Published Online on 12 June 2018

Proc Indian Natn Sci Acad **84** No. 2 June 2018 pp. 385-407

DOI: 10.16943/ptinsa/2018/49340

Review Article

Blockchain: The Revolution in Trust Management

R K SHYAMASUNDAR and VISHWAS T PATIL*
IIT Bombay

Introduction

TRUST is the cornerstone of our relationships; whether in business, society, or with the institutions that govern us. As Internet has extended the sphere of our ability to do business and conduct personal interactions across the world, its trustworthiness has come under stress in past two decades. Our collective journey through the Internet seems inalienable now as almost all the services that we use today rely on it. Anyone who controls the Internet or the information flowing through it, controls and manipulates our access to online services. It had been a continuous quest to bring trustworthiness to the Internet and the services it enables. Invention of blockchain seems to have quenched that quest.

Since Gutenberg invented the printing press more than 500 years ago, making books and scientific tomes affordable and widely available to the masses. In current times, no other invention empowered individuals and transformed access to information as profoundly as Google. Access to information, to combined with global supply and demand, is reshaping the established conventions and destroying old definitions of doing trade. Technology does not create prosperity any more than it destroys privacy. In this digital era, technology is at the heart of just about everything — the good and the bad. The explosion in online communications for social interactions, online financial transactions and commerce has lead to enormous opportunities for cyber crime. While there had been serious efforts to solve Internet's issues of security and privacy via cryptographic technology, there had always been information leaks due to the underlying trusted third parties (TTP). TTPs have evolved as facilitators of e-transactions. They act as trusted intermediaries between two transacting parties. For example; banks, DNS servers, search engines, news outlets, government registries for land or voters, *et al*. — some interchangeable, others enforced. By definition, TTPs wield enormous power over the transactions they facilitate, since they are at the centre of all the transactions between two or more relying parties. This centralized power constitutes knowledge of information about the transactions, their inclusion and exclusion from ledgers (as in the case of bank's ledgers) or just plain rent-seeking (as in the case of digital certificate issuance by PKIs). Even paying online with credit cards reveals too much personal details with the added issue of high transaction cost. TTPs can quickly turn from facilitators to controllers, at times, with the blessings of the regulators that are statutorily entrusted by the people through their elected governments. The role TTPs play is undeniably important. However, it is equally important to be able to verify the trust enshrined in them is not being abused. So far, we have taken refuge in legislation to do the verification and we have failed miserably time and again as we have tried to solve a technological challenge through non-technological tool, which itself is subject to misuse, favoritism, and malfeasance. Thus, one of the challenging engineering quest had been to build a *Trust Protocol*[1], that would naturally blend with the trust as conceived in our society. The underlying protocol of Bitcoins referred to as Blockchains is expected to disruptively revolutionize the notion of Trust among citizens and governments with respect to currency, societal transactions, finance, asset management, etc.

Blockchain — a new type of database that is immutable, auditable, and distributed — is expected to overcome persistent structural and systemic obstacles confronting people with limited means in getting societal benefits by bringing in transparency to actions by the stakeholders (that includes, among others, government as well) of asset and financial

*Author for Correspondence: E-mail: ivishwas@gmail.com

[1]Or as Nick Szabo termed it *The God Protocol*

systems — thus leading to overcoming excessive bureaucracy, cultural snobbery and corruption. In this exposition, we shall address the possible impact of these concepts in various social sectors for realizing trust and transparency, particularly in the Indian context.

Societal History of Trust

The notion of "trust" as conceived in the society demands a glance at the history of money and currency. Historically, those who had the strongboxes and those who had strong moral fiber emerged as the custodians of people's money and other forms of wealth [Pitroda and Desai, 2010]. Wealth requires protection. In the era of kings, who had armies to protect the wealth, people used to store their produce/ wealth against receipts issued by the kingdom. These receipts were used as a *medium of exchange* for trade. Scarce metals like gold and silver[2] were also used as a medium of exchange in the form of coins having additional benefits of *divisibility, unit of value, fungibility, and universal store of value* (being acceptable across kingdoms). However the precious metal coins suffered by *debasement*. With the invention of printing, paper notes were introduced as currency. Classically, sovereign states appoint central banks to perform this task. In 1609, the Bank of Amsterdam was guaranteed by the City of Amsterdam (major commercial center at that time) and was tasked with bringing *order and efficiency* to the wide range of coinage in circulation in Amsterdam. The Bank accepted local, foreign and debased coins, valued them according to common standards, and then gave *credit* in an account with a common value, bank currency, for which it issued receipts (and charged a small administrative fee.) This standardization of values significantly diminished the incentives to debase money (and the profitability of doing so) and was an important step in making money more *efficient*. The act of state becoming a guarantor of a bank for the protection of wealth is *an act of transitive flow of trust* from the state to a bank (a public or private entity.) The Bank of Amsterdam, initially operated solely as a depository institution, on a 100% reserve basis. In other words, none of the precious metals on deposit were loaned out to other parties. Each receipt issued by the Bank of Amsterdam had equivalent amount of metal deposits in its vault; thus maintaining a *full convertibility* of receipts into precious metals and vice versa. However, the Bank of Amsterdam started *lending* money to the Dutch East India Company, initially on a short-term basis, out of the deposits of others and this activity is known today as *fractional reserve banking*. This was one of the earliest steps toward modern *fiat currency*, generating notes that were only fractionally backed by metal deposits.

