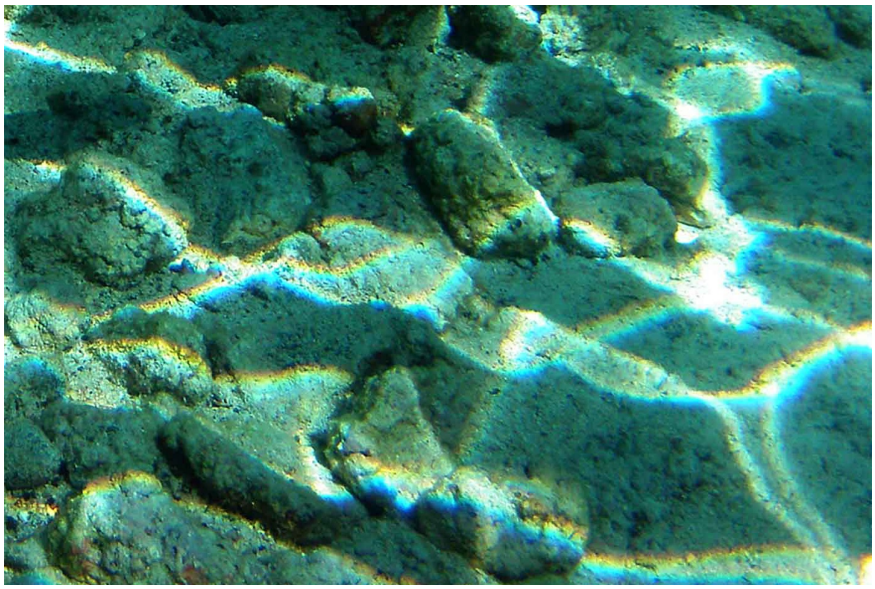
Understanding the blockchain

We must be prepared for the blockchain's promise to become a new development environment.

By William Mougayar, January 16, 2015



Under water in Kona, Hawaii (source: Wikimedia Commons).

Editor's note: this post originally published on the author's website in three pieces: "The Blockchain is the New Database, Get Ready to Rewrite Everything," "Blockchain Apps: Moving from the Jungle to the Zoo," and "It's Too Early to Judge Network Effects in Bitcoin and the Blockchain." He has revised and adapted those pieces for this post.

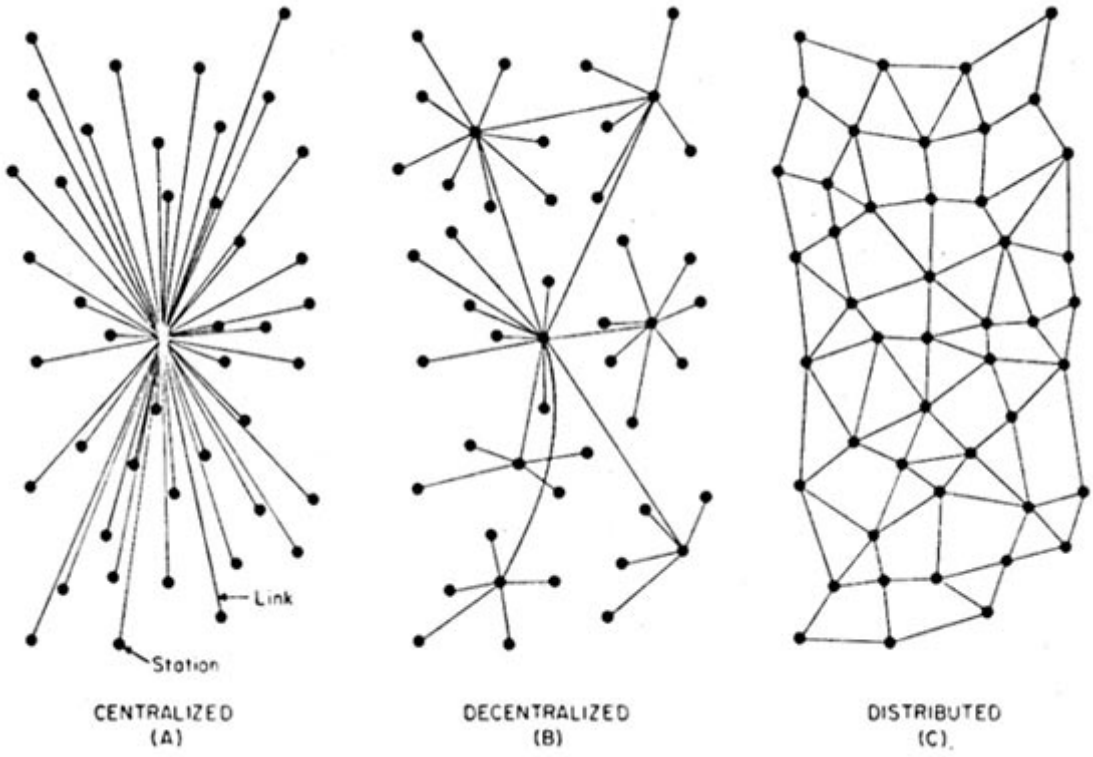
There is no doubt that we are moving from a single cryptocurrency focus (bitcoin) to a variety of cryptocurrency-based applications built on top of the blockchain.

