Unenumerated

An unending variety of topics

Thursday, February 09, 2017

Money, blockchains, and social scalability

Introduction

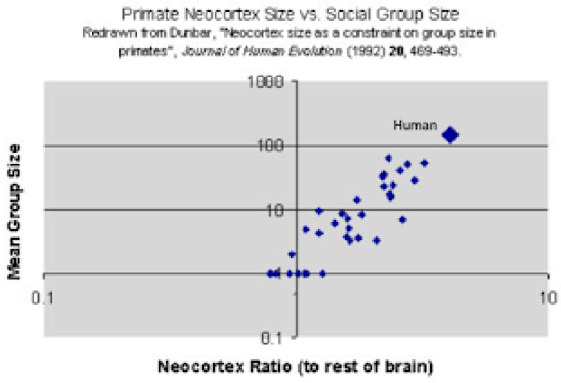
Blockchains are all the rage. The oldest and biggest blockchain of them all is Bitcoin, which over its eight-year history so far starshipped in value from 10,000 bitcoins per pizza (before there were exchanges that priced bitcoin in traditional currencies) to over $1,000 per bitcoin. As of this writing Bitcoin has a market capitalization of over $16 billion. Running non-stop for eight years, with almost no financial loss on the chain itself, it is now in important ways the most reliable and secure financial network in the world.

The secret to Bitcoin's success is certainly not its computational efficiency or its scalability in the consumption of resources. Specialized Bitcoin hardware is designed by highly paid experts to perform only one particular function – to repetitively solve a very specific and intentionally very expensive kind of computational puzzle. That puzzle is called a proof-of-work, because the sole output of the computation is just a proof that the computer did a costly computation. Bitcoin's puzzle-solving hardware probably consumes in total over 500 megawatts of electricity. And that is not the only feature of Bitcoin that strikes an engineer or businessman who is focused on minimizing resource costs as highly quixotic. Rather than reduce its protocol messages to be as few as possible, each Bitcoin-running computer sprays the Internet with a redundantly large number of "inventory vector" packets to make very sure that all messages get accurately through to as many other Bitcoin computers as possible. As a result, the Bitcoin blockchain cannot process as many transactions per second as a traditional payment network such as PayPal or Visa. Bitcoin offends the sensibilities of resource-conscious and performance-measure-maximizing engineers and businessmen alike.

Instead, the secret to Bitcoin's success is that its prolific resource consumption and poor computational scalability is buying something even more valuable: social scalability. Social scalability is the ability of an institution –- a relationship or shared endeavor, in which multiple people repeatedly participate, and featuring customs, rules, or other features which constrain or motivate participants' behaviors -- to overcome shortcomings in human minds and in the motivating or constraining aspects of said institution that limit who or how many can successfully participate. Social scalability is about the ways and extents to which participants can think about and respond to institutions and fellow participants as the variety and numbers of participants in those institutions or relationships grow. It's about human limitations, not about technological limitations or physical resource constraints. There are separate engineering disciplines, such as computer science, for assessing the physical limitations of a technology itself, including the resource capacities needed for a technology to handle a greater number of users or a greater rate of use. Those engineering scalability disciplines are not, except by way of contrast with social scalability, the subject of this essay.

Even though social scalability is about the cognitive limitations and behavior tendencies of minds, not about the physical resource limitations of machines, it makes eminent sense, and indeed is often crucial, to think and talk about the social scalability of a technology that facilitates an institution. The social scalability of an institutional technology depends on how that technology constrains or motivates participation in that institution, including protection of participants and the institution itself from harmful participation or attack. One way to estimate the social scalability of an institutional technology is by the number of people who can beneficially participate in the institution. Another way to estimate social scalability is by the extra benefits and harms an institution bestows or imposes on participants, before, for cognitive or behavioral reasons, the expected costs and other harms of participating in an institution grow faster than its benefits. The cultural and jurisdictional diversity of people who can beneficially participate in an institution is also often important, especially in the global Internet context. The more an institution depends on local laws, customs, or language, the less socially scalable it is.

Without institutional and technological innovations of the past, participation in shared human endeavors would usually be limited to at most about 150 people – the famous "Dunbar number". In the Internet era, new innovations continue to scale our social capabilities. In this article I will discuss how blockchains, and in particular public blockchains that implement cryptocurrencies, increase social scalability, even at a dreadful reduction in computational efficiency and scalability.



Cognitive capacity – here in the form of the relative size of a species' neocortex – set limits on how large primate groups can be. Maintaining animal or intimate human groups requires extensive emotional communications and investments in relationships, such as grooming in primates and gossiping, humor, story-telling, and other conversations, songs, and play in traditional human groups. Overcoming human cognitive limits to who or how many people can participate in an institution – the famous "Dunbar number" of around 150 people -- requires institutional and technological innovation. (Source)

Innovations in social scalability involve institutional and technological improvements that move function from mind to paper or mind to machine, lowering cognitive costs while increasing the value of information flowing between minds, reducing vulnerability, and/or searching for and discovering new and mutually beneficial participants. Alfred North Whitehead said, "It is a profoundly erroneous truism, repeated by all copy-books and by eminent people when they are making speeches, that we should cultivate the habit of thinking what we are doing. The precise opposite is the case. Civilization advances by extending the number of important operations which we can perform without thinking about them." Friedrich Hayek added: "We make constant use of formulas, symbols, and rules whose meaning we do not understand and through the use of which we avail ourselves of the assistance of knowledge which individually we do not

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

Blog Archive

▼ 2017 (3)
► March (1)
▼ February (2)
Conflict and collectibles among the Yurok
Money, blockchains, and social scalability
► 2016 (4)
► 2015 (3)
► 2014 (3)
► 2013 (3)
► 2012 (8)
► 2011 (12)
► 2010 (9)
► 2009 (29)
► 2008 (55)
► 2007 (47)
► 2006 (130)
► 2005 (44)

possess. We have developed these practices and institutions by building upon habits and institutions which have proved successful in their own sphere and which have in turn become the foundation of the civilization we have built up."

