies to disrupt whole industries—or maybe to selling themselves and their services to incumbents to forestall such disruptions.

So what principles of economics and strategy will govern this brave new world?

[1] By convention, the digital payment system is Bitcoin (with a capital B); the unit of currency is bitcoin.

[2] See "Jamie Dimon: You're Wasting Your Time with Bitcoin," *Fortune*, November 4, 2015, video, http://fortune.com/video/2015/11/04/jamie-dimon-youre-wasting-your-time-with-bitcoin/.

[3] Blockchains unrelated to payments may still need a digital coin in order to reward nodes for providing the validation service.

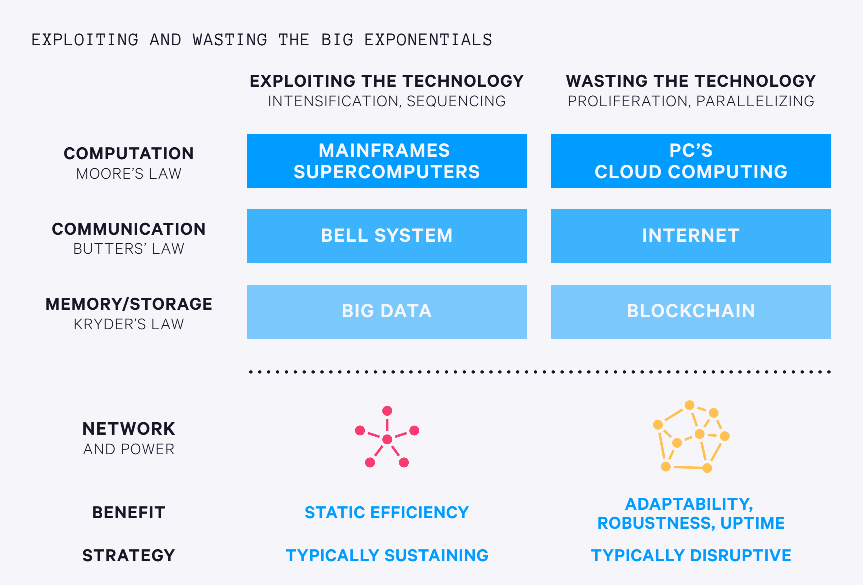
2

```
{"hash":"f4184fc596403b9d638783cf57adfe4c75c605f6356fbc913385
1,"vin_sz":1,"vout_sz":2,"lock_time":0,"size":275,"in":[{"pre
cd7f8525ceed2324359c2d0ba26006d92d856a9c20fa0241106ee5a597c9"
"304402204e45e16932b8af514961a1d3a1a25fdf3f4f7732e9d624c6c615
22ec8eca07de4860a4acdd12909d831cc56cbbac4622082221a8768d1d090
```

WASTING RESOURCES

Blockchain and digital tokens deliberately waste storage, which is cheap, to create something new that is valuable. This is actually the third chapter in an old story. Over the past 50 years, the information revolution has been propelled by exponential advances in the cost, speed, and capacity of three functions: computing, communication, and memory/storage.[4] Organizations have exploited these "big exponentials" in two ways. Incumbents compute more, communicate more, and store more data to run their businesses more efficiently, to create better and cheaper products, and to enable extensions to their current business models. But at some point, a resource becomes so cheap and abundant that

EXHIBIT 2



EXPLOITING AND WASTING THE BIG EXPONENTIALS

	EXPLOITING THE TECHNOLOGY INTENSIFICATION, SEQUENCING	WASTING THE TECHNOLOGY PROLIFERATION, PARALLELIZING
COMPUTATION MOORE'S LAW	MAINFRAMES SUPERCOMPUTERS	PC'S CLOUD COMPUTING
COMMUNICATION BUTTERS' LAW	BELL SYSTEM	INTERNET
MEMORY/STORAGE KRYDER'S LAW	BIG DATA	BLOCKCHAIN
NETWORK AND POWER		
BENEFIT	STATIC EFFICIENCY	ADAPTABILITY, ROBUSTNESS, UPTIME
STRATEGY	TYPICALLY SUSTAINING	TYPICALLY DISRUPTIVE

wasting it to create something completely different makes economic sense.

PCs were less efficient than mainframes, but they gave end users greater control. PCs disrupted the mainframe industry. The internet was vastly less efficient than hierarchically switched telecommunications architecture, but it offered robustness and shifted the locus of innovation to the periphery. The internet disrupted everything.

Memory and storage are now following that same pattern. With cost per terabyte in free fall, the first response is to accumulate more data—hence, big data. But what can you create if you *waste* storage? Bitcoin, for one thing. The Bitcoin blockchain provides an inviolable record of each bitcoin's history at the cost of storing each transaction record 5,700 times over.

Exhibit 2: At some point, resouces becomes so cheap and abundant that wasting it to create something completely different makes economic sense.

SOURCE: BCG ANALYSIS

Thus blockchain is the disruptive technology for storage, as the PC was for computation and the internet for communication. It is the last response to the transformative power of the big exponentials.[5] (SEE EXHIBIT 2.)

But what exactly is achieved by wasting storage?

[4] Ray Kurzweil brilliantly describes exponential technologies in chapters 1 and 2 of *The Singularity Is Near: When Humans Transcend Biology*, Viking Press, 2005.

[5] One of the ironies—indeed, the contradictions—of Bitcoin is that to secure the network it extravagantly wastes another resource: energy. This heavy carbon footprint limits its scalability—a point to which we shall return.

3

```
{"hash":"f4184fc596403b9d638783cf57adfe4c75c605f6356fbc913385
1,"vin_sz":1,"vout_sz":2,"lock_time":0,"size":275,"in":[{"pre
cd7f8525ceed2324359c2d0ba26006d92d856a9c20fa0241106ee5a597c9"
"304402204e45e16932b8af514961a1d3a1a25fdf3f4f7732e9d624c6c615
22ec8eca07de4860a4acdd12909d831cc56cbbac4622082221a8768d1d090
```

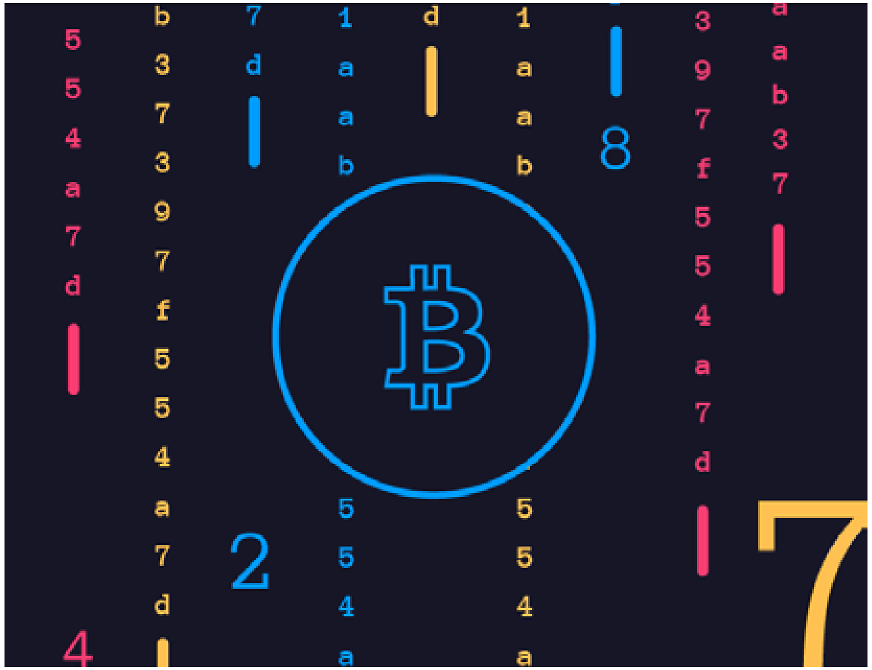
VIRTUAL CONTINUITY

Digital tokens such as bitcoin waste storage in massively duplicative blockchains to create virtual *continuity*. This is the fundamental breakthrough. Continuity—outside the domain of quantum physics—is a universal property of the physical world. If I pass an object behind my back, you can be reasonably sure that what reappears in my left hand is what disappeared from my right. Continuity permits identity of both things and people; it permits property because a continuously identified thing can be owned by a continuously identifiable person. It therefore permits transactions—transfers of property. It permits trust.[6] Microeconomics is predicated on contracts, which in turn are predicated on identity, property, transactions, and—often—trust. So the whole panoply of the capitalist system is predicated on continuity. Continuity is not sufficient for property and contracts (you also need law), but it is necessary. This point is so obvious that no economics textbook even mentions it. Signatures, passports, notaries, seals, chops, photo IDs, and so forth all scale and extend continuity in the real world.

But in the virtual world, there is no continuity. There is no guarantee—indeed, generally no meaning in saying—that a string of data is an original as opposed to a copy. Neither an object nor a person has identity. The old joke: on the internet nobody knows you're a dog. In many contexts, of course, that is a desirable feature. It lowers the cost of broadcasting and relaying information to near zero. But absent continuity, there is no peer-to-peer basis for identity, ownership, transactions, trust, or contracts.

> **“**
>
> **THE TECHNOLOGIES OF TOKEN AND BLOCKCHAIN ENDOW DATA WITH CONTINUITY: THEY MAKE THE VIRTUAL REAL.**

Where the parties have a prior real-world relationship, they can establish a virtual equivalent directly through encryption. But otherwise, the world addresses the lack of virtual continuity through intermediaries. I have a real-world relationship with my bank, for example, you have a real-world relationship with yours, and the banks have real-world relationships with one another. Collectively, intermediaries (of which banks are just one type) guarantee our respective virtual identities and mediate our transactions.



