

# SLOCK.IT

## Enabling IoT and the Universal Sharing Network

Alan Majer  
Good Robot

December 2017





## Realizing the new promise of the digital economy

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

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

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



**Blockchain Research Institute, 2018**

Except where otherwise noted, this work is copyrighted 2018 by the Blockchain Research Institute and licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License. To view a copy of this license, send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA, or visit [creativecommons.org/licenses/by-nc-nd/4.0/legalcode](http://creativecommons.org/licenses/by-nc-nd/4.0/legalcode).

This document represents the views of its author(s), not necessarily those of Blockchain Research Institute or the Tapscott Group. This material is for informational purposes only; it is neither investment advice nor managerial consulting. Use of this material does not create or constitute any kind of business relationship with the Blockchain Research Institute or the Tapscott Group, and neither the Blockchain Research Institute nor the Tapscott Group is liable for the actions of persons or organizations relying on this material.

Users of this material may copy and distribute it as is under the terms of this Creative Commons license and cite it in their work. This document may contain material (photographs, figures, and tables) used with a third party’s permission or under a different Creative Commons license; and users should cite those elements separately. Otherwise, we suggest the following citation:

Alan Majer, “Slock.it: Enabling IoT and the Universal Sharing Network,” foreword by Don Tapscott, Blockchain Research Institute, 21 Dec. 2017.

To request permission for remixing, transforming, building upon the material, or distributing any derivative of this material for any purpose, please contact the Blockchain Research Institute, [www.blockchainresearchinstitute.org/contact-us](http://www.blockchainresearchinstitute.org/contact-us), and put “Permission request” in subject line. Thank you for your interest!



## Contents

<b>Foreword</b>	<b>3</b>
<b>Case in brief</b>	<b>4</b>
<b>The problem to be solved</b>	<b>4</b>
<b>Slock.it's solution</b>	<b>5</b>
DAO: The hope, the hack, and the hard fork	6
Culture reboot: Grounded in practical applications	7
Radical transparency: The universal sharing network	10
<b>Key takeaways</b>	<b>11</b>
<b>About the author</b>	<b>13</b>
<b>About the Blockchain Research Institute</b>	<b>14</b>
<b>Notes</b>	<b>15</b>





## Foreword

The subtitle (and key theme) of *Wikinomics* was “how mass collaboration changes everything.” The sharing economy proved to be a promising early example of how this theme could manifest. The trouble was, the movement’s leading stars such as Uber and Airbnb never represented true sharing. They became central authorities who control the ecosystem and collect rent for connecting borrowers and loaners or renters and owners.

This project investigates how the start-up Slock.it is deploying blockchain technology to enable a true “universal sharing network.” This network will enable people to rent their idle assets in a manner so non-intrusive and seamless that even microtransactions such as using someone’s bicycle to ride to the store are viable. This case study describes how the company’s inspiration came from an attempted high-tech heist and outlines the conditions necessary for such a network to succeed.

*The sharing economy’s leading stars such as Airbnb never enabled true sharing. They represent centralized intermediaries who control the ecosystem and collect fees for connecting renters and owners.*

I have collaborated with Alan Majer for almost twenty years on multiple research projects similar to the Blockchain Research Institute. I believe that, out of the top twenty most innovative projects we have completed during that time, Alan authored at least five. His work is most prescient when he investigates technology at its cutting edge, especially when it incorporates robotics or the “maker” community. Alan is not only an accomplished researcher and writer but also a practitioner. His dual expertise readily benefits the readers of this project.



DON TAPSCOTT

*Co-Founder and Executive Chairman  
Blockchain Research Institute*



*Slock.it is creating a universal sharing network, that is, a blockchain-enabled platform for true sharing that will integrate with devices and real-world assets.*

## Case in brief

- » The history of Slock.it reads like a fast-paced science fiction novel: a brainy group of technologists breathe life into an autonomous system, frenzied cryptocurrency speculators try to cash in on this invention, and then an anonymous hacker puts in place a devious trap that seized over \$50 million in one of the largest attempted heists in corporate history.
- » These dramatic events have at times thrust Slock.it into an unwanted storm of controversy and media attention, but they have also positively influenced Slock.it's founders and their business approach. The company has emerged with a practical focus on building its business the old-fashioned way: becoming cash flow positive, acquiring customers and partners, and turning prototypes into products and profits.
- » Slock.it's goal is straightforward: to create a blockchain-enabled platform for the sharing economy, a *universal sharing network* (USN). This USN will enable true peer-to-peer (P2P) sharing and exchange via the blockchain and will integrate with real-world assets and devices.
- » Users of the USN can share objects—bikes, washing machines, or apartments—directly with one another with the aid of smart contracts, a unique combination of cryptocurrency, distributed applications (Dapps), and the Internet of Things (IoT) that brings cryptocurrency transactions into the real world.<sup>1</sup>
- » While a bold vision of peer-based IoT sharing is at the heart of the company, it differentiates between the speculative hype surrounding blockchain and the practical challenges of building and implementing a blockchain business.