A wide variety of innovations reduce our vulnerability to fellow participants, intermediaries, and outsiders, and thereby lower our need to spend our scarce cognitive capacities worrying about how an increasingly large number of increasingly diverse people might behave. Another class of improvements motivates the accurate collection and transmission of valuable information between an increasing number and variety of participants. Yet other advances enable a wider number or variety of mutually beneficial participants can discover each other. All these kinds of innovations have over the course of human prehistory and history improved social scalability, sometimes dramatically so, making our modern civilization with its vast global population feasible. Modern information technology (IT), especially by making use of the historically recent discoveries of computer science, can often discover many more mutually beneficial matches, can improve motivations for information quality, and can reduce the need for trust within certain kinds of institutional transactions, with respect to an increasingly large number and variety of people, thereby further increasing social scalability in some very important ways.

Information flows between minds – what I have called intersubjective protocols – include spoken and written words, custom (tradition), the contents of law (its rules, customs, and case precedents), a variety of other symbols (e.g. "star" ratings common in online reputation systems), and market prices, among many others.

Trust minimization is reducing the vulnerability of participants to each other's and to outsiders' and intermediaries' potential for harmful behavior. Most institutions which have undergone a lengthy cultural evolution, such as law (which lowers vulnerability to violence, theft, and fraud), as well as technologies of security, reduce, on balance, and in more ways than the reverse, our vulnerabilities to, and thus our needs to trust, our fellow humans, compared with our vulnerabilities before these institutions and technologies evolved. In most cases an often trusted and sufficiently trustworthy institution (such as a market) depends on its participants trusting, usually implicitly, another sufficiently trustworthy institution (such as contract law). These trusted institutions in turn traditionally implement a variety of accounting, legal, security, or other controls that make them usually and sufficiently, at least for facilitating the functionality of their client institutions, trustworthy, by minimizing vulnerability to their own participants (such as accountants, lawyers, regulators, and investigators). An innovation can only partially take away some kinds of vulnerability, i.e. reduce the need for or risk of trust in other people. There is no such thing as a fully trustless institution or technology.

The nonexistence of complete trustlessness is true even of our strongest security technology, encryption. Although some cryptographic protocols do guarantee certain specific data relationships with astronomically high probability against opponents with astronomically high computing power, they do not provide complete guarantees when accounting for all possible behaviors of all participants. For example, encryption can strongly protect an e-mail from direct eavesdropping by third parties, but the sender still trusts the recipient to not forward or otherwise divulge the contents of that email, directly or indirectly to any undesired third parties. As another example, in our strongest consensus protocols harmful behavior by certain fractions of participants or intermediaries well short of 100% (as measured by their computing power, stake-holding, or individuation and counting) can compromise the integrity of transactions or information flows between participants and thereby on balance harm the participants. The historically recent breakthroughs of computer science can reduce vulnerabilities, often dramatically so, but they are far from eliminating all kinds of vulnerabilities to the harmful behavior of any potential attacker.

Matchmaking is facilitating the mutual discovery of mutually beneficial participants. Matchmaking is probably the kind of social scalability at which the Internet has most excelled. Social networks like Usenet News, Facebook, and Twitter facilitate the mutual discovery of like-minded or otherwise mutually entertaining or mutually informing people (and even future spouses!). After they have allowed people more likely to be of mutual benefit to discover each other, social networks then facilitate relationships at various levels of personal investment, from casual to frequent to obsessive. Christopher Allen among others has done some interesting and detailed analyses about group size and time spent mutually interacting in online games and associated social networks.

eBay, Uber, AirBnB, and online financial exchanges have brought social scalability via often great improvements in commercial matchmaking: searching for, finding, bringing together, and facilitating the negotiation of mutually beneficial commercial or retail deals. These or related services also facilitate performances such as payment and shipping, as well as verification that other obligations undertaken by strangers in these deals have been performed and communication about the quality of such performances (as with "star rating" systems, Yelp reviews, and the like).

Whereas the main social scalability benefit of the Internet has been matchmaking, the predominant direct social scalability benefit of blockchains is trust minimization. A blockchain can reduce vulnerability by locking in the integrity of some important performances (such as the creation and payment of money) and some important information flows, and in the future may reduce the vulnerability of the integrity of some important matchmaking functions. Trust in the secret and arbitrarily mutable activities of a private computation can be replaced by verifiable confidence in the behavior of a generally immutable public computation. This essay will focus on such vulnerability reduction and its benefit in facilitating a standard performance beneficial to a wide variety of potential counterparties, namely trust-minimized money.

Money and Markets

Money and markets directly benefit the participants in each particular trade by the market matching a buyer with a mutually beneficial seller and by a widely acceptable and standardized counter-performance (money). I use markets here in the sense Adam Smith used the term: not as a specific place or service where buyers and sellers are brought together (although it might sometimes involve these), but rather the broad set of typically pairwise exchanges whereby the supply chain that makes a product is coordinated.

Money and markets also incentivize creation of more accurate price signals that reduce negotiation costs and errors for participants in other similar exchanges. The potent combination of money and market thereby allowed a far higher number and variety of participants to coordinate their economic activities than previous exchange institutions, which more resembled bilateral monopolies than competitive markets.

Markets and money involve matchmaking (bringing together buyer and seller), trust reduction (trusting in the self-interest rather than in the altruism of acquaintances and strangers), scalable performance (via money, a widely acceptable and reusable medium for counter-performance), and quality information flow (market prices).