There are two problems. When there is just one intermediary, it will be a monopolist, which—if profit maximizing—will underinvest, overprice, and appropriate most of the value. But if instead the market is competitive, the intermediaries themselves require intermediation. In the multilayered system of international remittances, a money transfer to Kiev generates multiple transactions, delays, duplicated effort, and errors.

Bitcoin demonstrates the revolutionary potential of tokens and blockchains. As explained on page 61, it establishes continuity between two sequential transactions, say X and Y. Although it is just a string of numbers, the structure of the bitcoin—the token—guarantees its “ancestry”: the coin in the earlier transaction X is the only “parent” of transaction Y. The authenticity of the coin can therefore be proved by tracing it back to its original mining.

SEVEN POSSIBLE KILLER APPS FOR BLOCKCHAIN AND DIGITAL TOKENS

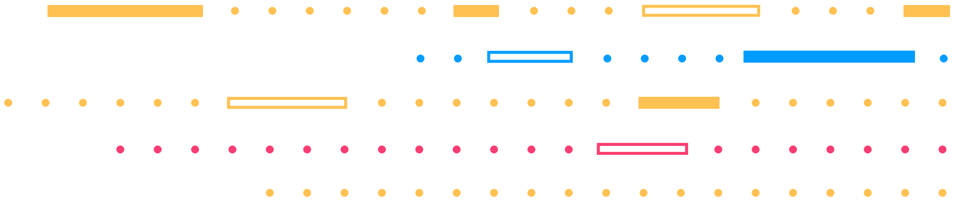
Beyond payments, there are many applications that could benefit from decreased transaction costs, a neutral shared database, and the superior security of a shared ledger.

To learn more, read the related article on page 65.

And the blockchain guarantees “inheritance”: the coin in the later transaction Y is the only “child” of transaction X. The coin cannot be spent twice. So the two aspects of Bitcoin technology together waste storage in order to create virtual continuity. Virtual continuity enables digital identity, ownership, transactions, and trust—and contracts and markets—among parties with no prior relationship and without intermediaries.

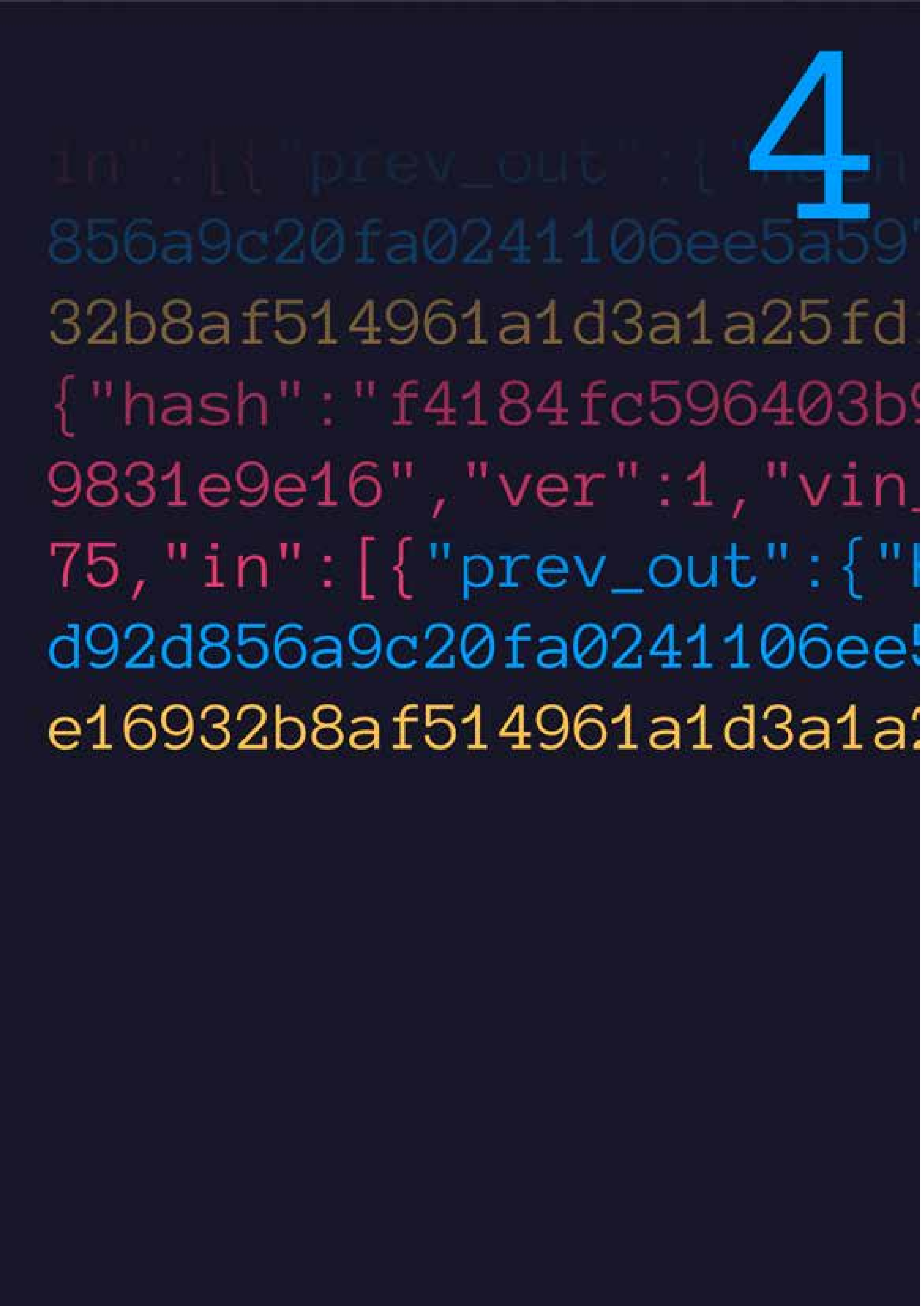
The technology is potentially disruptive to all virtual intermediaries. Its disruptiveness is proportional to the cost, complexity, and degree of transaction duplication in the current system of intermediation.

Virtual continuity leads to one final symmetry. Recent technology waves—notably the Internet of Things, the proliferation of smart mobile devices, and augmented reality—directly endow physical objects with information and intelligence: *they make the real virtual.* The technologies of token and blockchain, conversely, endow data with continuity: *they make the virtual real.* When the real and the virtual converge, it is as if our world and our map of the world become the same thing.[7]



[6] On the impact of technology on trust, see Philip Evans, “From Reciprocity to Reputation,” BCG Perspectives, April 2006.

[7] This broad convergence of the real and the virtual is facilitated by the interaction of four mutually multiplicative and very recent technologies: the Internet of Things, big data, artificial intelligence, and mobile devices. See Philip Evans and Patrick Forth, “Borges’ Map: Navigating the World of Digital Disruption,” BCG article, April 2015.



4

STACKED ARCHITECTURE

Bitcoin has a stacked architecture that serves as the model and template for all other tokens and blockchains. (SEE EXHIBIT 3.) A stack is a set of interoperable modules arranged in a hierarchy. Upper-level functions depend on lower-level functions, but not the reverse. General-purpose functions needing scale and reliability reside at the bottom of the stack (the infrastructure), while functions benefiting more from customization, experimentation, and innovation occupy the upper layers.[8] Interoperability among the layers permits the system to be both efficient (at the bottom) and adaptive (at the top). The internet has a stacked architecture.

EXHIBIT 3

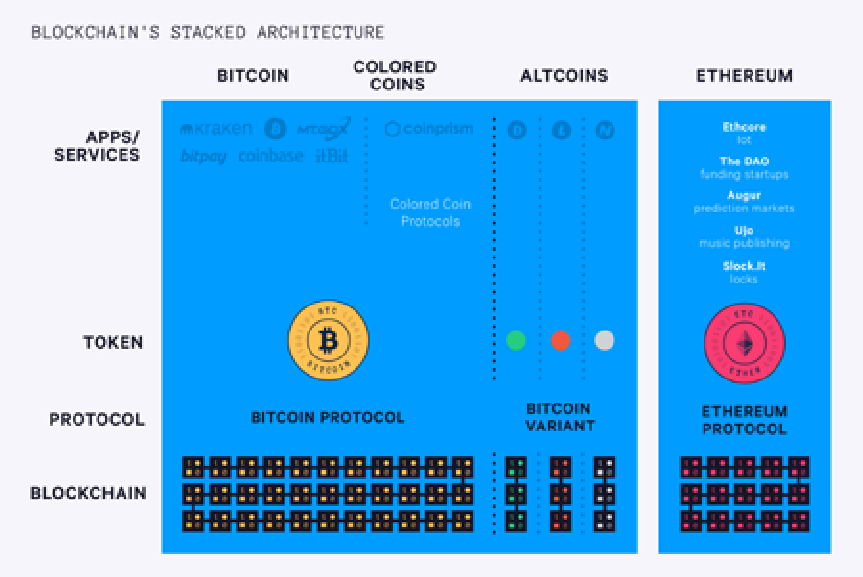


Exhibit 3: Blockchains and digital tokens are two key elements of a four-layered technical architecture.

SOURCE: BCG ANALYSIS

With Bitcoin, the economics of each layer are radically different.