## The problem to be solved

Around the world, companies such as Airbnb, Uber, GetAround, and Fon have created platforms for putting unused assets to work. Owners of cars, apartments, and even Wi-Fi hotspots can grant others access to these assets through such platforms. Some call it the "sharing economy," but it is really another form of matchmaking where a middleman aggregates all the offers to share something,



*Technology platforms tend to compete in markets with strong network effects—that is, the more people or machines that use a platform, the more valuable and more dominant it becomes.*

takes fees for making matches, and captures everyone's data in the process, potentially monetizing its proprietary view of a particular market.

Large participants in the sharing economy aren't automatically generous. The challenge of these so-called sharing businesses is that they tend to operate in domains that have strong *network effects*—that is, as the network grows, it becomes more valuable. In business terms, it creates a winner-take-all environment where the dominant firms wield increasing influence. The same network effects that cause these firms to struggle in the beginning as they fight for critical mass (often enticing users with special benefits or cut-rate commissions), later cause them to do the opposite (sometimes raising rates and extracting higher commissions) once they've attained market dominance. Uber, for example, has pressured drivers by continuing to reduce the price per mile paid to them, while raising its own commission rates at the same time.<sup>2</sup>

Physical technologies such as the IoT can help automation systems to improve efficiency and potentially alter that middleman role. Those overseeing a matchmaking system should consider all the elements of cost and friction in the system. That means streamlined payments, verifying identities, or providing physical access to an asset: any activity or process that contributes to making the system easier to use is a candidate for automation. So, embedding the sharing process itself into physical assets like cars, houses, and more, is a potentially potent source of innovation and efficiency.

Using blockchain technologies, Slock.it can address both issues: supporting more P2P exchanges that depend less on a middleman and creating IoT technologies that automate a system via autonomous objects (like locks) connected to the blockchain.

## Slock.it's solution

*Slock.it can support not only peer-to-peer exchanges but also peer-to-thing and machine-to-machine transactions via autonomous objects connected to the blockchain.*

One of the unusual properties of a currency like bitcoin is that it enables software, not just people, to own money. Following bitcoin's invention, discussion began to circulate about this strange new possibility. In 2011, Gregory Maxwell speculated how a Dropbox-like system might be able to buy storage from the cloud and resell it at a profit.<sup>3</sup> It was a curious concept, "and it fascinated me," said Stephan Tual, who would later co-found Slock.it.<sup>4</sup> Mike Hearn, another prominent blockchain technologist, discussed a variation of this idea, that machines in the real world might use blockchain currency to support their autonomous livelihood. Imagine a self-driving car that could earn money with fares.<sup>5</sup> While interesting, these ideas seemed largely theoretical. Moreover, the Bitcoin blockchain was promising for payments but difficult for building smart contracts: simply put, the money on Bitcoin was not "programmable," limiting its usefulness for an autonomous system. In 2013, the situation started to change when Stephan received an e-mail from Vitalik Buterin, who had done





his own thinking about the potential of autonomous systems. Vitalik wondered:

*What if, with the power of modern information technology we ... create an inviolable contract that generates revenue, pays people to perform some function, and finds hardware for itself to run on, all without any need for top-down human direction?*<sup>6</sup>

*A universal sharing network is an open blockchain system where users can publicly deploy sharing applications for others to use. It is not a centralized intermediate platform but a distributed system that enables true peer-to-peer sharing.*

By the end of 2013, Vitalik had laid out a vision for Ethereum, a new blockchain that could support smart contracts.<sup>7</sup> That convinced Stephan to do everything he could to join Ethereum, where he was exposed to research that indicated an interest and potential in the mixture of IoT and blockchain technologies.<sup>8</sup> Convinced that this was the future, Stephan left Ethereum in 2015 to pursue his entrepreneurial ideas.

Then Christoph Jentzsch reached out to him: “Hey, come over to Berlin. I’ve got something to show you that you’re going to love,” Stephan recalled.<sup>9</sup> Christoph had built a working prototype of a physical lock linked to the blockchain—send it money and it opens. “Holy crap, that’s it, you’ve built it!” Stephan told Christoph, and Slock.it was born, with Stephan as chief operating officer.<sup>10</sup>

Christoph, Slock.it’s CEO, described the company’s vision as “connecting all kind of smart locks to the blockchain, enabling them to receive payments directly and be used to rent, sell, or share just about anything. We call this the ‘universal sharing network.’”<sup>11</sup>

In these earliest days, the company took what would turn out to be a dramatic detour. Like many crypto- or blockchain-related businesses, Slock.it’s founders weighed the idea of an *initial coin offering* or ICO, to the point that they began coding some enabling smart contracts. The initial idea was to issue tokens with built-in voting rights so that token holders could guide how Slock.it spent money.<sup>12</sup>

The founders wondered whether they could take these ideas further. Christoph explained: “After further consideration, we gave token holders even more power, by giving them full control over the funds, which would be released only after a successful vote on detailed proposals backed by smart contracts.”<sup>13</sup>