The greatest early thinker about money and markets was Adam Smith. At the dawn of the industrial revolution in Britain, Smith observed in *The Wealth of Nations* how making even the most humble of products depended, directly and indirectly, on the work of large numbers of a wide variety of people:

> *Observe the accommodation of the most common artificer or day-laborer in a civilized and thriving country, and you will perceive that the number of people of whose industry a part, though but a small part, has been employed in procuring him this accommodation, exceeds all computation. The woolen coat, for example, which covers the day laborer, as coarse and rough as it may appear, is the produce of the joint labor of a great multitude of workmen. The shepherd, the sorter of the wool, the wool-comber or carder, the dyer, the scribbler, the spinner, the weaver, the fuller, the dresser, with many others, must all join their different arts in order to complete even this homely production. How many merchants and carriers, besides, must have been employed in transporting the materials from some of those workmen to others who often live in a very distant part of the country! How much commerce and navigation in particular, how many shipbuilders, sailors, sail makers, rope makers, must have been employed in order to bring together the different drugs made use of*

> *by the dyer, which often come from the remotest corners of the world! What a variety of labor, too, is necessary in order to produce the tools of the meanest of those workmen! To say nothing of such complicated machines as the ship of the sailor, the mill of the fuller, or even the loom of the weaver, let us consider only what a variety of labor is requisite in order to form that very simple machine, the shears with which the shepherd clips the wool. The miner, the builder of the furnace for smelting the ore, the feller of the timber, the burner of the charcoal to be made use of in the smelting-house, the brick maker, the brick layer, the workmen who attend the furnace, the millwright, the forger, the smith, must all of them join their different arts in order to produce them. Were we to examine, in the same manner, all the different parts of his dress and household furniture, the coarse linen shirt which he wears nest his skin, the shoes which cover his feet, the bed which he lies on, and all the different parts which compose it, the kitchen grate at which he prepares his victuals, the coals which he makes use of for that purpose, dug from the bowels of the earth, and brought to him perhaps by a long sea and a long land carriage, all the other utensils of his kitchen, all the furniture of his table, the knives and forks, the earthen or pewter plates upon which he serves up and divides his victuals, the different hands employed in preparing his bread and his beer, the glass window which lets in the heat and the light, and keeps out the wind and the rain, with all the knowledge and art requisite for preparing that beautiful and happy invention, without which these northern parts of the world could scarce have afforded a very comfortable habitation, together with the tools of all the different workmen employed in producing those different conveniences; if we examine, I say, all these things, and consider what a variety of labor is employed about each of them, we shall be sensible that without the assistance and co-operation of many thousands, the very meanest person in a civilized country could not be provided, even according to what we may falsely imagine the easy and simple manner in which he is commonly accommodated.*

And this was before the many successive waves of industrial revolution and globalization between 1776 and now that refined, elaborated, and extended the division of labor many times more. Rather than trusting in the unlikely altruism of so many strangers, markets and money create many pairings of mutual benefit and thus motivate this large network of mutually oblivious people to act in our interests:

> *In civilized society man stands at all times in need of the cooperation and assistance of great multitudes, while his whole life is scarce sufficient to gain the friendship of a few persons…[In contrast to other animals, man has an almost constant occasion for the help of his brethren, and it is vain for him to expect it from their benevolence only. [Exchange is the] manner in which we obtain from another the far greater part of those good offices which we stand in need of. It is not from the benevolence of the butcher, the brewer, or the baker, that we expect our dinner, but from their regard for their own interest.*

Smith goes on to describe how division of labor, and thus labor productivity, depends on the extent of the network of pairwise exchanges: “As it is the power of exchanging that gives occasion to the division of labor, so the extent of this division must always be limited by the extent of that power, or, in other words, by the extent of the market”. As the exchange network around a country and around the globe grows, involving a greater number and variety of producers, so grows the division of labor and thereby labor productivity.

Money facilitates social scalability by increasing the opportunities for this exchange. By lowering coincidence problems (coincidence-of-wants in exchange and coincidence-of-want-and-event in unilateral transfers), via a widely acceptable and reusable form of wealth storage and transfer, money greatly lowered transaction costs, making possible more exchanges of a greater variety of goods and services involving exchanges and other wealth transfer relationships with a much larger number and much wider variety of people.

A wide variety of media, from oral language itself, clay, paper, telegraph, radio, and computer networks, have served to communicate offers, acceptances, and the resulting deals and prices, as well as performance monitoring and other business communications. One of the most knowledgeable observations of the price network produced by markets and money can be found in Friedrich Hayek’s essay, “The Use of Knowledge in Society”:

> *In a system in which the knowledge of the relevant facts is dispersed among many people, prices can act to coordinate the separate actions of different people…in any society in which many people collaborate, this planning, whoever does it, will in some measure have to be based on knowledge which, in the first instance, is not given to the planner but to somebody else, which somehow will have to be conveyed to the planner. The various ways in which the knowledge on which people base their plans is communicated to them is the crucial problem for any theory explaining the economic process, and the problem of what is the best way of utilizing knowledge initially dispersed among all the people is at least one of the main problems of economic policy—or of designing an efficient economic system… The mere fact that there is one price for any commodity—or rather that local prices are connected in a manner determined by the cost of transport, etc.—brings about the solution which (it is just conceptually possible) might have been arrived at by one single mind possessing all the information which is in fact dispersed among all the people involved in the process…The marvel is that in a case like that of a scarcity of one raw material, without an order being issued, without more than perhaps a handful of people knowing the cause, tens of thousands of people whose identity could not be ascertained by months of investigation, are made to use the material or its products more sparingly; i.e., they move in the right direction….The price system is just one of those formations which man has learned to use (though he is still very far from having learned to make the best use of it) after he had stumbled upon it without understanding it. Through it not only a division of labor but also a coordinated utilization of resources based on an equally divided knowledge has become possible…a solution is produced by the interactions of people each of whom possesses only partial knowledge.*

The Social Scalability of Network Security

Where long ago we used clay, and more recently paper, today programs and protocols running on our computers and data networks implement most of our commercial dealings. While this has greatly improved matchmaking and information flow, it has come at the cost of an increase in vulnerability to harmful behavior.