BLOCKCHAIN

At the bottom of the stack is the Bitcoin blockchain: a database of all transactions, grouped into "blocks" and replicated across thousands of "nodes." It is monolithic and scale sensitive (there is only one), and it becomes more reliable and robust as the number of nodes (currently 5,700) and the number of blocks (currently 430,000) continue to grow. Physically, these nodes are racks of dedicated computing devices, operated in data centers owned by so-called mining pools and concentrated mainly in China. Mining is a for-profit, commodity business.

PROTOCOL

The Bitcoin protocol—its "operating system"—sits on top of the blockchain. This is free, open-source software, maintained by the Bitcoin Core team. Like Linux, it has the strengths of the open-source "business model": rigorous code testing by all comers, rapid improvement cycles, and trust in the collective product because nobody owns it. It also has the model's weakness: the difficulty of making strategic choices by consensus.

TOKENS

Bitcoins themselves are the next layer. They are tokens that are exchanged within the system and minted by miners (the network of nodes that validate transactions) as a reward for validating transactions. Like any medium of exchange, the tokens have value only because people think that other people think they have value. The first known bitcoin purchase occurred in 2010, when Hacker Laszlo Hanyecz bought a couple of Papa John's pizzas with 10,000 freshly mined bitcoins. Today those bitcoins are worth more than $6 million.

APPLICATIONS AND SERVICES

Applications and services make up the top layer and consist of "wallets" (software to hold and manage bitcoins on a smartphone or computer); exchanges that convert bitcoins to and from fiat currency; and information services. There are hundreds of such products and services, chiefly developed by startup companies.

The bottom of the stack, the Bitcoin blockchain, is extraordinarily secure. The total value of all bitcoin—some $10 billion—is a sufficiently rich honeypot to have tempted the best hackers in the world, yet the blockchain has never been successfully attacked. The top of the stack is another story, with claims of incompetence and criminality circulating around such well-known failures as Mt Gox and Silk Road. But the beauty of stacked architecture is that the moral and economic frailty at the top does not compromise the revolutionary robustness at the bottom.

As shown in Exhibit 3, this stacked architecture defines the recombinatorial framework within which new currencies, new services, and entirely new concepts have been developed.

COLORED COINS

Colored coins are top-of-stack innovations that exploit a blank field within each bitcoin to record unrelated data. The UK-based company Everledger, for instance, initially leveraged bitcoins to put "bling on the blockchain" by recording some 40 unique, laser-read identifiers of a diamond, providing proof of provenance and ownership. The bitcoin was not used to buy the diamond, just to create an inviolable record of the transfer of a specific authenticated stone. The same approach could be used to track any valuable asset with a complex transaction history. [9]

ALTCOIN

Altcoins borrow most or all of the Bitcoin protocol to create a separate token with its own stack. Many are exotically named jokes or Ponzi schemes: BaconBitsCoin (symbol: YUM), Kimdotcoin (KOIN), and Zombiecoin (ZMB), among others. However, some are more ambitious tweaks on the Bitcoin protocol. Litecoin, for example, is designed to produce blocks at a faster rate and with less computation than Bitcoin, and Monero pools transactions to prevent even pseudonymous tracing of payments.

ETHEREUM

Ethereum is an entirely new stack, which only a year after its launch, in July 2015, had a market value of nearly $1 billion. Many call it Bitcoin 2.0. Ethereum has its own blockchain and token (ether), and a protocol that supports not just payments but programmable transactions: "smart contracts" that are executed in code, not law.[10] Its creator, Vitalik Buterin, describes Ethereum as "the world computer." Ethereum has nurtured a rapidly growing ecosystem of applications, with (perhaps predictably) mixed results. Notably, The DAO (a DAO is a decentralized autonomous organization) was an attempt to build a venture funding "company" from Ethereum smart contracts alone. In June 2016, after raising an unprecedented (and unanticipated) $130 million in ether, it was defrauded and collapsed. But the vulnerability was in the DAO programming. Open-source developers building applications beyond payments continue to focus on Ethereum as their preferred platform.

PERMISSIONED BLOCKCHAINS

Permissioned blockchains deviate substantially from the open Bitcoin paradigm, restricting certain roles or access to a club of participants, typically financial institutions. Only members are variously allowed to inspect the blockchain, engage in transactions, and operate as a processing node. Permissioned blockchains allow transactions to be written in legal language as well as in computer code; they also enable regulatory review. Today they are only at the proof-of-concept stage, but consortia such as R3 CEV in banking and many financial technology companies are focused on making permissioned blockchains a reality, especially for clearing and settling transactions in securities and foreign exchange.

[8] This is a crude summary of the "end to end" principle first proposed by Jerry Saltzer, David Reed, and David Clark in "End-to-End Arguments in System Design," *ACM Transactions on Computer Systems*, November 1984.

[9] Everledger subsequently shifted from the Bitcoin to the Hyperledger platform and is thus no longer a colored coin.

[10] "Smart contracts" are not legal contracts. A typical contract puts ethers into escrow on initiation and releases them when defined conditions have been fulfilled. It thus substitutes computer code for legal code. In theory, a party injured by such a contract could litigate. In practice, it might be hard to determine jurisdiction or even the identity of the counterparty.

5

{"hash":"f4184fc596403b9d638783cf57adfe4c75c605f6356fbc913385
1,"vin_sz":1,"vout_sz":2,"lock_time":0,"size":275,"in":[{"pre
cd7f8525ceed2324359c2d0ba26006d92d856a9c20fa0241106ee5a597c9"
"304402204e45e16932b8af514961a1d3a1a25fdf3f4f7732e9d624c6c615
22ec8eca07de4860a4acdd12909d831cc56cbbac4622082221a8768d1d090

PERIPHERAL TRUST

Distributed ledgers are often described as a “trustless” systems, but that is not quite right. More precisely, their locus of trust moves to the periphery.

When Everledger certifies a diamond, you know with blockchain-level certainty that someone possessing Everledger’s private key posted certain data on a certain date. But you still have to trust Everledger. Everledger therefore relies on a global network of industry-respected certification houses to authenticate the diamond.[11] Everledger inscribes its certification into the blockchain, along with associated data points and high-res photography, to create a digital record of provenance for the stone. Under an Ethereum smart contract for crop insurance,

EXHIBIT 4

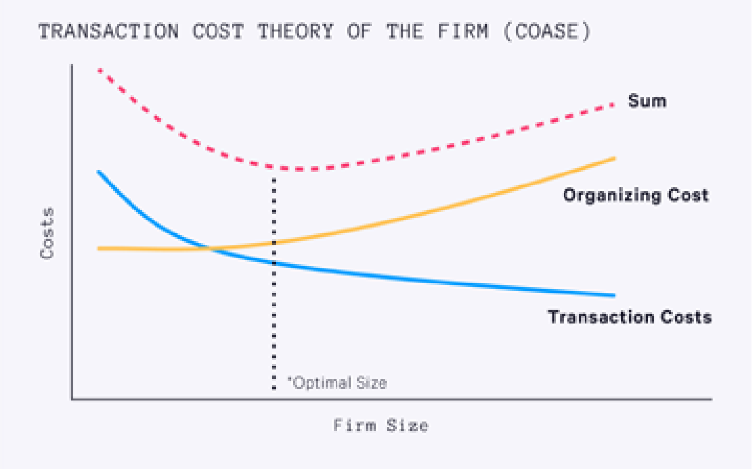


EXHIBIT 5

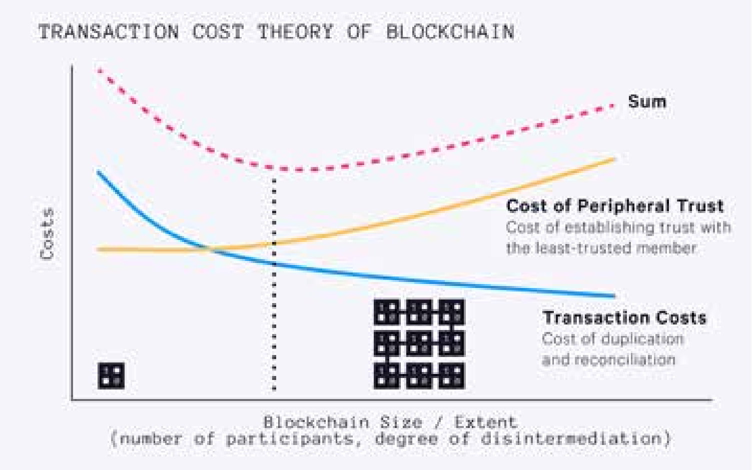


Exhibit 4: The optimal size of the firm is determined by the tradeoff between transaction costs, which decrease with scale, and organizing cost, which increases.

Exhibit 5: The optimal size of a blockchain is determined by the tradeoff between transaction costs, which improve with scale, and peripheral trust, which deteriorates.