## DAO: The hope, the hack, and the hard fork

Could they go still further and create a radically decentralized and fully autonomous organization? Christoph believed so and detailed how they could achieve it in a provocative white paper, “Decentralized Autonomous Organization to Automate Governance.”<sup>14</sup> The company took a daring decision that would hurl the blockchain itself into uncharted territory, and it began coding the framework for an autonomous organization that could solicit proposals and distribute funds to any entity, Slock.it or otherwise. Formally, the *decentralized autonomous organization* (or DAO as it came to be known) would



be out of Slock.it's hands, too. Stephan said, "We did not run the DAO, we did not launch the DAO," and that autonomy was what people loved about the DAO.<sup>15</sup> "A 'Slock.it dao' would actually be the antithesis of what a true DAO stands for—autonomy—and would have actually counterintuitively hindered its success rather than help[ed]," suggested Stephan—it was a distinction that would be pivotal.<sup>16</sup>

Operations went exceedingly well—at first. In May of 2016, the DAO raised a record-breaking 12 million ether, worth more than \$150 million at the time (and \$4.53 billion today).<sup>17</sup> It was the largest crowdfunding event in history.<sup>18</sup> This unexpected growth was a mixed blessing for the innovative new entity. Christoph admitted, "The time for a project of its magnitude turned out to be too early."<sup>19</sup> On June 6, *Wired* labeled the DAO "very much a work in progress," and a "risk on an enormous scale."<sup>20</sup>

Then, on June 17, the unthinkable happened: an attacker started draining millions from the DAO, eventually holding more than \$50 million in ether hostage.<sup>21</sup> The attack exploited a bug in the DAO's code—a recursive transaction call that allowed the attacker to dump a balance multiple times into an account before subtracting it—combined with a DAO feature involving splits.<sup>22</sup> It appears to have required advanced planning to lay the groundwork for the attack; the required split feature of the attack was realized when the attacker submitted proposal 59, titled "lonely, so lonely," on June 8—a full nine days before launching the main attack.<sup>23</sup>

The aftermath was more complicated than the attempted heist itself. First, a group of "Robin Hoods" used the same attack vector to attempt to drain and store the remaining DAO funds, a gallant effort that created legal complications for them. The magnitude of the attack itself was so great that the community decided to alter the previously inviolable blockchain with a something called a *hard fork*. The fork would keep the rest of the blockchain history intact but rewrite a single "tiny" historical fact: it would take back the attacker's funds and put them into a refund account, effectively making it look as if the attack never happened.<sup>24</sup> With the reversal of these funds, the bold experiment in autonomy ended.<sup>25</sup>

*The culture and attitudes of Slock.it owe a lot to its experience with the DAO. While Slock.it shares the typical start-up's excitement about blockchain's possibilities, an atypical air of temperance, even conservatism, pervades the company's current business approach.*

## Culture reboot: Grounded in practical applications

The culture and attitudes at Slock.it today owe a lot to its experience with the DAO. While Slock.it shares the typical start-up's excitement about new blockchain possibilities, an atypical air of temperance, even conservatism, pervades the company's current business approach. "One thing that differentiates Slock.it from all other companies is that we have a ten-year plan," and that allows Slock.it to take a step back, said Stephan Tual.

*We differentiate between the speculative aspect of this stuff where Ethereum is three times the entire market cap of Twitter, for example, but has zero users—which is also ridiculous—and the actual genuine benefits of this technology when it comes to integration with the IoT.*<sup>26</sup>





*"We differentiate between the speculative aspect of this stuff ... and the actual genuine benefits of this technology when it comes to integration with the IoT."*

 **STEPHAN TUAL**  
Co-founder and COO  
Slock.it

While Stephan enjoys the open-ended possibilities of P2P sharing and autonomous contracts, he's quick to point out that the future of truly autonomous machines is more of a lifelong pursuit than a short-term aspiration. It will take 20 years to build this economy, said Stephan. "People say, 'Oh, it's like the Internet in 1993.' Well, I don't think so. I think it's more like the Internet in 1968 when Douglas Englebart was presenting the mouse, collaborative editing, hypertext—all that stuff was right in his head."<sup>27</sup> The culture and focus of Slock.it today is grounded in building practical IoT and blockchain applications with clients. The company is focused on three areas:

- » Building blockchain applications in conjunction with its customers
- » Developing a universal sharing network
- » Enabling blockchain IoT via an "Ethereum computer"<sup>28</sup>

The Share&Charge service by MotionWerk is one of Slock.it's first customer deployments on the Ethereum blockchain.<sup>29</sup> Siemens AG is working with Slock.it to implement a blockchain-based DAO that allows for voting on projects with a social purpose. An initiative with a Fortune 500 electronics firm is also in the works.<sup>30</sup> The MotionWerk service is an ideal crossover between P2P blockchain transactions and IoT.

It's a perfect business case for P2P sharing. In Germany, there are just over 6,000 public charging stations for electric vehicles (EV), yet EV drivers themselves collectively own over 45,000 home charging stations; sharing just a small number of these chargers would more than double the publicly available infrastructure.<sup>31</sup>

That's where Slock.it comes in. In addition to MotionWerk's own stations and those provided by smaller utilities, private owners of charging stations could share or rent theirs to others. Each MotionWerk station communicates with a Share&Charge app to handle the blockchain-driven control of the charging station and accounting.<sup>32</sup> Slock.it would like to integrate blockchain directly into charging stations at the hardware level, as it did in one case using a Raspberry Pi.<sup>33</sup> The blockchain system consists of Ethereum smart contracts. Simon Jentzsch, Slock.it co-founder and chief technology officer, detailed the system's operation in "Share&Charge Contracts: The Technical Angle."<sup>34</sup> Three aspects of the system stand out:<sup>35</sup>

- » All contracts are 100 percent updatable, giving full control for future adjustments or emergency situations.
- » There is a clear separation in the system between data and logic, a common design principle consistent with "separation of concerns."
- » There is a fully backed digital euro at the heart of the system to facilitate transaction settlement.