As networks grow, more people with fewer mutually understood habits of and constraints on behavior are added. Security via root-trusting access control, designed for small and chummy offices like Bell Labs where co-workers were well known and income and expenditures well controlled by paper procedures rather than performed on these office computers, breaks down as an efficient and effective security mechanism as organizations become larger, as organizational boundaries are crossed, and as more valuable and concentrated resources such as money are put on or activated via the computers. The more strangers one receives emails from, the more likely one is likely to get a phishing attack or a malware-laced attachment. Traditional computer security is not very socially scalable. As I describe in The Dawn of Trustworthy Computing:

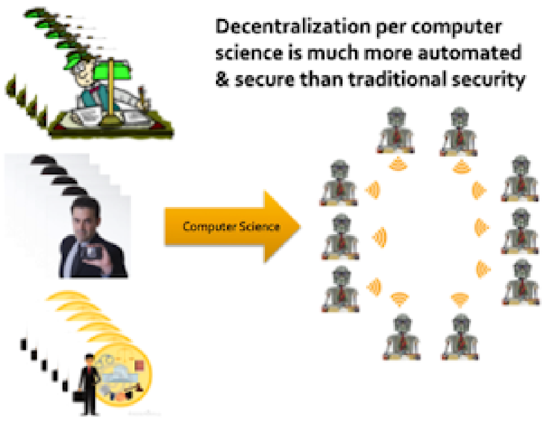
> *When we currently use a smart phone or a laptop on a cell network or the Internet, the other end of these interactions typically run on other solo computers, such as web servers. Practically all of these machines have architectures that were designed to be controlled by a single person or a hierarchy of people who know and trust each other. From the point of view of a remote web or app user, these architectures are based on full trust in an unknown "root" administrator, who can control everything that happens on the server: they can read, alter, delete, or block any data on that computer at will. Even data sent encrypted over a network is eventually unencrypted and ends up on a computer controlled in this total way. With current web services we are fully trusting, in other words we are fully vulnerable to, the computer, or more specifically the people who have access to that computer, both insiders and hackers, to faithfully execute our orders, secure our payments, and so on. If somebody on the other end wants to ignore or falsify what you've instructed the web server to do, no strong security is stopping them, only fallible and expensive human institutions, which often stop at national borders.*

Many server computers are not valuable enough for insiders or outsiders to attack. But an increasing number of others contain valuable concentrations of resources, motivating attack. Centralized root-trusting security scales poorly. As the resources controlled by computers become more valuable and more concentrated, traditional root-trusting security becomes more like the "call the cop" security we are used to in the physical world. Fortunately, with blockchains we can do much better for many of our most important computations.

Blockchains and Cryptocurrencies

Scalable markets and prices require scalable money. Scalable money requires scalable security, so that a greater number and variety of people can use the currency without losing its integrity against forgery, inflation, and theft.

An individual or group communicating under the name "Satoshi Nakamoto" brought Bitcoin to the Internet in 2009. Satoshi's breakthrough with money was to provide social scalability via trust minimization: reducing vulnerability to counterparties and third parties alike. By substituting computationally expensive but automated security for computationally cheap but institutionally expensive traditional security, Satoshi gained a nice increase in social scalability. A set of partially trusted intermediaries replaces a single and fully trusted intermediary.


Decentralization per computer science is much more automated & secure than traditional security
Computer Science

Financial controls on computational steroids: a blockchain as an army of robots, each checking up on each other's work.

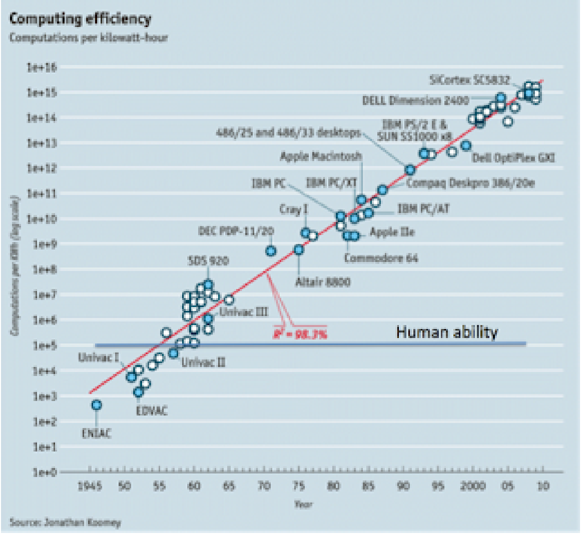
When we can secure the most important functionality of a financial network by computer science rather than by the traditional accountants, regulators, investigators, police, and lawyers, we go from a system that is manual, local, and of inconsistent security to one that is automated, global, and much more secure. Cryptocurrencies, when implemented properly on public blockchains, can substitute an army of computers for a large number of traditional banking bureaucrats. "These block chain computers will allow us to put the most crucial parts of our online protocols on a far more reliable and secure footing, and make possible fiduciary interactions that we previously dared not do on a global network." (Source)

The characteristics most distinctively valuable in blockchain technology in general, and Bitcoin in particular — for example

- independence from existing institutions for its basic operations

- ability to operate seamlessly across borders

come from the high levels of security and reliability a blockchain can maintain without human intervention. Without that high security it's just a gratuitously wasteful distributed database technology still tied to the local bureaucracies it would have to depend upon for its integrity.