In 1694, the Bank of England was founded as a private bank, incorporated to allow William III to borrow 1.2M Sterling that the city goldsmiths could not support. In exchange, for the share rights offer of 1.2M Sterling (that was then lent to the government), the bank gained the *right to issue notes*, including against the government bonds it had received. This was an important right and another step towards modern fiat currency. In time, through a succession of Acts restricting its competitors, the Bank of England came to monopolize bank note issuance in England and Wales, and effectively became the Central Bank of UK. Pound Sterling became the world reserve currency during the period of British East India Company dominating the world trade.

By the 20th century, the US dollar (USD) had replaced the pound Sterling (GBP) as the most important reserve currency in the world and, as a consequence, the Federal Reserve became the key Central Bank in the world. Like the GBP, the USD exhibited a long history of fluctuating through periods of convertibility and non-convertibility to precious metals throughout its history. The US adopted the gold standard in 1879. Having a currency backed by an actual precious metal helped lend *credibility* to the governments that issue it. It facilitated the trust these institutions needed to make their financial system work.

In 1933, President Roosevelt and Congress began taking the US off the gold standard with a resolution[3] nullifying the *right* of citizens to demand payment in gold for their currencies. People were also required to deliver all gold coins, gold bullion, and gold certificates owned by them to the Federal Reserve at a pre-set price of USD 35. By hoarding all of the gold and controlling its price, the Federal

[2]Money must be a store of value and maintain its purchasing power over long periods of time.

[3]an authoritative order or official decree — known as fiat.

Government effectively controlled how much money was in circulation. The irony of the situation is that abandonment of the gold standard was done to build confidence in the economic system of that time of The Great Depression. This introduced the Keynesian model of stimulating economy in recession through state spending.

In 1971, President Nixon announced that the US was no longer in the business of converting dollars to gold at the fixed value of USD 35 per ounce, and thus the gold standard was abandoned *completely*. With the absence of a gold-backed dollar, *US citizens inherited a fiat currency system backed by nothing but the trust in the government*.

Today, the USD is a 100% fiat currency, with no redeemability into any commodity assets, managed by the Federal Reserve. Almost all national currencies that exist today are fiat currencies managed by their respective central banks. US law allows foreign central banks and several international organizations to maintain dollar-denominated deposit accounts at the Federal Reserve. The Federal Reserve is the *fiscal agent* of the US Treasury. Major outlays of the Treasury are paid from the Treasury's general account at the Federal Reserve. Similar relationships exist between national treasuries (i.e., the governments) and national central banks across the globe.

Thus, the societal trust has moved from gold deposits to fiat currency system in each country and also among the countries that are often linked through the US dollar. In other words, for a functional monetary (currency) system to work, citizens need to keep *trust* in it, mediated/guaranteed by its elected[4] government. A point to be seriously noted is that citizens may lose the trust due to excessive bureaucracy, cultural snobbery and corruption. Thus, if citizens don't trust a government to represent their interests, they won't trust its currency—or better put, they won't trust the monetary (currency) system around which their economy is organized. So when given a chance, they will sell that currency and flee it for something they regard as more trustworthy, whether it is the US dollar, gold, or some other safe haven [Vigna and Casey, 2016]. The question is where does the *Trust* flee? *Trust needs an anchor*. And a government's fiat as a foundation for anchoring trust is as credible as the government. As the proverb goes: *trust, but verify*; the promise of fiat cannot be verified in present but only in future, since fiat is a promissory note on future good and it is backed by the strength and stability of a geopolitical system, legal system, and the economy.

Trust in the Internet Era

In the recent history, with the increase in online transactions, and e-commerce, there is naturally a significant increase in privacy leaks and financial fraud — mostly due to the negligence/malfeasance of the TTPs. Thus, started a huge effort on arriving at a cohesive trust protocol to overcome these issues. One of the main impediments for electronic cash *a la* currency was double-spending that reflects the capability of spending the spent cash again and again — arising due to copying coming for free in the digital world. In 1993, a brilliant, secure, anonymous payment system over the Internet, called eCash [Chaum et al., 1988] by Chaum, Fiat, and Naor, was invented mimicking the societal traits and solving the problem of *double-spending* in digital currency. As perhaps the e-commerce volume had not yet reached its tipping point, the scheme did not go far. Also, centralization of trust became a contentious issue with the Cypherpunks[5], since to check the double-spending efforts of the eCash in circulation a central trusted server was required. eCash solved the problem of double-spending and brought anonymity to buyers from the merchants but the central server verifying the double-spend efforts would know behavior of its clients. Cypherpunks wouldn't settle for this drawback. And thus, the quest of a universal, decentralized *trust protocol* continued.