Because the system itself is deployed on a public blockchain, it is radically transparent, and allows third parties to engage directly with system operations via contracts, tokens, and accounts, should they choose to do so.

As of 5 October 2017, there were three core tokens viewable through Simon's JSON ABIs (JavaScript object notation application binary interfaces), etherscan.io, or similar tools:

*These open pieces of blockchain infrastructure are radical departures from traditional electronic commerce and business practices.*

Mobility Token:  
0x8262a2a5c61A45Aa074cbeeDE42c808D15ea3ceD

Charging Poles:  
0xb642a68bD622D015809bb9755d07EA3006b85843

Library Manager:  
0xf4d9d65481352C3Afd0750B46FbE0462eb29206d

These open pieces of blockchain infrastructure are radical departures from traditional electronic commerce and business practices. They are far beyond an application programming interface (API), the vanilla way to achieve open interoperation. A traditional API is, in effect, an external *transaction interface* that allows us to get inside a proprietary system. Here, start-ups such as Slock.it are *taking the insides out* and allowing users to operate directly with these systems.

## Figure 1: Simon Jentzsch's coded charging example at GitHub

Note the assignment of an identity to the charging pole .

```
// adjust these values
poleID      = '0x2678394866d17d16a619706d5fd36cacf02d259fd901decbb0b27930f48d6325' // the chargingPole-ID
account     = web3.eth.accounts[0] // the account to use
secondsToCharge = 2 * 3600 //2h
maxCharging = 22000 // 22kwh-charging car

tokenContract = web3.eth.contract(
  [{type: 'function', name: 'approve', inputs: [{name: '_spender', type: 'address'}, {name: '_amount', type: 'uint256'}], outputs: [{name: 'success', type: 'bool'}], payable: false}]
).at('0x8262a2a5c61A45Aa074cbeeDE42c808D15ea3ceD')

chargingContract = web3.eth.contract(
  [{type: 'function', name: 'stop', inputs: [{name: '_poleID', type: 'bytes32'}, {name: '_measuredWatt', type: 'uint32'}], outputs: [], payable: false},
   {type: 'function', name: 'costTimebased', constant: true, inputs: [{name: '_poleID', type: 'bytes32'}, {name: '_user', type: 'address'}, {name: '_wattPower', type: 'uint256'},
   {name: '_secondsToRent', type: 'uint256'}], 'outputs': [{name: 'chargingCost', type: 'uint256'}], 'payable': false},
   {type: 'function', name: 'start', inputs: [{name: '_poleID', type: 'bytes32'}, {name: '_wattPower', type: 'uint32'}, {name: '_secondsToRent', type: 'uint32'}], outputs: [],
   payable: true}]
).at('0x61c810e21659032084444808D2F498789f81CB5')

// unlock you account with your password
personal.unlockAccount(account)

// calculate costs
costs = chargingContract.costTimebased(poleID, account, maxCharging, secondsToCharge)

// approve the tokens
tokenContract.approve(chargingContract.address, costs,{from:account})

// start the transaction
chargingContract.start(poleID,maxCharging,secondsToCharge,{from:account})

// stop it again
chargingContract.stop(poleID,0,{from:account})
```

Source: [gist.github.com/simon-jentzsch/527f6935008509e57b6873af36fe8133](https://gist.github.com/simon-jentzsch/527f6935008509e57b6873af36fe8133). Used with permission.



## Radical transparency: The universal sharing network

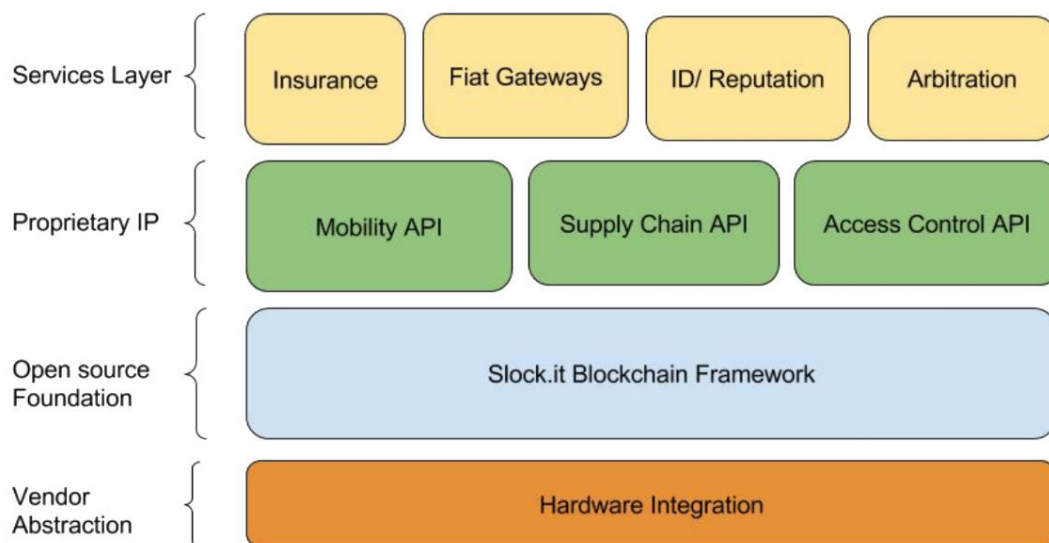
*For the model to succeed, it must overcome the basic liquidity concerns of every other matching or capacity sharing system: it must achieve critical mass.*