Source: Jonathan Koomey

Since the mid-20th century computing has increased in efficiency by many orders of magnitude, but humans are using the same brains. This has created plenty of possibility for overcoming human limitations, and institutions based solely on human minds, with computational capabilities, including in security, doing what they do best, with human minds doing what they still do best. As a result, humans have no more raw mental ability to scale up our institutions than we ever have. But there is plenty of potential for improving social scalability by replacing some human functions with computational ones. (An important note – this argument depends on the slope, not the absolute position, of the human ability line. The absolute position shown above is arbitrary and depends on what human "computation" we are measuring).

A new centralized financial entity, a trusted third party without a "human blockchain" of the kind employed by traditional finance, is at high risk of becoming the next Mt. Gox; it is not going to become a trustworthy financial intermediary without that bureaucracy.

Computers and networks are cheap. Scaling computational resources requires cheap additional resources. Scaling human traditional institutions in a reliable and secure manner requires increasing amounts accountants, lawyers, regulators, and police, along with the increase in bureaucracy, risk, and stress that such institutions entail. Lawyers are costly. Regulation is to the moon. Computer science secures money far better than accountants, police, and lawyers.

In computer science there are fundamental security versus performance tradeoffs. Bitcoin's automated integrity comes at high costs in its performance and resource usage. Nobody has discovered any way to greatly increase the computational scalability of the Bitcoin blockchain, for example its transaction throughput, and demonstrated that this improvement does not compromise Bitcoin's security.

It is probable that no such big but integrity-preserving performance improvement is possible for the Bitcoin blockchain; this may be one of these unavoidable tradeoffs. Compared to existing financial IT, Satoshi made radical tradeoffs in favor of security and against performance. The seemingly wasteful process of mining is the most obvious of these tradeoffs, but Bitcoin also makes others. Among them is that it requires high redundancy in its messaging. Mathematically provable integrity would require full broadcast between all nodes. Bitcoin can't achieve that but to even get anywhere close to a good approximation of it requires a very high level of redundancy. So a 1 MB block consumes far more resources than a 1 MB web page, because it has to be transmitted, processed, and stored with high redundancy for Bitcoin to achieve its automated integrity.

These necessary tradeoffs, sacrificing performance in order to achieve the security necessary for independent, seamlessly global, and automated integrity, mean that the Bitcoin blockchain itself cannot possibly come anywhere near Visa transaction-per-second numbers and maintain the automated integrity that creates its distinctive advantages versus these traditional financial systems. Instead, a less trust-minimized peripheral payment network (possibly Lightning) will be needed to bear a larger number of lower-value bitcoin-denominated transactions than Bitcoin blockchain is capable of, using the Bitcoin blockchain to periodically settle with one high-value transaction batches of peripheral network transactions.

Bitcoin supports a lower rate transactions than Visa or PayPal, but due to its stronger automated security these can be much more important transactions. Anybody with a decent Internet connection and a smart phone who can pay $0.20-$2 transaction fees – substantially lower than current remitance fees -- can access Bitcoin any where on the globe. Lower value transactions with lower fees will need to be implemented on peripheral bitcoin networks.

When it comes to small-b bitcoin, the currency, there is nothing impossible about paying retail with bitcoin the way you'd pay with a fiat currency — bitcoin-denominated credit and debt cards, for example, with all the chargeback and transactions-per-second capabilities of a credit or debit card. And there are also clever ways to do peripheral bitcoin retail payments in which small value payments happen off-chain and are only periodically bulk-settled on the Capital-B Bitcoin blockchain. That blockchain is going to evolve into a high-value settlement layer as bitcoin use grows, and we will see peripheral networks being used for small-b bitcoin retail transactions.

When I designed bit gold I already knew consensus did not scale to large transaction throughputs securely, so I designed it with a two-tier architecture: (1) bit gold itself, the settlement layer, and (2) Chaumian digital cash, a peripheral payment network which would provide retail payments with high transactions-per-second performance and privacy (through Chaumian blinding), but would like Visa be a trusted third party and thus require a "human blockchain" of accountants, etc. to operate with integrity. The peripheral payment network can involve only small value transactions, thereby requiring much less of a human army to avoid the fate of Mt. Gox.

Ralph Merkle: pioneer of public-key cryptography and inventor of hierarchical hash-tree structures (Merkle trees).

Money requires social scalability in its design, via security. For example it should be very hard for any participant or intermediary to forge money (to dilute the supply curve leading to undue or unexpected inflation). Gold can have value anywhere in the world and is immune from hyperinflation because its value doesn't depend on a central authority. Bitcoin excels at both these factors and runs online, enabling somebody in Albania to use Bitcoin to pay somebody in Zimbabwe with minimal trust in or and no payment of quasi-monopoly profits to intermediaries, and with minimum vulnerability to third parties.