This article examines the impact of the blockchain on developers, the segmentation of blockchain applications, and the network effects factors affecting bitcoin and blockchains.

The blockchain is the new database — get ready to rewrite everything

The technology concept behind the blockchain is similar to that of a database, except that the way you interact with that database is different.

For developers, the blockchain concept represents a paradigm shift in how software engineers will write software applications in the future, and it is one of the key concepts that needs to be well understood. We need to really understand five key concepts, and how they interrelate to one another in the context of this new computing paradigm that is unravelling in front of us: the blockchain, decentralized consensus, trusted computing, smart contracts, and proof of work/stake. This computing paradigm is important because it is a catalyst for the creation of decentralized applications, a next-step evolution from distributed computing architectural constructs.



Source: On Distributed Communications Networks, Paul Baran, 1962

But this is not just a computing phenomena. Decentralized applications are going to enable a decentralization trend at the societal, legal, governance, and business levels because there is a race to decentralize everything and give power to the edge of the networks. So, let's get ready to understand these concepts.

1. Decentralized consensus (on or off bitcoin's blockchain): Decentralized consensus breaks the old paradigm of centralized consensus — i.e., when one central database used to rule transaction validity. A decentralized scheme, on which the bitcoin protocol is based, transfers authority and trust to a decentralized virtual network and enables its nodes to continuously and sequentially record transactions on a public "block," creating a unique "chain": the blockchain. Each successive block contains a "hash" (a unique fingerprint) of the previous code; therefore, cryptography (via hash codes) is used to secure the authentication of the transaction source and removes the need for a central intermediary. The combination of cryptography and blockchain technology together ensures there is never a duplicate recording of the same transaction.

What's important here is that with this degree of unbundling, the consensus logic is separate from the application itself; therefore, applications can be written to be organically decentralized, and that is the spark for a variety of system-changing innovations in the software architecture of applications, whether they are money or non-money related.

You could think of consensus as the first layer of a decentralized architecture. It is the basis for the underlying protocol that governs a blockchain's operation.

2. The blockchain (and blockchain services): A blockchain is like a place where you store any data semi-publicly in a linear container space (the block). Anyone can verify that you've placed that information because the container has your signature on it, but only you (or a program) can unlock what's inside the container because only you hold the private keys to that data, securely.

So, the blockchain behaves almost like a database, except that part of the information stored — its "header" — is public.

The data stored can be a token of value, or a crypto money balance. So, the blockchain acts as an alternative value transfer system that no central authority or potentially malicious third party can tamper with (because of the encryption process). It's based on the public/private hegemony, which is the yin-yang of the blockchain: public visibility, but private inspection. It's a bit like your home address. You can publish your home address publicly, but that doesn't give any information about what your home looks like on the inside. You'll need your private key to enter your private home, and since you have claimed that address as yours, no one else can claim the same address as theirs.

The blockchain can also be seen as a software design approach that binds a number of peer computers together that commonly obey the same "consensus" process for releasing or recording what information they hold, and where all related interactions are verified by cryptography.