In the meantime, the relevance of the quest for universal trust protocol seemed urgent in light of the following events [Vigna and Casey, 2016]:

1. The remittance of money had increased enormously (the transaction cost and the settlement time remaining quite high.)

[4]Election is a process of entrusting a set of people, for a stipulated period of time, to carry out an agenda that is agreed upon by the majority of the people — irrevocable transfer of trust from the people to the elected.

[5]An informal group, since late 1980s, aimed to achieve privacy and security through proactive use of cryptography. PGP (by Phil Zimmermann) was one of the first notable tools from this movement. David Chaum was also part of this movement.

2. The privacy issues involved and the (hidden!) cost of transactions of credit cards had increased significantly (both in the developed and the developing world.)

3. While the overall literacy in the world increased, a vast majority of the population in poor countries and a large fraction in middle income countries did not have bank accounts. The important point to note is that the reason for not having bank accounts was not education or literacy but due to persistent structural and systemic obstacles [RBI, 2015; Force, 2016][6] confronting people with limited means; in other words, it was due to undeveloped systems of documentation and property titling, excessive bureaucracy, cultural snobbery and corruption.

4. In past decades, hyper-inflation had been experienced in countries like Zimbabwe, Venezuela, Greece, etc. as an outcome of systemic deficiencies in their respective monetary/financial systems. This shows that the elected governments are susceptible to tread a financially disastrous path at the expense of populist decisions. It is understandable that no government would like to undertake arduous path of fiscal prudence to rectify the inherited financial mess, instead they tend to pass it on to the next government, thus increasing the severity of the economic consequences in future. Hyper-inflation, once set in motion, can gradually debase[7] the fiat currency of respective state.

5. In 2008, the global financial system collapsed. It was an epic outcome of lack of transparency in evaluation of toxic assets with banks, failure of (or abuse by) regulators (entrusted legal entities) to identify discrepancies in audits. In hindsight, it appeared to be a collusion between auditors and regulators.

[6]Excessive KYC requirements can hinder financial inclusion as providers might find it too onerous to deal with the poor. The Goal: Design KYC rules that are adequate to the task of maintaining financial integrity, yet do not create unnecessary barriers to financial inclusion. Or get rid of KYC altogether? We shall see one such possibility in the later part of this report.

[7]In 1609, Bank of Amsterdam had done away with the problem of debasement of precious metals by introducing paper currency. Inflation (beyond a moderate level, usually above 2%) is a way of debasing a currency by its issuer! So, how do we control such a potential manipulation of currency? In other words, such a control is a desired property of a digital currency.

Around the same time (end of year 2008), arrived a new decentralized protocol for peer-to-peer digital currency system, using standard cryptographic functions, called *bitcoin* [Nakamoto S, 2008] by a pseudonymous person or a group of people under the name Satoshi Nakamoto. This digital currency, due to the use of cryptographic functions, also referred as cryptocurrency, is different from the fiat currencies as it is neither created nor controlled by any country but is governed by cryptographic algorithms. Bitcoin established a protocol involving distributed computations by the disparate stakeholders that collectively ensure integrity of the data exchanged among billions of subjects without involving a trusted third party. The data created is essentially a distributed ledger denoting the actions (history of transaction) by the stakeholders. This collective data about transactions among subjects, generated periodically as blocks, is referred to as "blockchain". Note that blockchain is cryptographically protected, and resides on distributed network and not on some central database that is under the purview or control of some organization like central bank and hence public! Each stakeholder can see every transaction (transfer of currency from one subject to the other) on the network and terms it to be valid only if it is unspent. Thus an immutable, append-only, global database of spends is generated and maintained by the subjects without any single stakeholder being able to manipulate the entries in the database, also called as ledger. Therefore, blockchain can be termed as a special type of database in which entries only can be *appended* and old entries in the database cannot be updated. Thus giving its transactions *immutability, integrity, transparency*.

In the digital era, all transactions are recorded in ledgers, i.e., in the local ledgers of transacting peers and a copy in the ledger of the TTP who facilitate these transactions. Integrity of these ledgers is of prime importance. Transacting peers implicitly trust a third-party who is tasked with maintenance of the transaction ledgers. To understand the importance of provable guarantees on immutability of transaction data in ledgers we need to first understand the shortcomings of digitally-signed entries in ledgers prevalent in pre-bitcoin internet era.