SOURCE: BCG ANALYSIS

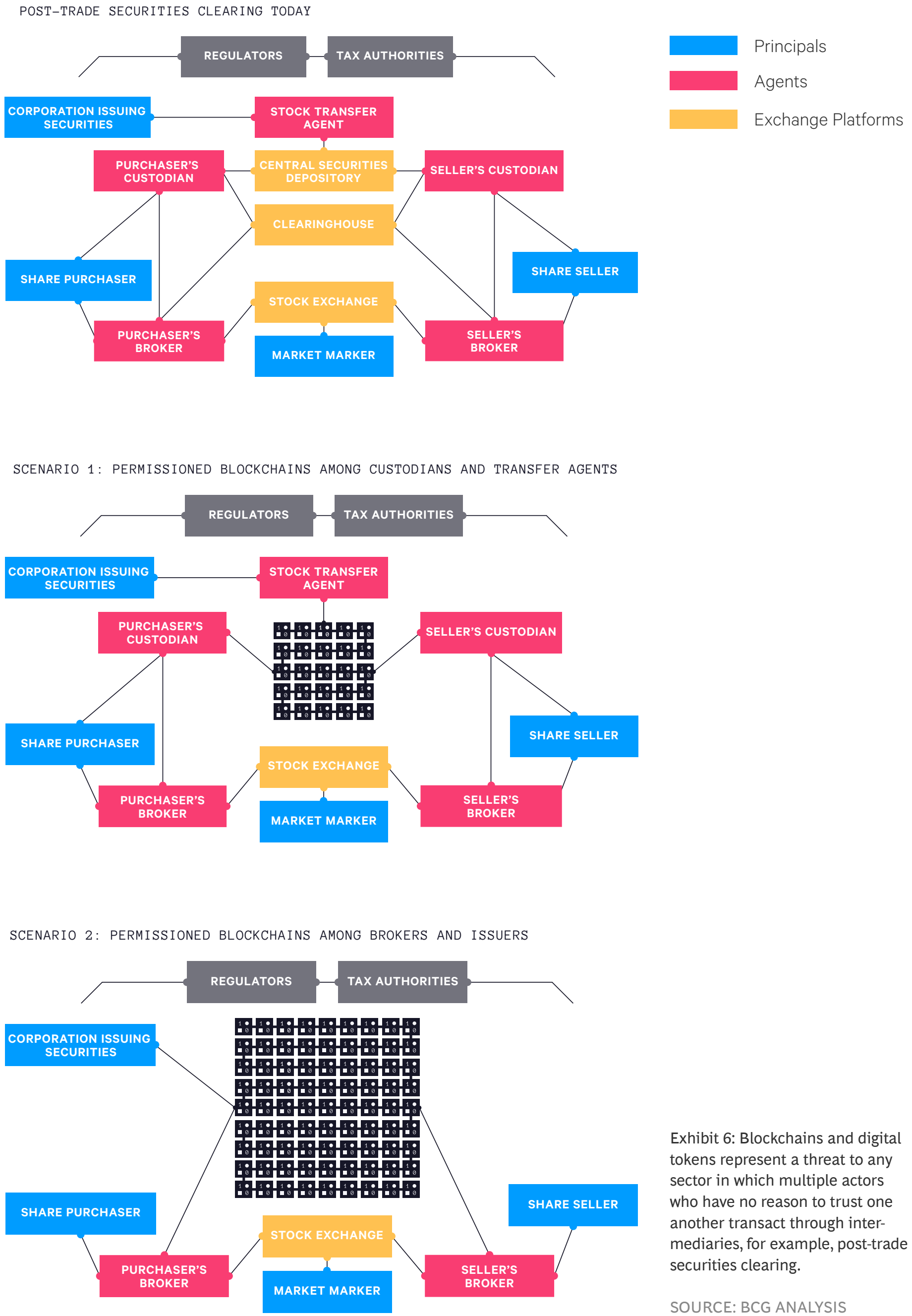
all parties still need to trust the "oracle" that posts weather data to the blockchain. With the exception of tokens that represent assets created within the chain itself (that is, digital coins), tokens are only as trustworthy as the party that originally posted the real-world data that they represent.

This leads to what we might term a Coasean theory of blockchains. Ronald Coase famously posited that corporations exist to economize on the transaction costs of markets. But when some degree of scale is reached, organizational complexity overwhelms. The optimal size of the company, according to Coase, is therefore the point at which the incremental benefit from transaction cost savings is offset by the incremental cost of complexity. (SEE EXHIBIT 4.)

Blockchains similarly exist to economize on transaction costs: they protect a common database from failure or attack; they eliminate duplicate record keeping and associated delays and errors; and they convey trust transitively across the network. But the larger or more comprehensive the blockchain, the less trustworthy is the data entered by the least trustworthy member. Thus, the optimal size of a blockchain is determined by the tradeoff between transaction costs, which improve with scale, and peripheral trust, which deteriorates. (SEE EXHIBIT 5.)

This is not mere theory. One of the most scrutinized uses of a blockchain is for the clearing and settlement of securities transactions, currently a complex network of brokers, custodian banks, stock transfer agents, regulators, and depositories. A single transfer can require a dozen intermediary transactions, and typically takes three days. Some 20% generate errors, which must be corrected by hand.

EXHIBIT 6



POST-TRADE SECURITIES CLEARING TODAY

SCENARIO 1: PERMISSIONED BLOCKCHAINS AMONG CUSTODIANS AND TRANSFER AGENTS

SCENARIO 2: PERMISSIONED BLOCKCHAINS AMONG BROKERS AND ISSUERS

Exhibit 6: Blockchains and digital tokens represent a threat to any sector in which multiple actors who have no reason to trust one another transact through intermediaries, for example, post-trade securities clearing.

SOURCE: BCG ANALYSIS

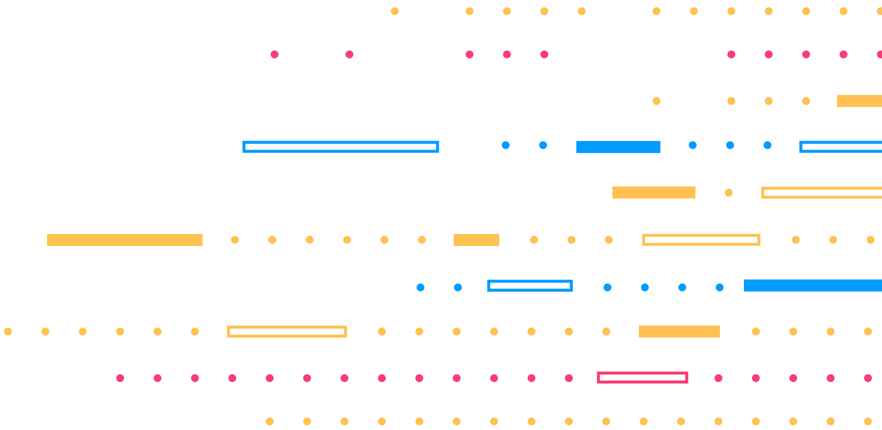
With a blockchain, two trading parties could read and write to a common, trusted, and error-free database. The transaction could be written in legal language as well as in computer code, so that the data exchange itself is the settlement. And it could be visible to regulators but not to other institutions. This is the concept behind Corda, a permissioned blockchain protocol under development by the R3 CEV consortium. It would eliminate bilateral errors and perhaps be cheaper than modernizing existing settlement platforms—the focus is on efficiency, not disruption.

But why stop there? The brokers (as agents of the buyer and seller) could trade on a larger blockchain to disintermediate the custodians, thereby further reducing total transaction costs. Institutions issuing securities, such as corporations and municipalities, could issue them directly onto the blockchain, thereby disintermediating their stock transfer agents. (SEE EXHIBIT 6.)

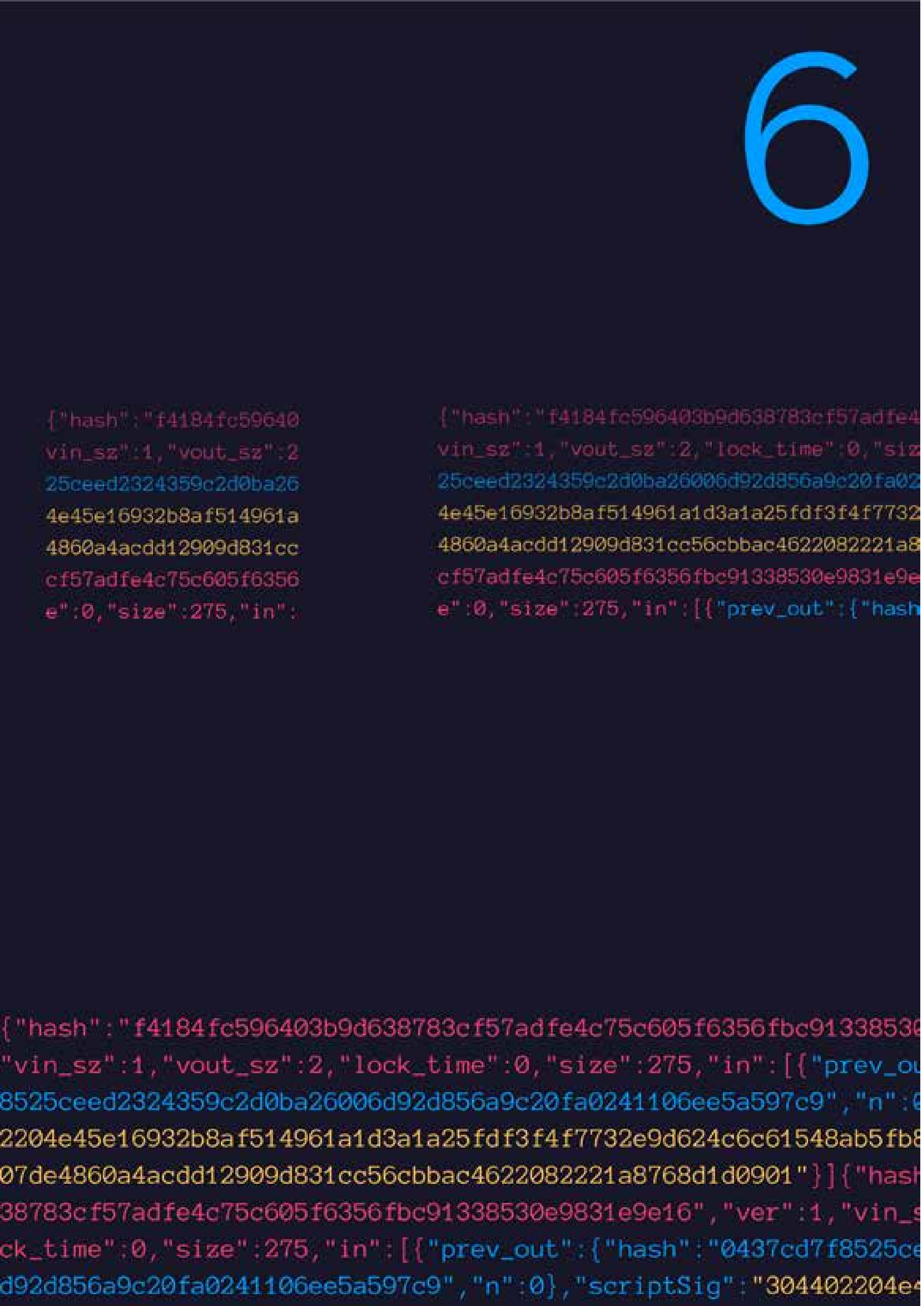
What limits these more ambitious solutions is peripheral trust. Some 50 regulated global banks might have sufficient reason to trust one another's honesty and competence. But for hundreds of brokers and thousands of issuing institutions, trust would be much, much harder to achieve. Hence the tradeoff between transaction costs and peripheral trust.