3. Smart contracts (and smart property): Smart contracts are the building blocks for decentralized applications. A smart contract is equivalent to a little program that you can entrust with a unit of value (as a token or money), and rules around that value. The basic idea behind smart contracts is that a transaction's contractual governance between two or more parties can be verified programmatically via the blockchain, instead of via a central arbitrator, rule maker, or gatekeeper. Why depend on a central authority when two (or more) parties can agree between themselves, and when they can bake the terms and implications of their agreement programmatically and conditionally, with automatic money releases when fulfilling services in a sequential manner, or incur penalties if not fulfilled?

The starting point that you assume when applying smart contracts is that third-party intermediaries are not needed in order to conduct transactions between two (or

several) parties. Instead, the parties define and agree on simple (or complex) rules, and they embed them inside the transactions, enabling an end-to-end resolution to be self-managed between computers that represent the interests of the users. Smart properties are digital assets (or things) that know who their owners are. Their ownership is typically linked to the blockchain.

4. Trusted computing (or trustless transactions): When you combine the concepts behind the blockchain, decentralized consensus, and smart contracts, you start to realize they are enabling the spread of resources and transactions laterally in a flat, peer-to-peer manner, and in doing that, they are enabling computers to trust one another at a deep level.

Whereas institutions and central organizations were necessary as trusted authorities, a certain number of their central functions can be codified via smart contracts that are governed by decentralized consensus on a blockchain.

Namely, due to the blockchain's role as the unequivocal validator of transactions, each peer can proceed and trust one another because the rules of trust, compliance, authority, governance, contracts, law, and agreements live on top of the technology.

If you fast forward to a not-too-distant future, smart contracts and smart property will be created, dispensed, or executed routinely between consenting parties, without either of them even knowing that blockchain technology was the trusted intermediary.

Arguably, "trusted computing" on the web is a key tenet of the new crypto-driven paradigm.

5. Proof of work (and proof of stake): At the heart of a blockchain's operations is the key concept of "proof-of-work," an integral part of Satoshi Nakamoto's original vision for the blockchain's role as the unequivocal authenticator of transactions. The "proof of work" is a "right" to participate in the blockchain system. It is manifested as a "big enough hurdle" that prevents users from changing records on the blockchain without re-doing the proof of work.

So, proof of work is a key building block because it cannot be "undone," and it is secured via the strengths of cryptographic hashes that ensure its authenticity.

But proof of work is expensive to maintain (estimated cost of $600M per year for bitcoin), and may run into future scalability and security issues because it depends solely on the miners' incentives, which will be declining over time. An upgraded

solution is "proof-of-stake," which is cheaper to enforce but more expensive and more difficult to compromise. Proof of stake not only determines who gets to update the consensus, but it also prevents unwanted forking of the underlying blockchain.

Edging toward a decentralized world

There will be a rush to develop new decentralized apps as a way to enable the decentralized world that we are edging toward.

To that end, business leaders and visionaries will need to learn a new vocabulary around crypto-related frameworks. Developers need to learn how to write decentralized apps that are enabled by blockchain technology. And end-users need to learn how to create or use smart contracts, for example as depicted via the Mist browser vision (Ethereum), which is a mix of marketplace discovery, management dashboard, and creation platform, all-in-one.

We will need to see comprehensive development environments that support a full stack of capabilities and value-add components on top of the blockchain services and consensus engines.