Triple-entry Accounting and Digital Ledgers

Databases play an important role of accounting in the

Internet era. They have replaced traditional paper based ledgers with double-entry[8] accounting (a balance sheet equation matching the two columns of assets and liabilities — a correct entry must refer to its counterparty) that helps in identifying unintentional human errors in the ledgers and correct them. In paper based ledgers an attempt to fudge the ledger leaves a physical trail of evidence which later could help in investigation of source of malfeasance. By intrinsic nature of digital records, it is not possible to rely on physical evidence of tampering. That is, there is a need for an out-of-the-ledger system to be deployed again in digital form – for which again the same issue applies. The challenge is to terminate the recursion at a level acceptable to the stakeholders. This is resolved through notion of *signed-receipts*, which is captured below.

Double-entry accounting using ledgers is prevalent in all organization including governments as they give an auditable state of movement of assets. Similarly, inter-connected double-entry ledgers give a state of movement of assets across organizations. Unlike the physical ledgers, digital ledgers are remotely accessible and thus can be altered by an attacker without leaving a physical trail. Therefore, while transitioning from physical ledgers to digital ledgers, integrity of ledgers was an important requirement. Double-entry book-keeping provides evidence of intent and origin, leading to strategies for dealing with errors of accident and fraud. The invention of the signed-receipt in the field of financial cryptography brought in these above-mentioned benefits of double-entry book-keeping to digital ledgers. Signed receipts are the digitally signed proofs of transactions — at a given point in time, this information was seen and marked by the signing computer. Digital signatures introduced a new way to create reliable and trustworthy entries, which can be constructed into accounting systems. There are three parties to such transactions: sender of a value, receiver of the value, and the contract manager of this transfer — receipt issuer; a *trusted party*. For example, when Alice wishes to transfer value to Bob in some unit or contract managed by Ivan, she writes out the payment instruction and signs it digitally, much like a cheque is dealt with in the physical world. She sends this to the server, Ivan, and Ivan presumably agrees and does the transfer in his internal set of ledgers. He then issues a receipt and signs it with his signing key. As an important part of the protocol, Ivan then reliably delivers the signed receipt to both Alice and Bob, and they can update their internal ledgers accordingly. This results in three active agents who are charged with securing the signed entry as their most important record of transaction. *In evidentiary terms, the signed-receipt is more powerful than double-entry records due to the technical qualities of its signature*. Triple-entry accounting is a logical arrangement of three-by-three entries, which is a meld of signed-receipts (providing evidentiary power) with double-entry accounting (providing convenience as well as the power to cross-check records locally).

Triple-entry accounting was one of the fundamental contributions of financial cryptography that paved way for modern digital ledgers that not only provide ACID (atomic, consistent, isolated, and durable) properties to the transactions but also the evidentiary property through signed-receipts.

Perils of Centralization of Trust

In this era of globalization, processes, workflows, supply-chains often span across many organizations. Therefore, ledger of an organization gets interfaced with the ledgers of its collaborators. For example, a purchase transaction on Amazon's online store not only leads to an entry in Amazon's ledger but also in the ledgers of sellers, couriers, and also in buyers's/seller's respective bank ledgers. A curious look around us will lead us to realize that everything around us is recorded in ledgers somewhere down the line, the phone calls, travel commutes, payments, property titles, share markets, remittances, *et al*. — almost everything spanning from personal finance to businesses! Whoever controls a ledger[9], wields an enormous power over the subjects of the ledger.

[8]More than 500 years ago a new accounting technique, later known as double-entry bookkeeping, emerged in northern Italy. It was a big step in the development of the modern company and economy. Werner Sombart, a German sociologist who died in 1941, argued that double-entry bookkeeping marked the birth of capitalism. It allowed people other than the owner of a business to keep track of its finances [Economist, 2017].

[9]There are ledgers about ledgers that are usually maintained by entities that are positioned at the top of our communication infrastructure — ISPs, telcos, Governments, PKIs, DNSs — do collect *data about data* called meta-data, which constitutes the ledgers about ledgers.

Digital ledgers with triple-entry feature, which are ubiquitous in our current digital economy are deficient in following aspects:

1. **Efficiency:** In a distributed setup, to preserve the atomicity of a transaction, each entity needs to wait for a signed-receipt before updating the local ledger. Usually, a highly-available, trusted third-party assists the transacting peers to settle transaction efficiently. This leads to a hierarchy where a TTP is at the top and has a view of all transactions being settled through it, which leads to generation of meta-data (data about data) that again forms a new proprietary ledger owned by the TTP!

2. **Cost:** TTPs facilitating online transactions do charge a fee. The problem arises when a TTP achieves a dominant market position (e.g., Western Union, Visa, Uber), the cost of facilitation appears exorbitant. The facilitation is not necessarily be always charged in legal currency, it could be recovered [Patil and Shyamasundar, 2017] by aggregating transaction's meta information and using such information to earn legal currency (e.g., OpenDNS, JustDial.) Despite charging a fees on transaction settlement, there is nothing that stops a TTP from monetizing the transactions' meta-information. Another input to the transaction cost is the cost of dispute resolution.