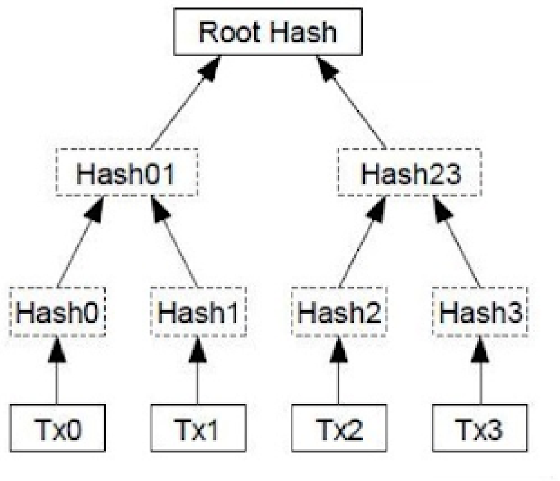
There are all sorts of definitions of "blockchain" out there, almost all of them just implicitly broad hand-waving amid the mountains of marketing hype. I suggest a clear definition that can be communicated to lay people. It is a blockchain if it has blocks and it has chains. The "chains" should be Merkle trees or other cryptographic structures with a similar integrity functionality of post-unforgeable   integrity. Also the transactions and any other data whose integrity is protected by a blockchain should be replicated in a way objectively tolerant to worst-case malicious problems and actors to as high a degree as possible (typically the system can behave as previously specified up to a fraction of 1/3 to 1/2 of the servers maliciously trying to subvert it to behave differently).

₿
¥
N
USh
KSh
CF
TSh

Bitcoin's socially scalable security, based on computer science rather than on police and lawyers, allows, for example, customers in Africa to pay suppliers in China seamlessly across borders. A private blockchain cannot accomplish this feat nearly as easily, since it would require an identification scheme, certificate authority, and PKI shared between these various jurisdictions. (Source)

Because of this fraction, and because of the (hopefully very rare) need to update software in a manner that renders prior blocks invalid – an even riskier situation called a hard fork -- blockchains also need a human governance layer that is vulnerable to fork politics. The most successful blockchain, Bitcoin, has maintained its immutable integrity via decentralized decision-making among experts in the technology combined with a strong dogma of immutability, under which only the most important and rare bug fixes and design improvements, that cannot be made any other way, justify a hard fork. Under this philosophy of governance accounting or legal decisions (such as altering an account balance or undoing a transaction) never justify a hard fork, but should be accomplished by traditional governance outside of (or on top of) the system (e.g. via a court injunction forcing a Bitcoin user to send a new transaction that effectively undoes the old one, or confiscating the particular keys and thus the particular holdings of a particular user).

To say that data is post-unforgeable or immutable means that it can't be undetectably alteredafter being committed to the blockchain. Contrary to some hype this doesn't guarantee anything about a datum's provenance, or its truth or falsity, before it was committed to the blockchain. That requires additional protocols, often including expensive traditional controls. Blockchains don't guarantee truth; they just preserve truth and lies from later alteration, allowing one to later securely analyze them, and thus be more confident in uncovering the lies. Typical computers are computational etch-a-sketch, while blockchains are computational amber. Important data should be committed to blockchain amber as early as possible, ideally directly from and cryptographically signed by the device in which it was generated, to maximize the blockchain's benefit in securing its integrity.



A Merkle tree of four transactions (tx0 through tx3). Combined with a proper replication and chains of transaction blocks protected by proof-of-work, Merkle trees can make data such as transactions post-unforgeable by consensus. In Bitcoin, a Merkle root hash securely summarizes and is used to verify the unaltered state of all the transactions in a block.

My own 1998 "secure property title" architecture had Merkle trees and replication of data tolerant against an objective fraction of arbitrarily faulty software or malicious actors, but not blocks. It demonstrated my theory that you could protect the integrity of globally shared data and transactions, and use that ability to design a cryptocurrency (bit gold). It did not have the more efficient and computationally scalable blocks-and-ledger system that Bitcoin does. Also like today's private blockchains, secure property titles assumed and required securely distinguishable and countable nodes.

Given the objective 51% hashrate attack limit to some important security goals of public blockchains like Bitcoin and Ethereum, we actually do care about the distinguishable identity of the most powerful miners to answer the question "can somebody convince and coordinate the 51%?

Blockchain security is objectively limited and blockchain governance is heavily influenced by the potential for a 51% attack. An attack of course does not have to be called an "attack" by the attackers; instead they might call it "enlightened governance" or "democracy in action". Indeed some kinds of software updates needed to fix bugs or otherwise improve the protocol require a soft fork. Some other kinds of software updates require hard forks, which in Bitcoin pose an even greater security and continuity risks than soft forks. Blockchains, although reducing trust far more than any other network protocols, are still far from trustless. Miners are partially trusted fiduciaries, and those who are not expert developers or computer scientists who have invested a great deal of time in learning the design principles and codebase of a blockchain must place a great deal of faith in the expert developer community, much as non-specialists who want to understand the results of a specialized science do of the corresponding scientists. During a hard fork exchanges can also be very influential by deciding which fork to support with their order books and trade symbol continuity.

Public blockchains thus mostly but not entirely dodge the identity-is-hard bullet and take care of its remaining problem of identifying the most powerful miners at a higher "wet"/"social" level, where it is probably more appropriate, rather than trying to securely map such an inherently wet (brain-based) concept onto the protocol, as PKI (public key infrastructure) rather awkwardly tries to do.

So I think some of the "private blockchains" qualify as bona fide blockchains; others should go under the broader rubric of "distributed ledger" or "shared database" or similar. They are all very different from and not nearly as socially scalable as public and permissionless blockchains like Bitcoin and Ethereum.