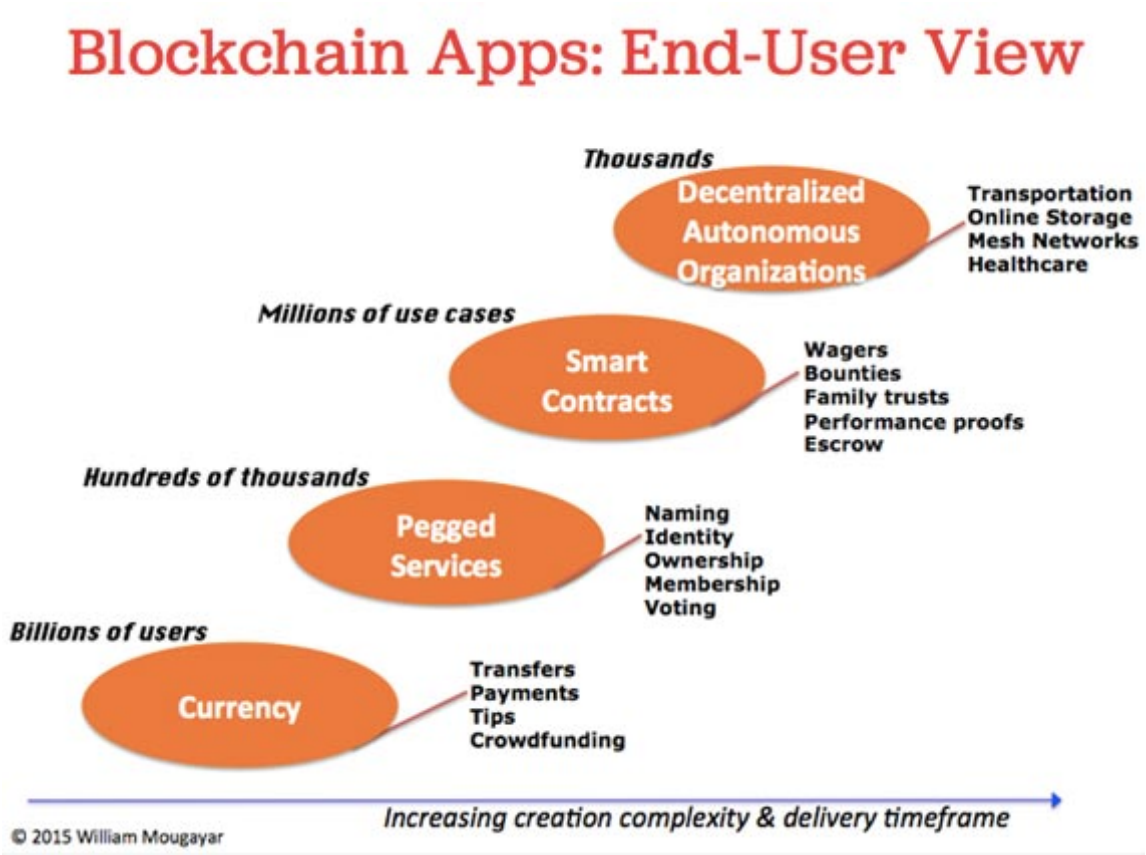
The original bitcoin blockchain technology had limitations as we started to push its limits outside of money-related services and into the software applications realm, so we shouldn't be surprised that the way forward is a world of multiple blockchains. Some of them will be working together, some competing with one another, and others just being benevolent to each other.

Decentralized apps will come in different flavors, sizes, and complexity levels, so we must be prepared for that variety, and we must see beyond the bitcoin promise to be the Internet of money, and into the blockchain's promise to become a new development environment, just as web development was the new paradigm back in 1996.

But decentralized apps are not for everything, and not everything fits a decentralized app paradigm. However, there are a lot of applications that do fit the blockchain distributed paradigm, and that presents a good number of opportunities for developers, creators, and visionaries. Let's call them "blockchain apps."

Four emerging segments for blockchain apps

The graph and table below illustrate these classifications, and I will narrate them, sequentially.



Source: Courtesy of William Mougayar

The *currency*-related segment targets money transfers, payments, tips, or funding applications. The end-user typically goes to an exchange or uses their own wallet to conduct such transactions, benefiting from transaction cost reductions, speeds in settlements, and freedom from central intermediaries. Today's exchanges are centralized, but it's likely we'll see another generation of decentralized trusted exchanges. And although the current bitcoin wallets today are "dumb" wallets, they could become smarter, via an ability to launch smart contracts.

Pegged services to the blockchain represent an interesting segment because these apps utilize the blockchain's atomic unit, which is a "value store" capability, but they also build on top of that with their unique off-chain services. For example, decentralized identity or decentralized ownership is a horizontal blockchain service, but it can be applied to any other vertical segments, such as for videos, music, or photography, just to name a few.

Smart contracts are small programs or scripts that run on a blockchain and govern legal or contractual terms on their own. They represent a simple form of decentralization. They will become available in a variety of application areas, such as for wagers, family

trusts, escrow, time stamping, proofs of work delivery, etc. In essence, they are about moving certain assets or value from one owner to another, based on some condition or event, between people or things. Smart contracts represent an "intermediate state" between parties, and we will trust these smart programs to verify and take action based on the logic behind these state changes.