3. **Transparency:** TTPs tasked with managing a centralized ledger, against which the state/ existence of transactions can be checked, derive an implicit trust of relying parties. Thus, TTPs derive an enormous power over sanctity of past transactions and inclusion/exclusion of on-going/ future transactions. In a distributed setup of inter-connected ledgers, a deliberate or accidental modification or suppression of transaction adversely impacts entries in connected ledgers (e.g., propagation of toxic loans in 2008 US mortgage crisis). Transparency is a trust enhancing property and improves accountability.

4. **Control:** Being the middleman for transactions TTPs have quasi-control over whose transactions can go through their system (e.g., 2010 financial blockade against WikiLeaks) and at what fee. Furthermore, as our digital identities have become our primary identities, TTPs can accidentally or maliciously may annihilate an individual's digital presence. The most serious impact of control is on the personal data front. In the data-driven economy, end users interact with online services that are run by algorithms, which in turn make decisions based on the supplied user data. An error, omission of user data affects the algorithms behavior. Though users are coerced/compelled to share personal data, their interaction with services generate meta-data, which is generated collectively but aggregated and controlled by the service provider without any curative interface for users. This has created a huge information inequality in the ecosystem. This stifles competition among incumbent service providers and puts high entry barrier for the new ones.

These problems stem from our reliance on centralized, trusted third-parties; such as banks, clearing-houses, telcos, credit-rating agencies, government departments and many other big players of our digital economy like Google, Amazon, Facebook that collect and control personal data to provide personalization and convenience. Computational and communication advances are enhancing the speed of transactions and reduction in cost of transactions. But, on the fronts of transparency, fraud-prevention, and control over the data, we have not seen much advancement. The reasons are two-fold: i) in digital economy, data and meta-data is equivalent to gold. It is a compelling differentiator and there is an on-going rush to hoard and control as much of it as possible, ii) lack of a global platform to orchestrate data life-cycle management.

In a stark comparison with old economy, where trust was under strain due to central banks and governments, new digital economy has further aggravated the strain on trust due to the necessity of trusted-third-parties to facilitate online services. Trust is eroding from public sphere in light of large-scale data breaches and a continued diffusion of businesses in personal sphere. At times the regulators appeared to be in collusion with the businesses.

Having foresight of impact of data economy on privacy and digital payment being the Achilles heel, Cypherpunks continued their journey beyond eCash

to build an electronic payment system based on cryptographic proofs instead of fiat trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

Bitcoin: A Currency System without Fiat

In response to the above mentioned impediments to achieve verifiable trust, an experimental, decentralized, P2P platform called Bitcoin was proposed by Satoshi Nakamoto in 2008 (of course, perhaps worked over the years.) The platform was specifically designed for keeping track of cryptocurrency called bitcoin, which is generated by the platform itself. It is a self-breeding platform that generates its own currency to keep itself running. The currency is issued transparently and is continuously accounted for. That is: new bitcoins are generated to represent some work done by someone in the network and they are rewarded to the worker by making an entry in the public ledger of the network. Later, the worker is allowed to spend those earned rewards (i.e., bitcoins) at will, provided such a will to spend is broadcasted to the network and recorded in the public ledger of the network. Similarly, a recipient of bitcoins from a worker is allowed to spend them at will, provided such a will to spend is again broadcasted to the network and recorded in the public ledger of the network. And this goes on. Any node in the network can read the ledger and thus can precisely know the owners of bitcoins at any given time. Therefore, there is transparency and freedom to verify each bitcoins origin and its traversal to current owner. Who (among the many) is authorized to write to the ledger is the challenge that Satoshi solved i.e., consensus in distributed system. Remember that whoever controls a ledger wields enormous power over the subjects relying on the ledger.

In a nutshell, Bitcoin is a global ledger of values that is collectively owned and governed by rules that cannot be amended without a global consensus. The Bitcoin system [Nakamoto, 2008] consists of two *intertwined* components:

- **blockchain:** the protocol to maintain the global ledger, and
- **bitcoin:** the currency to incentivise the maintenance of the global public ledger.

Since the ledger is maintained collectively there is no dependence on a TTP — thus not inheriting the perils of relying on a TTP. Being a global, collectively maintained ledger, everybody can read & validate the transactions in the ledger. The issuance of currency is done as per the ledger maintenance work called mining. Each peer in the Bitcoin network can read the ledger and be assured of ownership of currency at any point in time — thus transparent and publicly auditable, which are trust evoking features.

> *The root problem with conventional currency is all the trust that is required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts.* — *Satoshi Nakamoto*

Through Bitcoin, Satoshi showed an alternative currency system without a central trusted party. The anchor for trust is rooted in cryptographic proofs rather than in governments' fiat. Therefore, very quickly, this currency received a global appeal and acceptance.