One can imagine a permissioned securities blockchain starting small but evolving to progressively larger scale and lower costs, as methods are developed to qualify the trustworthiness of additional participants. But there is a radical, if speculative, alternative: significant functions currently performed by "securities" could be performed by new, deconstructed smart contracts that are denominated in tokens native to some blockchain.

For those contracts, peripheral trust would be a lesser constraint, perhaps irrelevant. Such a blockchain would disrupt the club of trusting intermediaries, directly connecting the principals who create, buy, and sell the contracts. “Securities trades” would then be as fast, cheap, and secure as Bitcoin payments. And a big piece of the financial services industry would disappear.



[11] For example, the Gemological Institute of America.



6

SCALE AND SCALABILITY

Within most transaction networks, the larger a common blockchain, the lower the transaction costs but the less trusted the parties at its periphery. These and other scale economics are constrained by a more narrowly technical set of issues: the blockchain's scalability.

Scale economics involve more than just balancing size and trust. There are four other mechanisms:

- The larger the number of nodes and the greater the height of the blockchain, the more secure are the recorded transactions. This gives established blockchains (notably those for Bitcoin and Ethereum) an advantage over smaller and newer alternatives—not just in payments but in any application that can be built on these blockchains.

- The larger the dollar volume of digital coins in circulation, the more liquid the currency and, probably, the more stable its exchange rate. This again favors established coins (such as bitcoin and ether) over startups. But more important, if a digital coin were to reach critical mass, it would become acceptable as a medium of exchange and a store of value in the economy at large, and a big piece of its associated transaction costs—the cost of trading into and then out of the coin—would disappear.

- A single compelling killer app can pull through an entire ecosystem of associated innovations and create a network effect at both the top and bottom of the stack. However, one of the striking features of the blockchain landscape is that no killer app has yet emerged. Bitcoin, the currency, appears to be entering the flatter part of its S-curve (daily transaction volume has grown by only a third in the past 12 months), and The DAO, which many thought was the killer app for Ethereum, has collapsed.

- The larger the blockchain and the more heterogeneous its participants, the more politically complex is the challenge of setting strategy. In permissioned chains, consortium management among members that otherwise compete with one another becomes critical. (Banks, in particular, have a checkered history of managing industry collaborations.) In permissionless chains, the challenge is to formulate and execute a technology roadmap in the face of the conflicting priorities of open-source coders, miners, and commercial developers. With digital currencies, conflicts escalate as the dollar value of the coins owned by some of these parties steadily grows. And open entry implies open exit: absent proprietary intellectual property, dissatisfied coders—convinced that they know better—can fork the code and steal the growth as well as the limelight.

> “
>
> **IF BLOCKCHAINS HAVE A SERIOUS FUTURE, THEY MUST OVERCOME CURRENT SCALABILITY ROADBLOCKS.**

Besides issues of business scale, there are huge challenges in technical scalability.

Currently, Bitcoin can handle 3 to 5 transactions per second and Ethereum 15 to 25. But the interbank Visa system handles 2,500. So if blockchains have a serious future, they must overcome current scalability roadblocks. Bitcoin’s capacity limit is dictated by the fixed rate at which blocks are created and the maximum block size. Faster block creation, it is feared, would destabilize validation, since a rogue chain could propagate faster than the consensus mechanism chasing it across the network could disown it. And larger block size would intensify economies of scale in mining, driving consolidation and making the validation system more vulnerable to collusion. (Already, 58% of the hashpower is held by four Chinese mining pools.[12])

Moreover, the deliberate inefficiencies of Bitcoin and Ethereum will eventually impose practical limits. Nodes can create a block only by solving a very arduous and arbitrary computation called proof-of-work (for each block, 10,000 terahashes). This inefficiency secures the network by massively escalating the cost of rewriting the blockchain. But bitcoin mining already consumes as much electricity as a US city of 280,000, and by one estimate, as much as Denmark will consume by 2020.[13] The cost and carbon dioxide burden will become economically and environmentally unsustainable as volumes grow by orders of magnitude.

The broad components of a scalability solution are widely recognized but have not as yet been implemented:

PROOF-OF-STAKE

Under this protocol, a string of blocks is deemed valid only if the nodes creating it demonstrate sufficient ownership of the asset represented by the token to give them a compelling motive not to subvert its value. Proof-of-stake would radically reduce computing and transaction costs, enabling blockchains to facilitate much smaller transactions.

CHANNELS

Channels are another layer in the stack. A subgroup of parties transacts directly but commits only a small fraction of transaction data to the main blockchain. Channels can thus proliferate without burdening the main blockchain and while still enjoying some of its security. There are many variants on this idea, such as the proposed Lightning Network for Bitcoin.

SIDECHAINS

Closely related to channels, sidechains are blockchains in their own right. They create and destroy their internal token as a mirror of a transaction that immobilizes an equivalent on the main chain. This effectively allows users to move tokens from the main chain to sidechains and back again. The sidechain can operate on any principle whatsoever: lower security for minuscule transactions, fast block creation, smart contracts. It can even be a closed, permissioned chain.

SHARDING

This is an approach that preserves a single global blockchain, but not all nodes validate all transactions. It sacrifices a measure of security for the benefits of scalability.

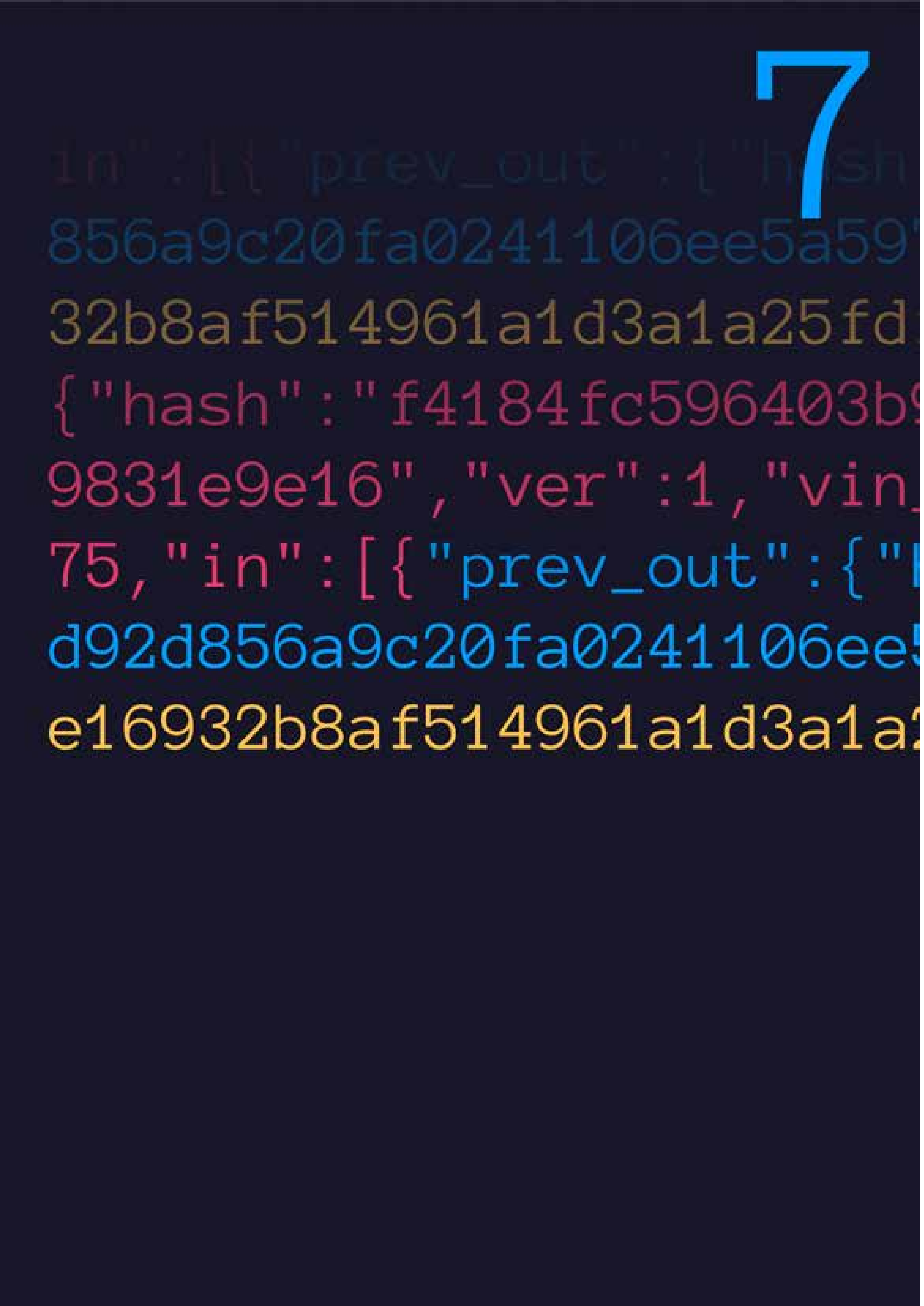
These developments are at the cutting edge of blockchain research and experimentation. The Bitcoin Core leadership is moving cautiously in these directions, as befits a blockchain advantaged for its security. The Ethereum developer community is moving much faster: the 2017 Release 2.0, code-named Serenity, will be explicitly built on all four design principles.