Legal issues aside, a *Distributed Autonomous Organization* is "kind of" incorporated on the blockchain because its governance is very dependent on the end-users who are part-owners, part-users, and part-nodes on that decentralized network. Key aspects of a DAO are that each user is also a "worker," and by virtue of their "work," they contribute to the value appreciation of the DAO via their collective participation or activity levels. Arguably, bitcoin itself is the "uber DAO."

Category	Protocol User	Frequency	Benefits	Examples
Currency	Exchanges, payment processors, miners, wallets.	Sporadic	Cost, speed.	Coinbase, ChangeTip, *any wallet*, *any exchange*
Pegged Services	Web business	Chronic	Openness, flexibility, new business models, network effects, empowered users.	OneName, Mine, Swarm, Streamium, OpenBazaar, Assembly
Smart Contracts	Contracts service provider, web apps, or end-user with self-service tools.	Episodic	Autonomy, cost, speed, irrefutability.	Mist (by Ethereum), SmartContract, Secure Asset Exchange
Decentralized Autonomous Organizations	DAO itself	Habitual	User protection, user voice, user governance, transparency, self-regulation, sovereignty.	La'Zooz, Storj, MaidSafe, OpenGarden, Bitnation
				Coinbase,

Currency	Exchanges, payment processors, miners, wallets.	Sporadic	Cost, speed.	ChangeTip, *any wallet*, *any exchange*
Pegged Services	Web business	Chronic	Openness, flexibility, new business models, network effects, empowered users.	OneName, Mine, Swarm, Streamium, OpenBazaar, Assembly
Smart Contracts	Contracts service provider, web apps, or end-user with self-service tools.	Episodic	Autonomy, cost, speed, irrefutability.	Mist (by Ethereum), SmartContract, Secure Asset Exchange
Decentralized Autonomous Organizations	DAO itself	Habitual	User protection, user voice, user governance, transparency, self-regulation, sovereignty.	La'Zooz, Storj, MaidSafe, OpenGarden, Bitnation

There may be more categories, but that's how I'm seeing them today. The examples given are only a sample. Regardless, for each segment, there's a simple question in a user's mind: "What is the benefit to me?", and "Why should I participate?" Blockchain apps providers should be focused on answering these questions clearly and via compelling arguments. End-users are the fuel for an app's success, so it's important to stay close to the network effects potential of blockchain apps.

Unpacking the ecosystem's network effects

The concept of "network effects" in the bitcoin and blockchain contexts is a misunderstood one because its inner makings are difficult to grasp accurately. As consumers, we are mostly users of these networks, and we think we understand them from the outside, but that's not enough to judge whether network effects exist or not.

The network effect topic often comes into play when discussing bitcoin versus "other" activity in the cryptocurrency ecosystem, as observers get the illusion there are "silos,"

as Vitalik Buterin aptly described, while others already declare bitcoin's network effect supremacy based on its current currency liquidity and ongoing mining activity.

Let's roll back judgment on network effects and start by understanding the various components of "network effect" sausage-making.

Union Square Ventures has a good definition of network effects in its post "Investment Thesis @USV," and its criteria can be summarized as follows:

- **Size:** Must be large and have scale (relative to the problem set or target community).
- **Inter-connectivity:** Must exist between groups or systems inside the network (a basic requirement).
- **Engaged users:** A good percentage of overall active users (about 30%) comes back often to use the service, at least weekly, if not daily.
- **User experience:** Must be unique, original, and enable some new value creation while users are on the service.
- **Network effects:** The value of the service increases for each user, as others use it or join it, and that value is propagated on the very network that was created.
- **Defensibility:** Barriers to entry are gradually erected and strengthened by virtue of growing the service while it gets more valuable with each new user, also resulting in high switching costs.
- **Monetization:** As the network matures, one or several atomic value units emerge and become the basis for sustainable economic activity.