Satoshi managed to engineer the concepts of economics; like scarcity, supply, demand, unit of work, incentive, into computer science. At the core of all these concepts is *unit-of-work*: a universally acceptable and verifiable method to quantify a unit of work using computers. Borrowing from the works of Dwork and Naor [Dwork and Naor, 1993], and Adam Backs [Bucks, 2002], Satoshi resorted to SHA256 cryptographic hash function[10], which is usually available on all computing devices, to define unit-of-work. SHA256 function takes an input string and produces a 256-bit long output. Therefore, given an input string, all computers in the world will produce the same 256-bit long output using SHA256. Successive invocations of this function constitutes amount of work. And to define the unit of work itself, Satoshi resorted to a simple condition of having first

[10]It is a mathematical algorithm that maps data of arbitrary size to a bit-string of a fixed size; 256 in the case of SHA256.

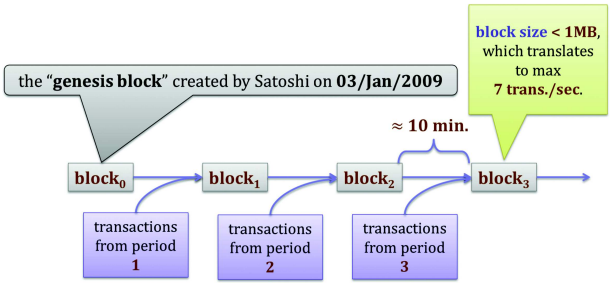

Fig. 5.1: Genesis block as the first block of blockchain (Credit: Stefan Dziembowski)

n bits of the output string to be *zero*, where *n* is a measure of determining hardness/difficulty of the work. In a given time period, a computer that can invoke SHA256 more number of times than other computers in the network has a higher chance of completing the work. How this definition of work is used to build an incentive-based, global, decentralized, ledger management system, we should understand the notion of proof-of-work. Proof-of-work is a method to tie an entity to its successful completion of work before the others and therefore claiming a reward from the system for successfully completing the work. The work is: to extend the ledger with previously unrecorded transactions. The extension is periodic and is constructed as a block consisting of a subset of valid transactions during that period. A block is a unit of successfully completed work — therefore, a sequence of blocks aptly named as blockchain.

Proof-of-Work

It is the algorithmic crux of Bitcoin system, where nodes are incentivized to do work. The first node that publishes a proof of doing a unit of work is rewarded by a pre-determined amount of bitcoins. Once a node broadcasts its proof of work to the network, all other nodes give up their efforts to complete that work (upon verifying the correctness of winning node's broadcasted proof). If the broadcasted proof is correct, a new round to do new work starts. Nodes put efforts to complete the new work before others in order to claim the associated reward. The algorithm adjusts the hardness of work such that, on an average, for every 10 minutes, a unit of work is done by someone in the network.

To collect rewards from the system, nodes need to be identified, which is done by allowing the nodes to independently generate a cryptographic key-pair where the public-key part of the key-pair is node's identifier and the associated private-key is the guardian of the rewarded bitcoins. Rewards (bitcoins) are issued to a public-key iff the corresponding node submits a valid proof-of-work. A node that receives bitcoins as reward is free to transfer these bitcoins (as payment/gift/donation) to others. To transfer a bitcoin, a node composes a transaction that consists of information about how it has received the bitcoin and to whom it wants to transfer that bitcoin. Similar such transactions constructed by other nodes are observed by all nodes and are used as input to generate proof-of-work in the hope of receiving reward from the system. Thus, the consecutive submissions of proofs-of-work that are peer validated and universally accepted, produce a series of blocks as depicted in Fig. 5.1. Each block represents a proof-of-work and its reward is assigned to the respective worker's (aka winner/miner) public key. A block contains transactions that were submitted for confirmation before the creation time of that block. Blocks being of a fixed size, i.e., less than 1MB, it is not guaranteed that all the unconfirmed transactions floating around in the Bitcoin network will be accommodated in current block. Unaccommodated (unconfirmed) transactions may get accommodated in subsequent rounds of proof-of-work. Transactions may optionally offer a fees as a premium so that its inclusion in current block can be prioritized. The creator of a block collects transaction fees on top of the pre-determined reward.

Programming the Concepts of Economics

Through proof-of-work we saw how Satoshi succeeded in defining a universally acceptable unit of work and a mechanism to irrevocably tie the proof to a public-key. In the following we shall see how ingeniously Satoshi encapsulated the other concepts of economics using computational engineering.