This spirit of transparency is central to Slock.it's vision of its universal sharing network. The typical sharing economy systems tend to have central gatekeepers. Very rarely are they true P2P sharing systems. That intermediary—an Airbnb, Uber, or other large middleman—will usually control and manage the system in exchange for a slice of the action. Yet as these systems grow, network effects start to work in their favor. As their power grows, often their slice of the action does, too.

Consider Uber: in addition to raising its own fee structure while pressuring drivers to accept lower payment, it has obfuscated the model for how drivers get paid.<sup>36</sup> Vitalik Buterin, the founder of Ethereum, said that corporations take this type of bait-and-switch approach to openness itself. A start-up might have an open philosophy to encourage system adoption in the beginning, but later locks things down to protect its ability to monetize, said Vitalik. "Building a decentralized service is the strongest way for an application developer to pre-commit not to be a jerk and not to shut down forever."<sup>37</sup>

However, for the USN model to succeed, it must overcome the basic liquidity concerns of every other matching or capacity sharing system: *it must achieve critical mass*. That's where Slock.it's business model comes into play. Rather than bootstrapping each blockchain-based sharing application, Slock.it works with clients to bring their existing customers, products, or sharing networks onto the blockchain, onboarding the liquidity and flow of transactions with them. For Slock.it's clients, the value proposition is an inexpensive ready-made infrastructure suited to their sharing application.

**Figure 2: The Slock.it stack**



Source: [slock.it/technology.html](http://slock.it/technology.html). Used with permission.



*Unlike an application programming interface, which creates access to functions held internally, the USN pulls the functionality onto the network, turning it into a piece of public infrastructure.*

So, while an Airbnb or an Uber could use Slock.it's platform to build its system, it would have to agree to transparency as a key condition of usage: any asset brought onto the network must be visible on the USN. It's open and designed for easy onboarding, too, and so entities don't necessarily need Slock.it's permission to use it.<sup>38</sup> Launching the USN along with compact hardware to handle IoT and smart contract interactions, Slock.it has made it easy to control washing machines and door locks or even to rent a microwave for popping popcorn on the fly. Christoph demonstrated the latter two examples to a live audience at Devcon3.<sup>39</sup>

Slock.it's USN is a *platform* and *delivery network* that allows true P2P sharing in a radically open fashion.<sup>40</sup> By creating sharing systems that operate over Ethereum's public blockchain, business applications operate via a series of public smart contracts. Unlike an API, which creates access to functions held internally, the USN pulls the functionality onto the network, in the process turning it into a piece of public infrastructure. Others can use this infrastructure freely, or extend it in some cases, as if it were their own.

The result is an exceptionally robust public infrastructure capable of mission-critical security. Other features and benefits of the platform include scalable deployment, modular architecture (which accommodates extensions of the system), straightforward clearance and settlement, simple data synchronization, and clear governance that specifies the contractual terms in code.

## Key takeaways

While many organizations are exploring the business applications of blockchain, none can claim to have done so on the public blockchain to the extent that Slock.it has. The process has led to some spectacular successes and failures, and yields immensely valuable insights for building public blockchain infrastructure and business applications.



**Focus on genuine business value, not ICO hype.** The ease with which many start-ups have raised funds through token sales has led to heady speculation. Some of the worst offenders are offering shares of businesses hastily cobbled for investment. "It's ridiculous," said Stephan Tual.<sup>41</sup> Don't get caught up in ICO hype or the dramatic swings in cryptocurrency values. Blockchain firms are just like any other business: they must create genuine value via innovations and customer acquisition.



**Prepare for extreme transparency.** Operating an application on the public blockchain isn't for the faint of heart. Business events are not only out on the blockchain for all to see, but your business and its processes potentially become bits of public infrastructure that anyone can use or

*Blockchain firms are just like any other business: they must create genuine value via innovations and customer acquisition.*



reassemble as they see fit.<sup>42</sup> Businesses themselves can act almost as pieces of open-source software. It's incredibly powerful, but also daunting for many corporate executives and government officials.



**Build in safety nets to handle unanticipated consequences.** Whether you subscribe to the “code as law” philosophy doesn't matter. Once a smart contract is deployed, it is irrevocable.<sup>43</sup> If you want to change your mind, then you need to build that option into the contract. For complex or dynamic systems, any design must allow for future iteration. Share&Charge contracts are 100 percent updatable, for example.<sup>44</sup>



**Look for business model innovation.** Automating your business on the public blockchain is about turning real-world activities into digital code and smart contracts. Before doing that, inspect your current business practices, question management assumptions about the business model, and identify opportunities to do things differently. Blockchain is about business model innovation, not just business model automation.