But startups with no legacy to protect are trying to beat established blockchains to the punch with the right combination of these principles. They may build on existing Bitcoin or Ethereum code and currency, or they could start afresh. The pieces are largely known, but the world is still waiting for the killer combination, the killer app.

a0626f1baded5c72a704f7e6cd84cOTP
d71302fa28414e7aab37397f554a7df5f
62fe09
{1a25fdf3f4f7732e9d624c6c61548ab5

[12] See the website Blockchain Info at https://blockchain.info/pools

[13] “Bitcoin Could Consume as Much Electricity as Denmark by 2020,” *Motherboard*, March 29, 2016.



7

FIVE STRATEGY PRINCIPLES

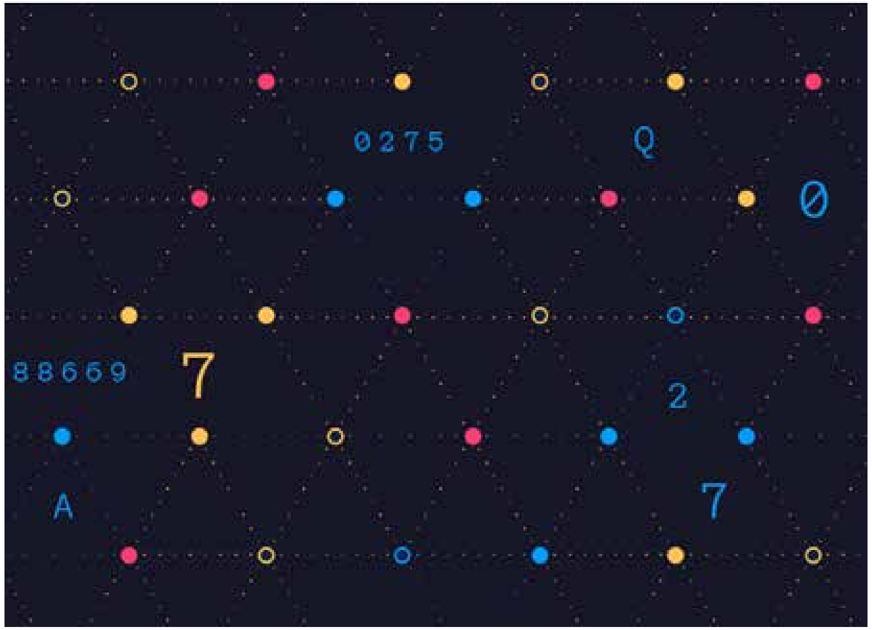
There are five broad principles that will shape strategy for token and blockchain technologies.

1. BLOCKCHAIN STRATEGY IS MORE ABOUT COLLABORATING THAN COMPETING.
It makes sense to expend resources on digital tokens and blockchains only when multiple entities are transacting at high cost and with imperfect trust. Therefore, the implementation opportunity presents itself to the entire transaction network, not to an individual participant. Global enterprise technology companies are investing to build alliances among their customers that could underpin transaction platforms in fragmented industries such as health care and international

trade. Hundreds of Silicon Valley startups are focused on the same goal, or at least on advancing far enough to get themselves acquired. These will be decade-long projects. Participants in those fragmented industries need to decide whether the gains in growth and efficiency are worth the risk of being at least partially commoditized by a new, dominant transaction platform—and, if not, whether they can act in concert (as banks are attempting to do) in order to protect their autonomy.

2. ORGANIZATION AS MUCH AS TECHNOLOGY WILL DETERMINE THE RELATIVE ADVANTAGE OF BLOCKCHAINS

A central conflict over the next few years will be between permissioned blockchains curated by coalitions of intermediaries and the far more radical program to give end users direct access through open protocols. Oligopoly versus democracy, as some would have it. In many intermediary industries such as financial services, incumbents are rationally responding by adopting the technology among themselves. But it is a big and open question whether that will ultimately suffice. Open blockchains enjoy an advantage in scale: they have more blocks, more nodes, and more rigorous validation. By design, they can add participants less constrained by diminishing peripheral trust. But permissioned blockchains have an advantage in scalability relative to their target transaction network. They need fewer participants and can dispense with nonscalable features such as proof-of-work. So whether and when the status quo is disrupted—and by how much—depends less on the absolute pace of technical advance than on the relative pace at which private and public implementations advance. And that is largely a contest of political organization. Industry consortia need to work together when their members are otherwise competing. And open communities need to stick to a single script when individuals have diverse ideological commitments and are tempted to fork the codebase. The strategist needs to understand both, intimately, and be clear-headed about which camp holds the winning hand.



3. GOVERNMENT IS A WILD CARD.

The current regulatory climate is surprisingly favorable. Bitcoin is legal in most jurisdictions, regulated as a commodity but not as a financial instrument. The primary focus of regulation is the top of the stack (exchanges, in particular) rather than the bottom (blockchains). Indeed, blockchains facilitate regulatory goals: they reduce counterparty risk, can comply with know-your-customer and anti-money-laundering rules, and can provide an efficient “backdoor” access to transactions. But of course the regulatory climate could change quite suddenly, especially in the face of security vulnerabilities. On top of that, governments themselves could drive transformative blockchain applications in identity, health care, and digital currency. They have the incentive and the critical mass. Many policymakers see this kind of technology as the catalyst for broader economic stimulus, job creation, and national competitive advantage. Some countries are more likely to think that way than others.

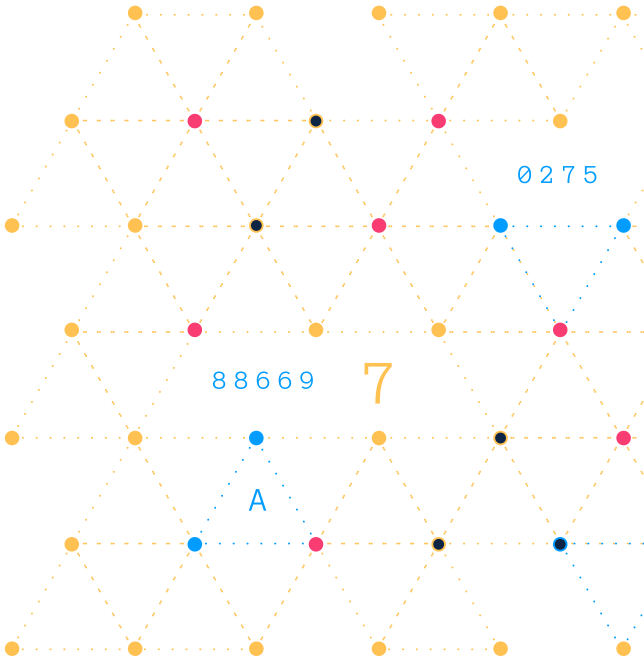
4. FINANCIAL SIGNALS ARE PROBLEMATIC.
There are already murmurs in some boardrooms that the ROI on these technologies is not that impressive. Highfalutin rhetoric about embracing digital disruption notwithstanding, incumbents have little incentive to collaborate and invest to create a level playing field that merely lowers industry prices. Executives have to believe either that such innovation will open new markets or that it is a necessary response to a real disruptive threat. Otherwise, it is easy to imagine the majority quietly shelving the technology and the grand industry coalitions falling apart. A few “visionary” CEOs will ignore their bean counters. If the disrupters later succeed, those visionaries will become the heroes of business school case studies—and if not, the fools.

5. RADICAL UNCERTAINTY IS THE NORM.
It only takes one really compelling and broad-based application, one killer app, to drive widespread adoption and pull through complementary infrastructure, products, and services. All we know is that it’s not bitcoin, the currency.

Conversely, some hacker could find an irreparable security flaw: not enough to deter enthusiasts, perhaps, but sufficient to spook the regulators. Or scalability could prove an insuperable problem.

Or a middle scenario: a few disparate applications might enjoy modest success without converging into a tidal wave comparable to the PC or the internet. Transformational ideas could die on the vine for lack of self-fulfilling momentum. Silicon Valley could have another bust or just move on to the next new thing.

The truth is that nobody knows.