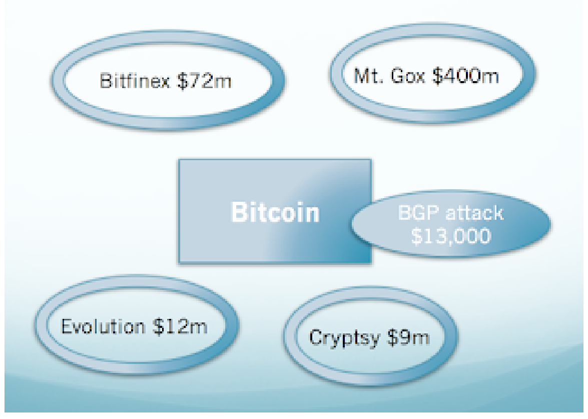
All of the following are very similar in requiring an securely identified (distinguishable and countable) group of servers rather than the arbitrary anonymous membership of miners in public blockchains. In other words, they require some other, usually far less socially scalable, solution to the Sybil (sockpuppet) attack problem:

- Private blockchains
- The "federated" model of sidechains (Alas, nobody has figured out how to do sidechains with any lesser degree of required trust, despite previous hopes or claims). Sidechains can also be private chains, and it's a nice fit because their architectures and external dependencies (e.g. on a PKI) are similar.
- Multisig-based schemes, even when done with blockchain-based smart contracts
- Threshold-based "oracle" architectures for moving off-blockchain data onto blockchains

The dominant, but usually not very socially scalable, way to identify a group of servers is with a PKI based on trusted certificate authorities (CAs). To avoid the problem that merely trusted third parties are security holes, reliable CAs themselves must be expensive, labor-intensive bureaucracies that often do extensive background checks themselves or rely on others (e.g. Dun and Bradstreet for businesses) to do so. (I once led a team that designed and built such a CA). CAs also act as a gatekeeper, rendering these permissioned systems. CAs can become singular points of political control and failure. "Public blockchains are automated, secure, and global, but identity is labor-intensive, insecure, and local."

PKI-enabled private blockchains are a nice for banks and some other large enterprises because they already have mature in-house PKIs that cover the employees, partners, and private servers needed to approve important transactions. Bank PKIs are relatively reliable. We also have semi-reliable CAs for web servers, but not generally speaking for web clients, even though people have been working on the problem of client certificates since the invention of the web: for example advertisers would love to have a more secure alternative to phone numbers and cookies for tracking customer identities. Yet it hasn't happened.

PKI can work well for some important things and people but it is not nearly so nice or so easy for lesser entities. Its social scalability is limited by the traditional wet identity bureaucracy on which it depends.



Some significant thefts in the broader bitcoin ecosystem. Whereas the Bitcoin blockchain itself is probably the most secure financial network in existence (and indeed must remain far more secure than traditional payment networks in order to maintain its low governance costs and seamless cross-border capability), its peripheral services based on older centralized web servers are very insecure. (Source: author)

We need more socially scalable ways to securely count nodes, or to put it another way to with as much robustness against corruption as possible, assess contributions to securing the integrity of a blockchain. That is what proof-of-work and broadcast-replication are about: greatly sacrificing computational scalability in order to improve social scalability. That is Satoshi's brilliant tradeoff. It is brilliant because humans are far more expensive than computers and that gap widens further each year. And it is brilliant because it allows one to seamlessly and securely work across human trust boundaries (e.g. national borders), in contrast to "call-the-cop" architectures like PayPal and Visa that continually depend on expensive, error-prone, and sometimes corruptible bureaucracies to function with a reasonable amount of integrity.

Conclusion

The rise of the Internet as seen the rise of a variety of online institutions, among them social networks, "long-tail" retail (e.g. Amazon), and a variety of services that allow small and dispersed buyers and sellers to find and do business with each other (eBay, Uber, AirBnB, etc.) These are just the initial attempts to take advantage of our new abilities. Due to the massive improvements in information technology over recent decades, the number and variety of people who can successfully participate in an online institution is far less often restricted by the objective limits of computers and networks than it is by limitations of mind and institution that have usually have not yet been sufficiently redesigned or further evolved to take advantage of those technological improvements.

These initial Internet efforts have been very centralized. Blockchain technology, which implements data integrity via computer science rather than via "call the cops", has so far made possible trust-minimized money -- cryptocurrencies – and will let us make progress in other financial areas as well as other areas where transactions can be based primarily on data available online.

This is not to say that adapting our institutions to our new capabilities will be easy, or indeed in particular cases anything short of difficult and improbable. Utopian schemes are very popular in the blockchain community, but they are not viable options. Reverse-engineering our highly evolved traditional institutions, and even reviving in new form some old ones, will usually work better than designing from scratch, than grand planning and game theory. One important strategy for doing so was demonstrated by Satoshi – sacrifice computational efficiency and scalability -- consume more cheap computational resources -- in order to reduce and better leverage the great expense in human resources needed to maintain the relationships between strangers involved modern institutions such as markets, large firms, and governments.

Posted by Nick Szabo at 9:22 AM G+

14 comments:

Anonymous said...

"The secret to Bitcoin's success is certainly not its computational efficiency or its scalability in the consumption of resources"

Success is a subjective term.

1000usd (16bn cap) and 3tx/s after 8 years is not impressive in the grand scheme of things.

Especially, that the alarm bells have been sounded about the implications of the 1MB limit 2 years ago. Today, it causes losses, inconvenience for everyone but speculators trading with IOUs on exchanges.

Insult to injury, the Core team became a group of incompetent narcissists who live in denial and hide behind censorship.

12:26 PM

Evan Sixtin said...

I think he was referring to the success of bitcoin to solve the initial hypothesis which it set out to solve, not any success based on financial value of its token.

2:02 PM

Matt said...

Is there any way to make the font even smaller, I can still read this...

2:08 PM

Johny J said...

There are two ways to scale it: Financially and technically. Lightning network is financial scaling using financial hubs, which is more or less the same as today's banking system.

A better way is to make bitcoin technically scale-able through two layers: Backbone consists of thousands of super nodes running on TB level network, and second layer consists of billions of SPV nodes running mobile app, thus the data traffic itself is scaled by 2 layer, and everyone would still do on-chain transactions with minimum fee

5:10 PM

Debitist said...

Satoshi said we can scale on-chain to VISA level. Szabo says we cannot. If we don't artificially cap the limit by a Politburo, we will find out.