**Pursue applications that harness key blockchain features.** Even Vitalik Buterin concedes that many apps are perfectly suited to traditional centralized systems.<sup>45</sup> The apps best suited to blockchain are those that embrace, and can benefit from, “trustless” technology features—accurate data storage that's widely distributed, globally accessible, and guaranteed forever with guaranteed execution of programs over long periods of time.<sup>46</sup>



**Insure against the unthinkable.** The Ethereum blockchain hosts digital assets with a market capitalization in excess of \$36 billion and consummates tens of millions of transactions, but this industrial strength and scale do not come easily. For mission-critical systems, put in place bug bounties, time delays, and other measures.



**Start cultivating talent.** Creating a smart contract is hard. Solidity, a language for coding smart contracts, seems easy to use but is actually quite complex. Users must understand the nitty-gritty *anti-patterns*, that is, software design patterns that might be commonly used but can cause code to execute in unintended ways.<sup>47</sup> Competent blockchain developers are also exceedingly difficult to find; Stephan estimated there are as few as 500 in the world.<sup>48</sup> Organizations—both commercial and educational—should look to develop curricula and training programs to meet the need for this expertise.



**Advocate for stewardship of the blockchain.** True autonomy is incredibly difficult. The DAO was challenging, not only technically, but because it involved the orchestration and governance of an autonomous system. Even a concept as simple as a Gregory Maxwell's

*Creating a smart contract is hard. Coders must understand the anti-patterns, that is, software design patterns that might be commonly used but can cause code to execute in unintended ways.*



hypothetical “autonomous Dropbox” turns out to be incredibly hard in practice because of such difficulties as humans gaming the system or dealing with falsified measures.<sup>49</sup> Complex systems are a delicate dynamic balancing act.

Significant short-term opportunities will come from traditional applications ported to the distributed versions on the blockchain, but others will be entirely new and disruptive applications: applications that only blockchain technologies themselves can *bring to life*.



## About the author

Alan Majer is the founder of Good Robot. For the first half of his career, Alan worked as a technology researcher and writer, helping to identify cutting-edge technology and business innovations. Today, Alan also works with new technologies hands on, exploring the potential of connected sensors and the Internet of Things, new display technologies, machine intelligence, robotics, and interactive interfaces. The result is exciting new opportunities to innovate and transform client experiences, and the ability to combine strategy and research activities with a real-world approach to their implementation. Alan is an active member of the local “maker” scene, frequenting spaces like HackLab.to and InterAccess, and he also holds an MBA from McGill University.

## Disclosures

The author has no professional or personal affiliation with or ownership stake in Slock.it or any other company discussed in this paper.







## About the Blockchain Research Institute

Co-founded in 2017 by Don and Alex Tapscott, the Blockchain Research Institute is a knowledge network organized to help realize the new promise of the digital economy. It builds on their yearlong investigation of distributed ledger technology, which culminated in the publication of their critically acclaimed book, *Blockchain Revolution* (Portfolio|Penguin).

Our syndicated research program, which is funded by major corporations and government agencies, aims to fill a large gap in the global understanding of blockchain technology and its strategic implications for business, government, and society.

Our global team of blockchain experts is dedicated to exploring, understanding, documenting, and informing leaders of the market opportunities and implementation challenges of this nascent technology.

Research areas include financial services, manufacturing, retail, energy and resources, technology, media, telecommunications, healthcare, and government as well as the management of organizations, the transformation of the corporation, and the regulation of innovation. We also explore blockchain's potential role in the Internet of Things, robotics and autonomous machines, artificial intelligence, and other emerging technologies.

Our findings are initially proprietary to our members and are ultimately released under a Creative Commons license to help achieve our mission. To find out more, please visit [www.blockchainresearchinstitute.org](http://www.blockchainresearchinstitute.org).

### Leadership team

Don Tapscott – Co-Founder and Executive Chairman  
Alex Tapscott – Co-Founder  
Joan Bigham – Managing Director  
Kirsten Sandberg – Editor-in-Chief  
Jane Ricciardelli – Director of Marketing  
Hilary Carter – Director of Research  
Jenna Pilgrim – Director of Business Development  
Maryantonett Flumian – Director of Client Experience  
Luke Bradley – Director of Communications