In order to properly evaluate the network effect puzzle, we need to look at the ecosystem along three key dimensions:

1. **Network effects criteria**
2. **Ecosystem components**
3. **Players and actors**

Buterin wrote a long post titled "On Bitcoin Maximalism, and Currency and Platform Network Effects," where he eloquently dived into the numerous factors surrounding the network effect topic. I agree with the substance of that article, though I'm proposing a more granular inspection of network effect factors (as depicted above).

The second dimension relates to the targeted ecosystem components, and I see them comprised of:

- **Currency liquidity**, including stability and low volatility.
- **Consensus engine**, including the underlying protocols that govern it or support it (e.g. mining).
- **Blockchain platform services**, including the software tools and external linkage capabilities.
- **End-user applications**, including wallets, special browsers, smart contracts, pegged services, or being part of DAO.

The third dimension includes the various players and actors, whether they are based on the bitcoin blockchain or another one, the bitcoin currency or another one, or a fully independent platform.

We could place all of this in a matrix, as depicted below, and if you evaluate your favorite players and actors inside each intersecting box, you will find there are a few holes, plenty of opportunities for improvements, and a lot of works-in-progress.

But wait, there is more to the makings of network effect. You also need to count on:

- Number of apps or services
- Number of users on these apps
- Market capitalizations
- Number of developers
- Security
- Scalability
- Reliability
- Marketing

Even if you evaluate bitcoin proper (because it has revealed itself the most, so far), you will find that it is ahead as a liquid cryptocurrency (though, with an undesirable volatility), has a stable consensus process, and has a developing blockchain platform environment, but its future evolution may face a few blind spots pertaining to its scalability, and it still lacks a large number of engaged/active users that depend on it, on a daily basis.

Bitcoin vs. “other” blockchains

The flip side of the bitcoin singular supremacy argument is that *the bitcoin network doesn’t need to replace the Internet because the Internet already is that global network*. All what bitcoin (or another cryptocurrency player) has to do is to overlay itself on the Internet with its own set of services, and to achieve network effects within those services and applications, based on their own merits. There is a strong case to be made for keeping bitcoin (or any other blockchain) as a thin platform and to not bloat it excessively — rather, let it enable a multiplicity of use cases on top of all of that.

Let’s hope we don’t create an Android versus iOS situation, where the chasm between operating systems, apps, and app stores became the mobile industry’s Achilles’ heel. With crypocurrency-based developments, if we stay within the silos, we might end up not with just two app stores, but with at least a dozen, and that’s not very desirable. Instead, let’s keep working with a little more hegemony and a lot more goodwill to make that happen. Maybe we’ll end up like the cellular carrier industry, where you can pick your carrier, plans, and phones with a reasonable degree of independence, while being assured that all calls will get properly routed.

Imagine that if you used a certain browser, you would only have partial access to the Internet. That would be awful.

While bitcoin’s real network effect may continue to get better, that doesn’t mean we can’t have network effects in other blockchain platforms. We need to think of the “Ecosystem” with a capital “E”, not a lower-case “e.”

There are developers who are writing their app services to be blockchain-agnostic in the future. Let’s not see the multiplicity of work around blockchains and related technologies as as distraction or fragmentation. Rather, we should see it as a multiplicity of innovation and experimentation, and we should celebrate it and support it. Of course, I don’t expect all current players to survive; as in typical start-up fashion, many won’t or might get acquired, but even in failures we will learn.

The reality is that the crypto-led computer science revolution is giving us concepts that go way beyond a one-currency type of scenario. Yes, bitcoin is programmable money, but the blockchain is also programmable value, programmable governance, programmable contracts, programmable ownership, programmable trust, programmable assets, etc. And we have barely scratched the surface on these applications.

It is too early to tell exactly where the cryptocurrency landscape will end up. Maybe it will be like social media, with four giant platforms, dozens of large players, thousands of other companies as beneficiaries, and of course, millions if not billions of end-users. And that would be a good thing.