Engineering scarcity, supply, and demand: In order to induce value in something, it has to be scarce and known to be limited in supply. Satoshi fixed the total number of bitcoins, to be ever generated by the Bitcoin network, to 21 millions. New bitcoins come to existence approximately every 10 minutes upon a successful proof-of-work round (in other words, upon creation of a new block). For the first 210,000 blocks

the reward was 50 bitcoins/block. For the next 210,000 blocks it halved to 25 bitcoins/block. At present (November 2017) it is 12.5 bitcoins/block. Alternatively,

$$210{,}000 * (50 + 25 + 12.5 + 6.25 + ...) \; 21{,}000{,}000$$

where the last block to be mined is expected in year 2140. Thus, there is a constant but reducing supply of bitcoins from the network. So far, 80% of the total bitcoins have been mined and each trading at USD 11,000 (November 2017) on global bitcoin exchanges. Whereas, it was trading at USD 376 and USD 742 in November 2015 and November 2016 respectively; this highlights the increase in demand of bitcoin. Each bitcoin is divisible up to 10^8 Satoshis — the indivisible unit of bitcoin currency.

Engineering fairness, integrity, and incentive (through proof-of-work): The indivisible unit of work in Bitcoin system is SHA256 — a cryptographic hash function. By definition, a cryptographic hash function maps an arbitrary sized input to a fixed size output such that it is infeasible to determine the input from a given output string. In other words, there is no efficient way to determine an input value mapping to a specific output value. Therefore, the only way to find an input value leading to a specific output value is by repeatedly trying out different input values. The time required to find an input value leading to a specific output value using SHA256 function is directly proportional to the number of invocations of SHA256 function with different inputs. These properties are exploited to construct the proof-of-work algorithm, where the input string consists of 3 elements (2 fixed and 1 random), which are: i) Merkle-root of unconfirmed, valid transactions viewed in the network, ii) hash of most recent block in the blockchain, and iii) a random value (aka salt/nonce), producing an output string of length 256-bits. Proof-of-work algorithm demands the output string conform to a pattern in which first *n* bits of the 256-bit string are *zeros*. The algorithm invokes SHA256 function recursively until an acceptable target string is not obtained. This is depicted in the equation below and in Fig. 5.2.

$H(salt, H_i, transactions) = target$

such that *target* starts with *n* zeros

where *n* is the hardness parameter for proof-of-work algorithm for *a period of time*, which is approximately

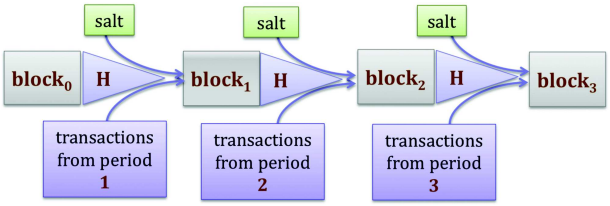

Fig. 5.2: PoW Construction, H is SHA256 (Credit: Stefan Dziembowski)

2 weeks. Hardness parameter is periodically adjusted because the computing power of nodes[11] changes. The hardness adjustment is automatic, and depends on how much time it took to generate the last 2016 blocks (i.e., 2016 x 10 mins = 14 days). If the previous 2016 blocks took more than two weeks to find their respective targets, the hardness is reduced. If they took less than two weeks, the hardness is increased.

Fairness: The probability of finding an acceptable target value for a successful proof-of-work is directly proportional to the disposable hash power of a miner. Miners sell their bitcoins (in open in market for USD to purchase new hardware) in order to increase their hash power so that their probability to find proof-of-work increases. The system takes care of potential spike in computational power in the network by adjusting the hardness value (depicted in Fig. 5.3) in finding a target value.

Integrity: The computational cost of changing any transaction in old blocks is compounded by each new block that gets appended to the chain. When a new block is being created, it contains the hash of the one before it. Any changes in old blocks will result in invalid hashes for all subsequent blocks. Therefore, it is impossible to insert bogus modifications into a previous block without having to repeat all the work that was performed after that block.

Incentive: Proof-of-work produces a block containing a special transaction (*coinbase*) that transfers the reward to the miner. Reward provides incentives to be a miner. It also makes the miners interested in broadcasting new block as soon as possible. On top of this, a specification in Bitcoin states that "from

[11]Nodes having relatively large dedicated hash power are called bitcoin miners. Analogy of miners for nodes is derived from gold miners who voluntarily spend their efforts to find gold in mines with the hope of finding gold. Finding gold is rewarding and vice versa is penalizing.