## Notes

1. Christoph Jentzsch, CEO, Slock.it, "Building a decentralized sharing economy on top of Ethereum," *Devcon3*, 4 Nov. 2017. [www.youtube.com/watch?v=iRtG\\_6pYqGE](http://www.youtube.com/watch?v=iRtG_6pYqGE), accessed 22 Nov. 2017.
2. Harry Campbell, Christian Perea, "What's the Real Commission That Uber Takes from Its Drivers?" *The Rideshare Guy*, 25 July 2016. [therideshareguy.com/whats-the-real-commission-that-uber-takes-from-its-drivers-infographic](http://therideshareguy.com/whats-the-real-commission-that-uber-takes-from-its-drivers-infographic), accessed 22 Nov. 2017.
3. Gregory Maxwell, "eBitcoin the enabler: Truly Autonomous Software Agents roaming the net," *Bitcoin Forum post*, 6 Dec. 2011. [bitcointalk.org/index.php?topic=53855.msg642768#msg642768](http://bitcointalk.org/index.php?topic=53855.msg642768#msg642768), accessed Oct 3, 2017.
4. Stephan Tual, interviewed by author, 11 Sept. 2017.
5. Mike Hearn, "Mike Hearn: Autonomous agents, self-driving cars and Bitcoin," *Turing Festival*, 23 Aug. 2013; video uploaded 26 March 2017. [www.youtube.com/watch?v=MVyy4t00Ke4](http://www.youtube.com/watch?v=MVyy4t00Ke4), accessed 22 Nov. 2017.
6. Vitalik Buterin, "Bootstrapping a Decentralized Autonomous Corporation: Part I," *Bitcoin Magazine*, 19 Sept. 2013. [bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274](http://bitcoinmagazine.com/articles/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274), accessed 22 Nov. 2017.
7. Vitalik Buterin, "Ethereum: The Ultimate Smart Contract and Autonomous Corporation Platform on the Blockchain," *Vitalik.ca*, 19 Dec. 2013. [web.archive.org/web/20131219030753/vitalik.ca/ethereum.html](http://web.archive.org/web/20131219030753/vitalik.ca/ethereum.html), accessed 22 Nov. 2017. For further reading, see [web.archive.org/web/20150627031414\\_vbuterin.com/ultimatescripting.html](http://web.archive.org/web/20150627031414_vbuterin.com/ultimatescripting.html) and [vitalik.ca/general/2017/09/14/prehistory.html](http://vitalik.ca/general/2017/09/14/prehistory.html).
8. Stephan Tual, interviewed by author, 11 Sept. 2017.
9. Tual, interview, 11 Sept. 2017.
10. Tual, interview, 11 Sept. 2017.
11. Christoph Jentzsch, "The History of the DAO and Lessons Learned," *Slock.it Blog*, 24 Aug. 2016. [blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5](http://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5), accessed Nov 22, 2017.
12. C. Jentzsch, "The History of the DAO and Lessons Learned," 24 Aug. 2016.
13. C. Jentzsch, "The History of the DAO and Lessons Learned," 24 Aug. 2016.
14. Christoph Jentzsch, "Decentralized Autonomous Organization to Automate Governance," *Slock.it website*, n.d. [download.slock.it/public/DAO/WhitePaper.pdf](http://download.slock.it/public/DAO/WhitePaper.pdf), accessed Nov 22, 2017.
15. Tual, interview, 11 Sept. 2017. While the DAO was an independent entity, it had eight named curators, among them Vitalik Buterin, Christian Reitweissner, and Vlad Zamfir.
16. Stephan Tual, communications with author, 13 Oct. 2017.
17. Matthew Leising, "The Ether Thief," *Bloomberg Markets*, Bloomberg Finance LP, 13 June 2017. [www.bloomberg.com/features/2017-the-ether-thief](http://www.bloomberg.com/features/2017-the-ether-thief), accessed 11 Dec. 2017. 12 million ether at a price of \$377.89 would be worth \$4.53 billion, as of 22 Nov. 2017.
18. Cade Metz, "The Biggest Crowdfunding Project Ever—The DAO—Is Kind of a Mess," *Wired*, 6 June 2016. [www.wired.com/2016/06/biggest-crowdfunding-project-ever-dao-mess](http://www.wired.com/2016/06/biggest-crowdfunding-project-ever-dao-mess), accessed 22 Nov. 2017.
19. C. Jentzsch, "The History of the DAO and Lessons Learned," 24 Aug. 2016.
20. Cade Metz, "The Biggest Crowdfunding Project Ever—The DAO—Is Kind of a Mess," *Wired*, 6 June 2016. [www.wired.com/2016/06/biggest-crowdfunding-project-ever-dao-mess](http://www.wired.com/2016/06/biggest-crowdfunding-project-ever-dao-mess), accessed 22 Nov. 2017.
21. Nathaniel Popper, "A Hacking of More Than \$50 Million Dashes Hopes in the World of Virtual Currency," *The New York Times*, 17 June 2016. [www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html](http://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html), accessed 22 Nov. 2017.
22. For the full anatomy of the attack, see [www.bloomberg.com/features/2017-the-ether-thief](http://www.bloomberg.com/features/2017-the-ether-thief), accessed 22 Nov. 2017.
23. BokkyPooBah, "Which accounts are involved in mounting the recursive call vulnerability attacks on The DAO?" *StackExchange*, 18 June 2016. Community updated 13 April 2017. [ethereum.stackexchange.com/questions/6224/which-accounts-are-involved-in-mounting-the-recursive-call-vulnerability-attacks](http://ethereum.stackexchange.com/questions/6224/which-accounts-are-involved-in-mounting-the-recursive-call-vulnerability-attacks), accessed 22 Nov. 2017.