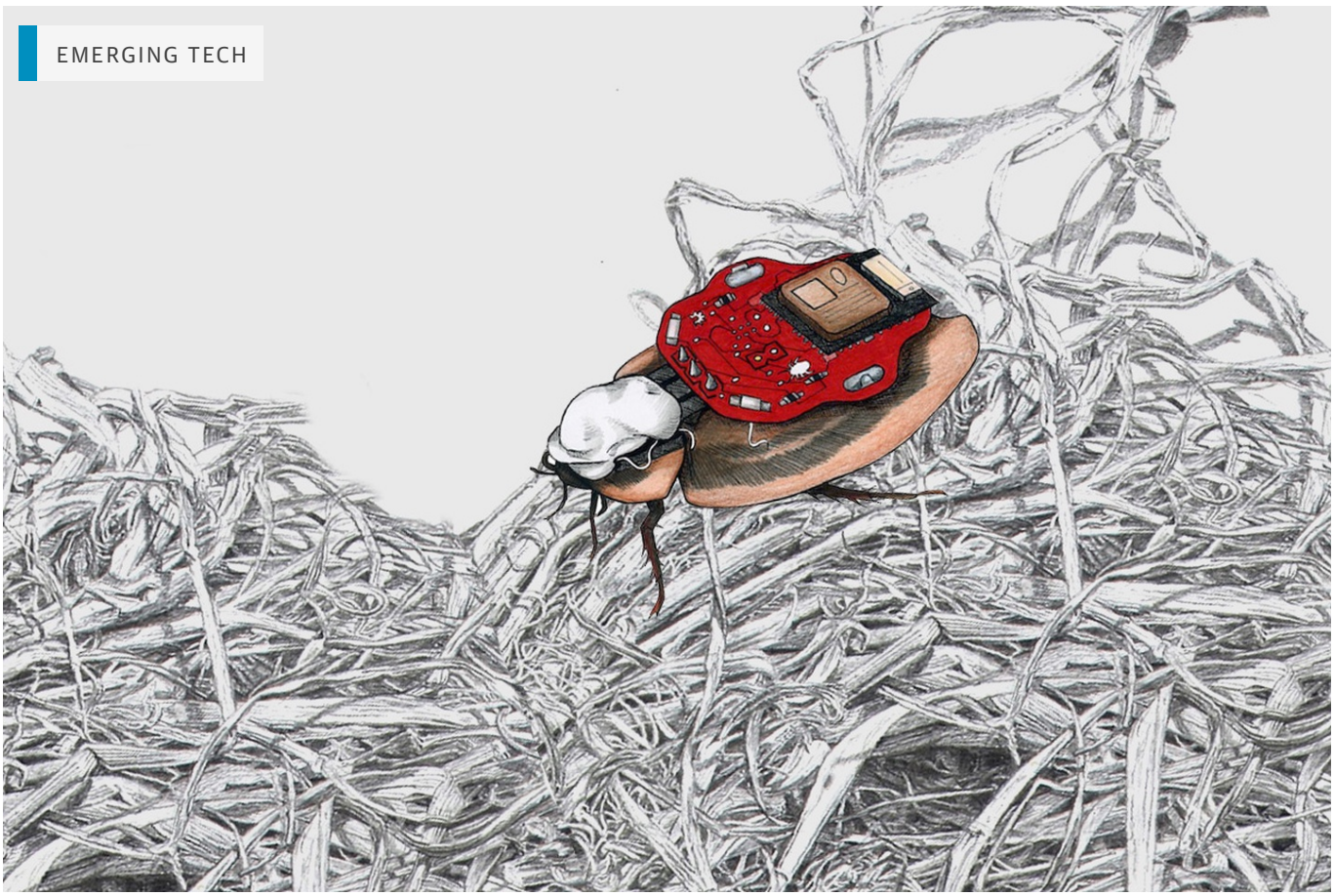
But to get there, let's not forget the basic golden rule of network effects: *without users, there is no network effect*.

Article image: Under water in Kona, Hawaii (source: Wikimedia Commons).

William Mougayar

William Mougayar is a 4x entrepreneur, venture advisor and angel investor, who previously held senior positions at Hewlett-Packard and Cognizant. He is the founder of Startup Management where he blogs and curates on start-ups and the cryptocurrency economy.

EMERGING TECH



Homegrown neuroscience: Backyard Brains and the RoboRoach

By Glen Martin

Control roaches with your smartphone.