8

```
{"hash":"f4184fc596403b9d638783cf57adfe4c75c605f6356fbc913385
1,"vin_sz":1,"vout_sz":2,"lock_time":0,"size":275,"in":[{"pre
cd7f8525ceed2324359c2d0ba26006d92d856a9c20fa0241106ee5a597c9"
"304402204e45e16932b8af514961a1d3a1a25fdf3f4f7732e9d624c6c615
22ec8eca07de4860a4acdd12909d831cc56cbbac4622082221a8768d1d090
```

THREE MANAGEMENT PRINCIPLES

As with any early-stage technology subject to network effects and strongly increasing returns, the business equilibrium is radically unstable. Strategy cannot be based on a "point estimate" of what the future will look like, whether derived from financial projections or a grand vision. Instead, strategy under conditions of uncertainty must focus on acuity, options, and experimentation.

1. ACUITY.
Your organization needs to know its environment intimately: the technology, competitive moves, alliance politics, crazy startups, and shifts in public policy. Look out for discontinuities. Some open blockchain protocol could eclipse the

closed efforts of an industry consortium; some government-sponsored initiative on the other side of the world could catalyze a killer app. Some breakthrough in encryption—or decryption—could transform security or scalability. Some development in another industry could wash over yours, the way whole industries became mere apps on the PC or the internet. Acuity cannot be delegated, because the correct framing of the threats and priorities is not yet apparent. Senior managers need to be part of a process of continuous learning.

2. OPTIONS.

In strategy as in finance, the greater the uncertainty the greater the value of having options. Options are an investment whether they pan out or not; it is false economy to skimp or delay until the outcome is evident. So at the risk of redundancy, and even of supporting contradictory or competitive initiatives, invest broadly. Buy into a portfolio of alternative technologies. Join industry alliances and consortia: membership will give your organization early participation in whatever succeeds, the chance to learn, and an opportunity to shape the group's priorities from the earliest stages.

3. EXPERIMENTATION.

Apply "agile" principles to the development of small-scale token and blockchain applications. Experiments matter because they can point to a "strategy" and also because the very practice builds operational capability and confidence. MIT's David Clark famously articulated the mantra of the early internet community as "rough consensus and running code.[14]

So stay close to the coders, the entrepreneurs, and the policymakers. Keep your options open. Experiment. These are the watchwords for thinking outside the blocks. And they are better guides to strategy than the airy enthusiasm of evangelists or the myopia of bean counters.

[14] D.D. Clark, "A Cloudy Crystal Ball: Visions of the Future," plenary presentation, 24th meeting of the Internet Engineering Task Force, Cambridge, MA, July 1992.

RELATED ARTICLES

HOW BITCOIN WORKS

The phenomenon we know as Bitcoin depends on two complementary technologies—digital tokens and blockchain—that together facilitate digital identity, ownership, transactions, contracts, and trust.

Bitcoin and blockchain are based on two cryptographic techniques—hashes and public/private-key encryption—that today invisibly secure the transmission of personal information and purchases online:

- A hash is a mathematical function that converts a string of arbitrary length into a string of fixed length. It is one-way: easy to compute but impossible to reverse. It serves as an efficient way to summarize a document. And it is hypersensitive: the slightest change to the document changes its hash totally.

- In public/private-key encryption, a string is encrypted with one number, but the result can be decrypted only by using its pair. One number (the "public key") is published in some universal and reliable manner, and the other is kept private. A party can securely send a message by encrypting with the intended recipient's public key, which only the latter can decrypt. Or a party can digitally "sign" a document by encrypting it (or more likely, its hash) with his or her private key. Anybody can then use the sender's public key to decrypt the document, thereby confirming that only the owner of the associated private key could have sent it.

As described in the companion article "Thinking Outside the Blocks," a bitcoin is simply a sequence of digital signatures, each certifying transfer from one pseudonymous holder to the next. ("Pseudonymous" because bitcoin owners are identified by their public keys.) Each payer signs with his or her private key a record of transfer to the recipient's public key. Included in the transaction record is a hashed summary of the previous transaction. So anybody can check that the record of one transaction was indeed correctly hashed into the next and thus trace an unbroken series of valid transfers back to the creation of the coin. The content of a bitcoin guarantees its "ancestry."

Proven ancestry does not prevent a valid bitcoin from being spent more than once. So the proposed transaction is distributed over the internet to an open network of "nodes" that compete to assemble valid transactions into a "block." Software run on a node checks the history of the bitcoin to make sure it has not already been spent by the payer. A new block, typically containing about 200 transactions, is created every ten minutes. The next block contains the hash of its predecessor, so the blocks form a continuous "blockchain." The blockchain thus guarantees "inheritance."

Very quickly a block becomes immutable, since the hashes in all subsequent blocks depend on it. Rewriting a transaction would require recomputing all subsequent blocks, and doing so faster than the rest of the network can add new blocks.

The owners of these node machines, called bitcoin "miners," are motivated to perform the service of validating transactions through a "contest" to create the next block. The winner receives 12.5 newly minted bitcoins. Because some 5,700 nodes are working in parallel, discrepancies may arise from fraud or slow synchronization. But nodes follow a simple rule: always prefer the longest blockchain. This is the so-called consensus mechanism. Nodes do not need to be trusted to do this. Following the consensus is rational because each node knows—and knows that all other nodes know—that the reward will be automatically cancelled if a string of blocks becomes orphaned. No external institution, legal obligation, or altruistic motivation is required; the software defines a positive-sum game.

The contest involves solving, by trial and error, a hashing problem. This requires on average 10,000 terahashes per block. The inefficiency is the point: this so-called proof-of-work raises the cost of corrupting the system. To rewrite a block or conduct a denial-of-service attack, an antagonist would have to overwhelm the immense computational power of 51% of the network. It is a better business proposition to mine bitcoin by validating transactions.

SEVEN POSSIBLE KILLER APPS FOR BLOCKCHAIN AND DIGITAL TOKENS

Beyond payments, there are many applications that could benefit from decreased transaction costs, a neutral shared database, and the superior security of a shared ledger.

The disruptive potential of tokens and blockchains initially surfaced with payments thanks to the controversy over and curiosity about their application in Bitcoin. But these two technologies could have much broader application. As explained in the companion article "Thinking Outside the Blocks," blockchains and digital tokens establish digital continuity. The technologies can undergird any number of applications that bring together many different parties that often have no reason to trust one another. They can eliminate duplicative and error-prone transactions, and they can help create digital identity.

Assuming (and it is a big assumption) that the tradeoffs among security, functionality, and scale will be largely resolved within five years, a range of radically new blockchain applications are possible. Here are seven potential killer apps.

1. TRANSACTING ON THE INTERNET OF THINGS.

Most current IoT applications connect devices with a common owner, so they only need to exchange information or instructions. When devices have different owners, however, they must transact. Today, when device owners lack a shared intermediary and the sums involved are minuscule, transacting is not economically worthwhile. But with a blockchain, especially one that enables smart contracts, transactions between devices become possible on a direct, peer-to-peer basis. A car can purchase parking simply by driving onto a space: a transponder in the car connects to a $25 meshed device embedded in the asphalt. (Streetline is already deploying such transponders.) The German company Slock.it has developed a cheap Ethereum computer prototype that mediates between smart devices in the home and the Ethereum blockchain. In one application, the computer negotiates a room rental as a smart contract and instructs the smart lock on the front door to open when the renter arrives. The blockchain holds the deposit in escrow and releases funds on fulfillment of the contract. This disintermediates not only PayPal and the banking system but also Airbnb.

2. TRANSFORMING THE ECONOMICS OF DIGITAL CONTENT.

Today, internet content is funded by either subscription or advertising. But with cheap, blockchain-based transactions, it would be possible to meter media consumption by the page or the minute. Especially if consumers' privacy concerns intensify, blockchain could drive a fundamental shift in the revenue models of the online media industry. An extension of this idea is using a blockchain to register and protect intellectual property. In October 2015, Imogen Heap, the British singer and songwriter, released her song "Tiny Human" on the Ethereum blockchain as a smart contract. It allowed fans to download, stream, remix, and sync the song, distributing royalties directly to the creators—and entirely bypassing the complex and costly web of music intermediaries.

3. MAKING SUPPLY CHAINS CHEAP AND TRANSPARENT.

The $40 trillion global supply chain is another inefficient transaction network characterized by slow and error-prone transactions among parties with imperfect mutual trust. Some banks are already registering letters of credit on a blockchain so that importers, exporters, and their respective financiers can share common data and release funds without delay or error. By extension, the item itself—like a bitcoin—can carry a continuous identifier that accesses digitally signed data entered on a blockchain by freight forwarders, customs authorities, shippers, wholesalers, retailers, and trusted independent certifiers. This can replace the bill of lading, but it can also certify that a good was handmade in Firenze, manufactured by a Fair Trade Federation member, or is free of genetically modified organisms. Provenance.org, similar to Everledger, provides an Ethereum-based platform that allows companies to register claims about themselves, their products, and even specific production batches. Paperwork is eliminated and the locus of trust shifted from intermediaries to the originator of the claim.