24. David Z. Morris, "The Bizarre Fallout of Ethereum's Epic Fail," *Fortune*, Sept. 4, 2016. [fortune.com/2016/09/04/ethereum-fall-out](http://fortune.com/2016/09/04/ethereum-fall-out), accessed 22 Nov. 2017. However, the story doesn't end there. A group of miners did not accept the fork, splitting away from the main blockchain in an "alternate universe" where the attack did happen, in effect creating another digital currency, Ethereum Classic.
25. However, debate in the aftermath continued. Even the SEC weighed in over a year later on July 2017, concluding that DAO tokens were "securities" but that in this case it would not press any charges. See: [www.sec.gov/news/press-release/2017-131](http://www.sec.gov/news/press-release/2017-131).
26. Tual, interview, 11 Sept. 2017.
27. Tual, interview, 11 Sept. 2017.
28. [slock.it/ethereum\\_computer.html](http://slock.it/ethereum_computer.html), accessed 11 Dec. 2017.
29. Share&Charge formally launched on 1 May 2017.
30. Slock.it staff, communications with author, Oct. 2017.
31. Stephan Tual, "Share&Charge launches its mobile app, on-boards over 1,000 charging stations on the blockchain," *Slock.it Blog*, 1 May 2017. [blog.slock.it/share-charge-launches-its-app-on-boards-over-1-000-charging-stations-on-the-blockchain-ba8275390309](http://blog.slock.it/share-charge-launches-its-app-on-boards-over-1-000-charging-stations-on-the-blockchain-ba8275390309), accessed 22 Nov. 2017.
32. Tual, "Share&Charge launches its mobile app, on-boards over 1,000 charging stations on the blockchain," 1 May 2017.
33. Tual, "Share&Charge launches its mobile app, on-boards over 1,000 charging stations on the blockchain," 1 May 2017.
34. Simon Jentzsch, "Share&Charge Smart Contracts: the Technical Angle," ed. Stephan Tual, Share&Charge, 3 May 2017. [shareandcharge.com/sharecharge-smart-contracts-technical-angle](http://shareandcharge.com/sharecharge-smart-contracts-technical-angle), accessed 22 Nov. 2017.
35. Tual, "Share&Charge launches its mobile app, on-boards over 1,000 charging stations on the blockchain," 1 May 2017.
36. Harry Campbell, Christian Perea, "What's the Real Commission That Uber Takes from Its Drivers?" *The Rideshare Guy*, 25 July 2016. [therideshareguy.com/whats-the-real-commission-that-uber-takes-from-its-drivers-infographic](http://therideshareguy.com/whats-the-real-commission-that-uber-takes-from-its-drivers-infographic); David Z. Morris, "Uber's New Fare System Raises Its Cut While Angering Drivers," *Fortune*, 20 May 2017. [fortune.com/2017/05/20/uber-new-pricing-angry-drivers](http://fortune.com/2017/05/20/uber-new-pricing-angry-drivers), all accessed 22 Nov. 2017.
37. Vitalek Buterin, "The not-so-paranoid case for decentralization," Meetup Presentation (London), 30 March 2015. [www.youtube.com/watch?v=tjxkdniYtkc](http://www.youtube.com/watch?v=tjxkdniYtkc), accessed 25 Sept 2017.
38. "This will take place within a "permissionless" environment, encouraging network effects through a free and easy onboarding of manufacturers' smart objects onto the USN." [slock.it/ethereum\\_computer.html](http://slock.it/ethereum_computer.html), accessed 5 Oct. 2017.
39. Christoph Jentzsch, CEO, Slock.it, "Building a decentralized sharing economy on top of Ethereum," *Devcon3*, 4 Nov. 2017. [www.youtube.com/watch?v=iRtG\\_6pYqGE](http://www.youtube.com/watch?v=iRtG_6pYqGE), accessed 22 Nov. 2017.
40. Global Solution Networks, "10 Types of Global Solution Networks," GSNnetworks, n.d. [gsnnetworks.org/ten-types-of-global-solution-network](http://gsnnetworks.org/ten-types-of-global-solution-network), accessed 22 Nov. 2017.
41. Tual, interview, 11 Sept. 2017.
42. For example, see the latest Share&Charge charging pole events at [etherscan.io/address/0xb642a68bD622D015809bb9755d07EA3006b85843](http://etherscan.io/address/0xb642a68bD622D015809bb9755d07EA3006b85843), accessed 5 Oct. 2017.
43. Primavera De Filippi, "Ethereum: Freenet or Skynet?" Berkman Klein Center Luncheon Series, 15 April 2014. [cyber.harvard.edu/events/luncheon/2014/04/difilippi](http://cyber.harvard.edu/events/luncheon/2014/04/difilippi), accessed 22 Nov. 2017.
44. Tual, "Share&Charge launches its mobile app, on-boards over 1,000 charging stations on the blockchain," 1 May 2017.
45. Vitalek Buterin, "The not-so-paranoid case for decentralization," Meetup presentation, London, 30 March 2015. [www.youtube.com/watch?v=tjxkdniYtkc](http://www.youtube.com/watch?v=tjxkdniYtkc), accessed 25 Sept. 2017.
46. Buterin, "The not-so-paranoid case for decentralization," 30 March 2015.
47. Indeed, some have blamed the Solidity language itself on the difficulty in identifying anti-patterns like the ones that caused the attack on the DAO.
48. Stephan Tual, interviewed by author, 15 Sept. 2017.
49. Tual, interview, 15 Sept. 2017.







[blockchainresearchinstitute.org](https://blockchainresearchinstitute.org)