10:55 PM

Anonymous said...

"Lightning network is financial scaling using financial hubs, which is more or less the same as today's banking system."

So what you're telling us is that, in today's banking system, clients digitally sign a transaction with their private key, opening a bi-directional payment channel with a hub that has locked up 100% collateral on a secure distributed ledger, and make payments to other people in the system, who may have like accounts open with other hubs, by passing around digitally signed transactions at line-rate through side channels, incrementing the amount paid to the hub, to be settled at a later date by broadcasting another digitally signed channel-close transaction that is confirmed on the same secure distributed ledger as the channel-open transaction, netting the difference between the hub and the client? I must have skipped that chapter during my Finance class in college!

10:58 PM

Anonymous said...

Nice Post. Just some comments on your paragraph:

"The nonexistence of complete trustlessness is true even of our strongest security technology, encryption. Although some cryptographic protocols do guarantee certain specific data relationships with astronomically high probability against opponents with astronomically high computing power, they do not provide complete guarantees when accounting for all possible behaviors of all participants. For example, encryption can strongly protect an e-mail from direct eavesdropping by third parties, but the sender still trusts the recipient to not forward or otherwise divulge the contents of that email, directly or indirectly to any undesired third parties."

This is not necessarily the case. Plausible deniability does exist for encryption
as does perfect forward secrecy, so you don't actually have to trust the receiver not to share it, it just has to be a situation where there is more than one possible interpretation for what they share. If there are for instance 2 possible interpretations then it might be impossible to determine which of the two is the correct interpretation without additional knowledge found only in the brain of the receiver.

The majority of the trust flows receiver -> sender because deception from the sender is where the problem is. The receiver would have to trust the sender not to lie or deceive more than the sender has to trust the receiver not to tell anyone. So while it's never completely trustless it is not because of the encryption but because of the ability of the sender to lie to the receiver.

- Dana

11:22 PM

Anonymous said...

On the topic of Bitcoin success and in response to the other posters, I don't think we can consider Bitcoin a success. It achieved a goal but it never went mainstream and probably never will.

The issue with Bitcoin is it has no legitimacy and without legitimacy marketing becomes almost impossible because people view it a certain way prior to using it or understanding it. Perhaps Bitcoin would be successful if the goal were to achieve 10 million users in 10 years but a social network can achieve 10 million users in only 2 years. So the amount of users isn't a good measure of success right? So adoption isn't a good measure of success if adoption is going so slow not just for Bitcoin but the entire cryptospace?

Mainstream adoption requires legitimacy and legitimacy is a scarce resource which is difficult to acquire and easy to lose. Unfortunately MtGox took away legitimacy from Bitcoin and Bitcoin may never recover, just as Ethereum lost legitimacy after The DAO got hacked and may never recover from that.

- Dana

11:30 PM

Anonymous said...

At the current transaction capacity, Bitcoin allows for only 10 million people saving a part of their monthly income in money they only control without the approval of any bank or institution. That is if Bitcoin is used only for that purpose, a more realistic number would probably be far less than 1 million people. Is that the aim of a cypherpunk Mr Szabo?

8:27 AM

Anonymous said...

@Anonymous: you didn't understand the essay. Many more people can use Bitcoin indirectly, but probably only about the number you quote can use it directly. There is no other way without sacrificing security and censorship-resistance: the things that make Bitcoin more than an extremely inefficient database.

If you don't agree with Nick (I do) the answer is to start an alternative crypto-currency to Bitcoin and show that it does scale (it won't). Don't just bump a magic number and break the most amazing system human civilization has ever produced. Next time those that run this world will kill it before it gets strong enough to be unkillable by any party on the planet.

8:45 AM

Anonymous said...

The keys to social scalability are closely related to distribution of pricing information and to exchange transaction costs. This discussion of disruption-through-blockchain would be served by more examination of the gains previous generations made or lost through such technologies as the clay tablet, the written law, the rise of mercantile law, the voting mechanisms of Greece and Rome, the shareholder corporation, moveable type, wireless. Our species has made huge scaling advances from the Dunbar number of our wetware: what are the mechanisms by which this scaling has evolved to our current state of huge nations, inscrutable laws, suffocating regulations, international financial vampire squid? Surely these have distributed price information increasingly quickly, and made individual transactions less risky. Salvation will not be found in Merkle trees unless we understand better the risk and cost tradeoffs which have gotten us to the 21st century of the C.E..

1:47 PM

zby said...

The problem with proof of work is not that it is just ineficient - the problem is that it is bound to waste nearlly all profits that it generates.

But there is also this thing that wastefull proof of work is only needed for timestamping. This does not need to be very trusted operation, given that the timestampers don't know what they are stamping. So I imagine you could have a PKI timestamping layer - plus a less trusted distributed layer that would add meaning to the timestamps. This way we could get relatively low trust requirements together with huge efficiency leap.

2:33 AM

Zac Mitton said...

Can you rephrase this sentence:

"This has created plenty of possibility for overcoming human limitations, and institutions based solely on human minds, with computational capabilities, including in security, doing what they do best, with human minds doing what they still do best"

I can't seem to make sense of it.

8:47 PM

Maciano Van der Laan said...

Great insights, I've been researching the blocksize debate and I couldn't make sense of the aggressiveness on bodes sides. I didn't follow the bitcoin community for years, since I'm a silent, confident holder who got tired of all the daily drama

If computer science prevents the bitcoin community, or rather: cryptocurrency community in general, from scaling, it's all that matters. We're stuck with a small blocksize on this layer, bigger ambitions are possible, but on layers on top of the "bitgold" layer.

8:24 AM

Post a Comment

Links to this post

Create a Link

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)