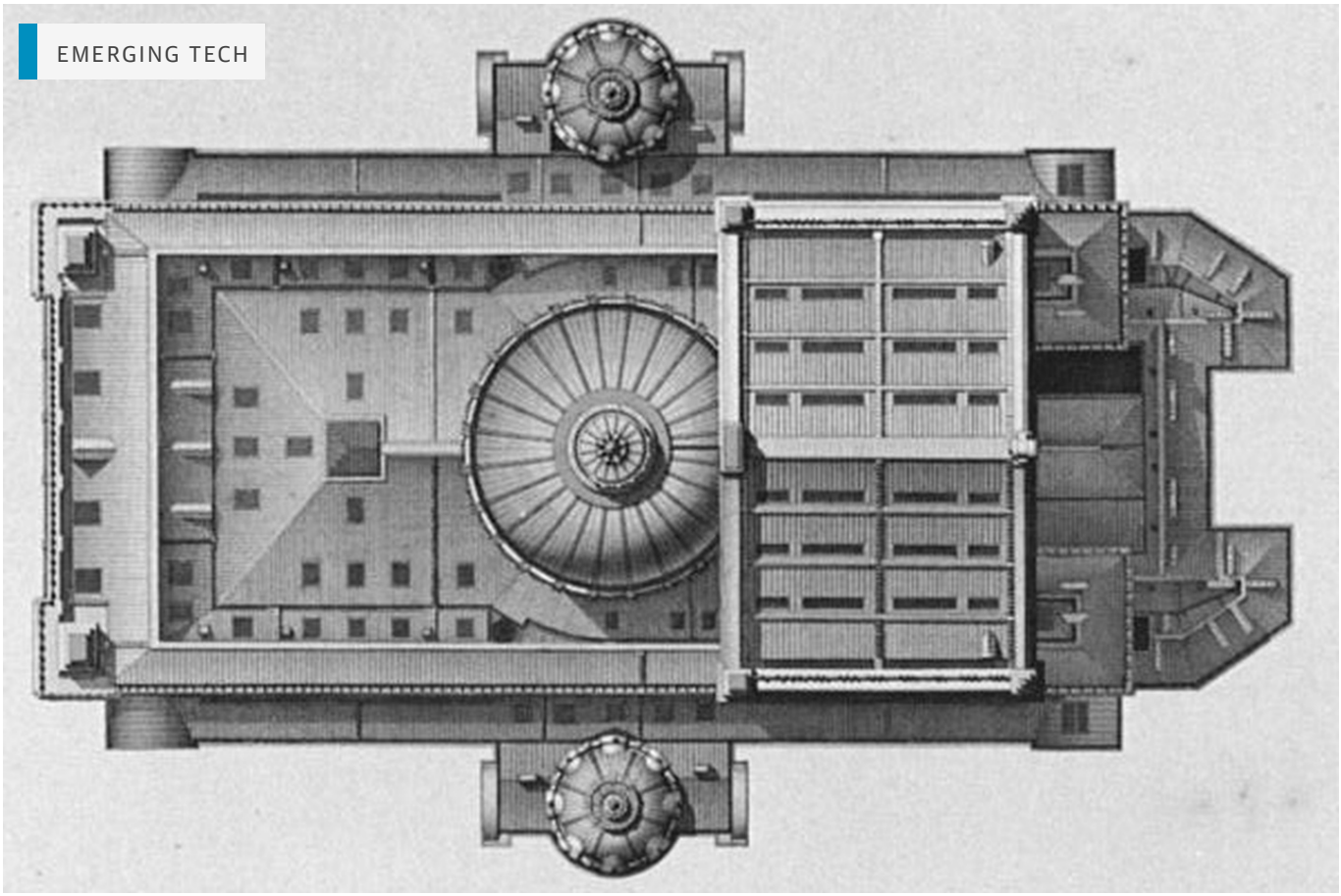
EMERGING TECH

P-values not quite considered harmful

By Mike Loukides

The crisis of reproducibility is an opportunity to get better at doing science.

EMERGING TECH



How the DevOps revolution informs software architecture

By Jenn Webb

The O'Reilly Radar Podcast: Neal Ford on the changing role of software architects and the rise of microservices.

Training in the big data ecosystem

By Jenn Webb

The O'Reilly Radar Podcast: Paco Nathan and Jesse Anderson on the evolution of the data training landscape.