4. REFORMING LAND REGISTRIES.

In mature economies such as the US, land registries are riddled with incomplete paperwork requiring manual inspection and expensive title insurance to protect against residual errors. In many emerging economies, registries are radically incomplete or corrupted, depriving poorer citizens of basic property rights. In Honduras, where some 60% of land has no registration, bureaucrats have been known to reassign property to themselves. A land registry lodged on a blockchain would be public and incorruptible. Honduras and the Republic of Georgia have launched such initiatives, but with mixed results so far. The long-term potential, however, is immense:

Peruvian economist Hernando de Soto has powerfully argued that establishing clear title to land would give poor people access to credit and the motive to invest.[1]

5. GUARANTEEING DIGITAL IDENTITIES.

Governments (or some broad coalition of service providers) can play a crucial role by giving their citizens digital identities, thereby enhancing peripheral trust in all peer-to-peer transactions. A digital identity would be data with provable ancestry from the authority, universally verifiable, just like a bitcoin. It is not obvious that such data would need to be stored on a blockchain. Citizens could create public/private-key combinations to release selected personal data to specific recipients. Thus, a young person could prove that he or she is old enough to purchase liquor without revealing other, irrelevant information, as with a driver's license. Over time, legally binding digital signatures, passports, licenses, security passes, key cards, certificates, log-ins, ownership documentation, voter registration, and a panoply of other legal information could be built on that foundation. The most ambitious step in this direction is the AADHAAR national-identity scheme, which has enrolled over a billion citizens in India. Visionaries see an entire "India stack" built on this foundation, possibly extending into payments for the unbanked.

6. STREAMLINING HEALTH CARE AND REVOLUTIONIZING RESEARCH.

Health care is characterized by duplicative, incompatible, and inconsistent medical records, while patient data is subject to stringent security and privacy requirements—a perfect application for a permissioned blockchain. But visionaries are looking beyond simple data sharing to "precision medicine": a continuously learning health care system built on electronic health records, data analytics, and universal disease registries. These new systems will record patient data (and ultimately, complete genomic maps), symptoms, treatments, and above all, outcomes. The central challenge in designing such systems is to reconcile patients' privacy with researchers' need for granular and universal data sets. Mere anonymization does not work.[2] Blockchains can be designed in which an individual's record is scrambled and distributed over multiple nodes, and database queries are distributed across the ledger. Access would be controlled through smart contracts and digital identities. But in the US, because of institutional fragmentation, even such a relatively straightforward innovation as electronic medical records has proved extraordinarily difficult to implement. Scandinavia, not the US, will be the pioneer in these approaches.

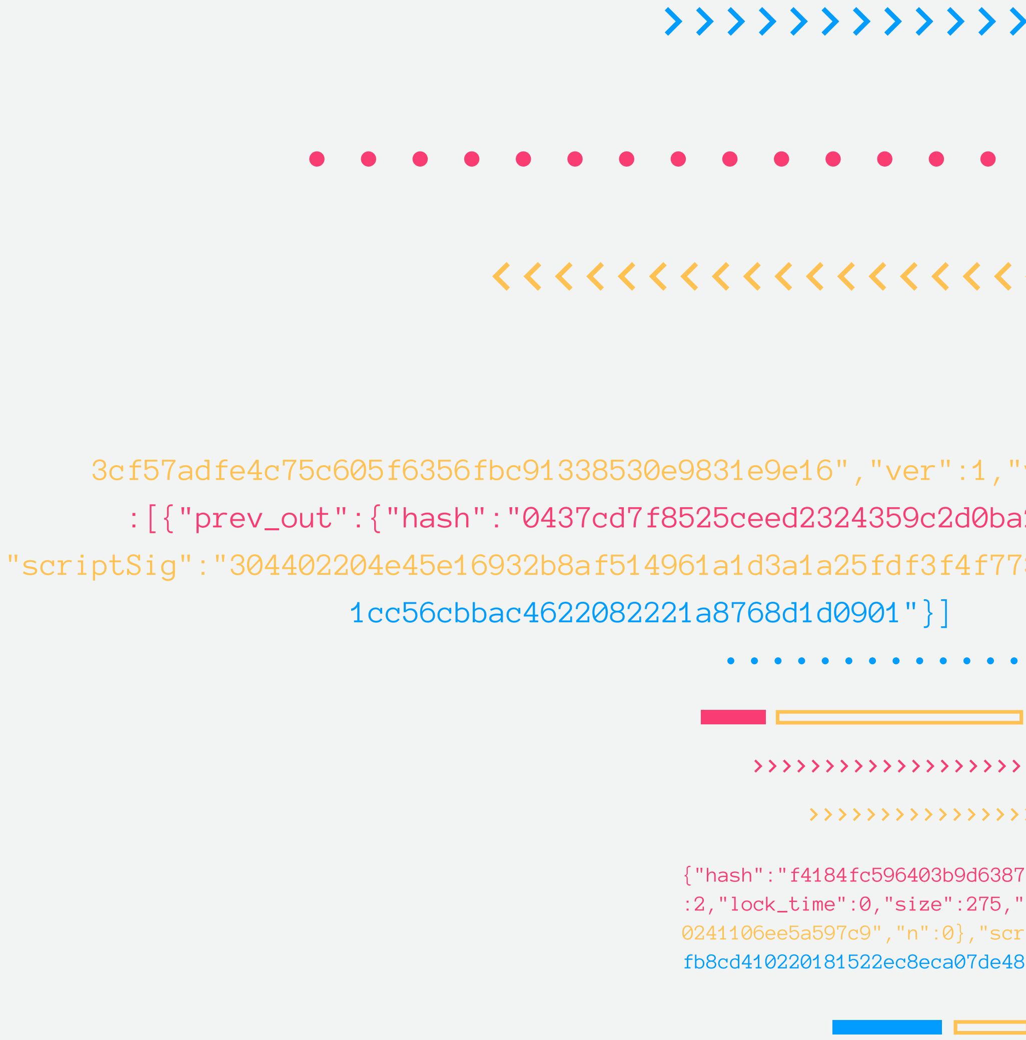
7. MINTING DIGITAL FIAT CURRENCY.

At least a half-dozen central banks are considering this step. The Bank of England, say, would mint "bit£" as digital bearer instruments. Unlike bitcoin, bit£ would have a fixed value and be backed by the full faith and credit of the government. The central bank would purchase government securities with bit£ through an interbank-permissioned blockchain. Commercial banks would then use the bit£ on their balance sheets to settle interbank obligations, massively reducing the counterparty risks that brought the financial system to the brink of collapse in 2008. Over time, access to bit£ could be extended, ultimately to all citizens. Bit£ would then displace physical cash and much of the traditional payments settlement function of commercial banks. Bitcoin itself would be disrupted by bit£, a universally acceptable, zero-risk competitor. Regulatory and compliance costs would be substantially reduced across the financial system. A recent Bank of England study even concluded that macroeconomic policy would be easier to administer (bit£ could pay a negative interest rate, for example) and that such a regime could permanently raise GDP by as much as 3% by lowering real interest rates, distortionary taxes, and transaction costs.[3]

[1] Hernando De Soto, *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else*, Basic Books, 2000.

[2] Justin Brickell and Vitaly Shmatikov demonstrated a severe tradeoff between the degree of anonymity and the utility of the resulting information. See "The Cost of Privacy: Destruction of Data-Mining Utility in Anonymized Data Publishing," *Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, August 2008.

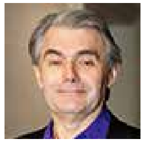
[3] John Barrdear and Michael Kumhof, "The Macroeconomics of Central Bank Issued Digital Currencies," Bank of England Staff Working Paper No. 605, July 2016.


3cf57adfe4c75c605f6356fbc91338530e9831e9e16","ver":1,"
:[{"prev_out":{"hash":"0437cd7f8525ceed2324359c2d0ba
"scriptSig":"304402204e45e16932b8af514961a1d3a1a25fdf3f4f77
1cc56cbbac4622082221a8768d1d0901"}]
{"hash":"f4184fc596403b9d6387
:2,"lock_time":0,"size":275,"
0241106ee5a597c9","n":0},"scr
fb8cd410220181522ec8eca07de48

n_sz":1,"vout_sz"
5006d92d856a9c20fa
2e9d624c6c61548ab5

cf57adfe4c75c605f6356fbc91338530e9831e9e16","ver":1,"vin_sz":1
":[{"prev_out":{"hash":"0437cd7f8525ceed2324359c2d0ba26006d9
tSig":"304402204e45e16932b8af514961a1d3a1a25fdf3f4f7732e9d624c6
a4acdd12909d831cc56cbbac4622082221a8768d1d0901"}]

ABOUT THE AUTHORS



PHILIP EVANS is a BCG Fellow and a senior advisor in the Boston office of The Boston Consulting Group. You may contact him by e-mail at evans.philip@bcg.com.

LIONEL ARÉ is a senior partner and managing director in the firm's Paris office and the global leader of the Financial Institutions practice. You may contact him by e-mail at are.lionel@bcg.com.

PATRICK FORTH is a senior partner and managing director in BCG's Sydney office and the global leader of the Technology, Media & Telecommunications practice. You may contact him by e-mail at forth.patrick@bcg.com.

NICOLAS HARLÉ is a senior partner and managing director in the firm's Paris office and the global topic leader for blockchain. You may contact him by e-mail at harle.nicolas@bcg.com.

MASSIMO PORTINCASO is a partner and managing director in BCG's Berlin office and the firm's global marketing director. You may contact him by e-mail at portincaso.massimo@bcg.com.

For information or permission to reprint, please contact BCG at:

E-mail: bcg-info@bcg.com

Fax: +1 617 850 3901, attention BCG/Permissions

Mail: BCG/Permissions
The Boston Consulting Group, Inc.
One Beacon Street
Boston, MA 02108
USA

To find the latest BCG content and register to receive e-alerts on this topic or others, please visit **bcgperspectives.com**.

Follow **bcg.perspectives** on Facebook and Twitter.

```
6356fbc91{
r
0437cd7f8525ceed2324359c2de
df3f4f773
{"hash":"f4184fc596403b9d638783cf57adf
```