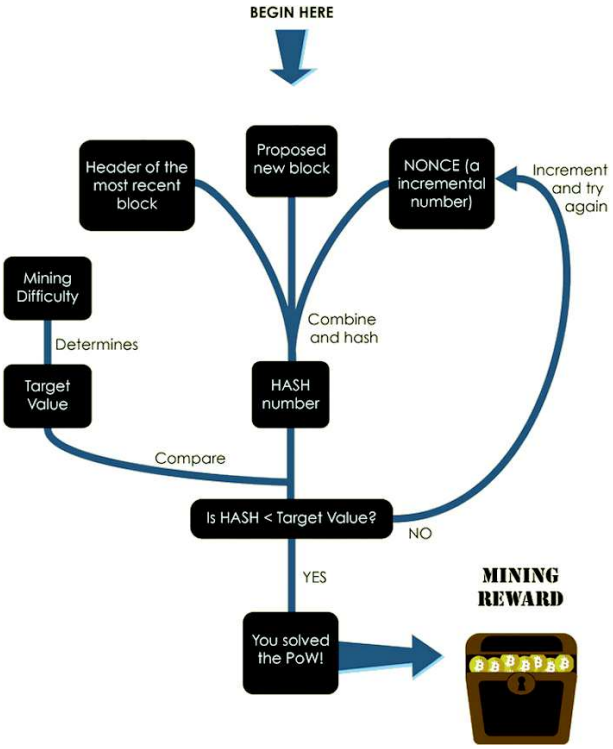

Fig. 5.3: Hardness determines the target value for proof-of-work in a given period (Credit: Patricia Estevão)

two blocks of equal length, mine on the first one that you received", which brings sense of urgency in broadcasting successful proof-of-work to the network at the earliest.

Engineering financial inclusion (through pseudonymity): Owners of bitcoins are identified by their public keys. Public keys are a very peculiar type of identifiers. They can be generated by anyone and are always associated with its corresponding private key which is generated simultaneously. As an analogy, if public key is considered as login, private key is its *permanent* password — and it can be used without providing it to its verifier. This is in stark contrast with other identifiers like email, bank account, mobile number, because these type of identifiers are generated by and assigned to subjects. And, a copy of passwords associated with these identifiers is stored with its issuer in order to perform authentication. Therefore, subjects using such identifiers can be identified and revoked (excluded from respective systems) by the identity issuer as the issuer owns the identifiers in its namespace. Whereas, a public key is an identifier generated and issued by a subject to self along with its corresponding private key. This helps a subject to remain pseudonomous as long as it desires.

Engineering transparency and auditability (therefore accountability): The chain of blocks at any given time provides the list of verified transactions accepted by the network. In its simplest configuration, the protocol allows any peer to scan through these verified transactions. The participants can trust the integrity of the network verified transactions because it is computationally infeasible for an adversary to change any network verified transaction. This is so because changing any transaction in a block will change the block's output hash, which will impact the proof-of-work value of the next block in the chain. Note that each block's creation requires previous block's hash value as an input to generate the proof-of-work. Furthermore, availability of all the previous transactions to each participant of the network brings non-repudiation to transactions and transparency in the network.

Bitcoin is the first real-world application of blockchain protocol where proof-of-work is used as a type of consensus algorithm. It is a trusted, self-regulating, transparent application of global transfer of money where the transactions listed in the *chain of blocks* are equivalent to the ledger entries of any traditional bank. Today's value-transfer systems rely on central ledgers. Banks, governments, telcos *et al*., have a big computer (database) that keeps track of who owns what. And when one makes a payment, the central ledger is updated. Bitcoin updates the ledger in a completely different way. It does not have a centrally controlled ledger. Instead, everybody who runs the (full node) software has their own copy of the ledger. Hundreds of thousands of people have a full copy of the ledger. This means no single person/entity can deny availability of the ledger, confiscate the value/asset marked against an identity, or charge an unfair fee for transactions to go through. And the genius of Bitcoin was to figure out a way to encourage people to maintain these ledgers collectively by consensus and with no trusted third parties.

This new way of deriving trust and transparency in a distributed environment like Internet has tremendous potential to re-engineer all the prevalent systems and applications that are under stress due to a lack of trust and transparency. Bitcoin is one such attempt to put forward an alternative financial system

where trust is anchored in cryptographic algorithms instead of the fiat of a government. The technology worked on the principle that currency is just an accounting tool — a method for abstracting value, assigning ownership, and providing a mean for transacting. It turns out that such a system may be useful for much more than just currency.

Bitcoin

By forcing miners to provide proofs and then rewarding them for their work, Satoshi created the first viable peer-to-peer digital currency. But he also solved a more general problem that had vexed computer scientists for decades — consensus. Consensus in distributed systems has been rigorously studied in Computer Science for past few decades as Byzantine Generals Problem or Chinese Generals Problem, in which two generals have to come to a common agreement on whether to attack or retreat, but can communicate only by sending messengers who might never arrive.

> Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors.
>
> Achieving reliability in the face of arbitrary malfunctioning is a difficult problem, and its solution seems to be inherently expensive. The only way to reduce the cost is to make assumptions about the type of failure that may occur. For example, it is often assumed that a computer may fail to respond but will never respond incorrectly. However, when extremely high reliability is required, such assumptions cannot be made, and the full expense of a Byzantine Generals solution is required BGP [Lamport *et al.*, 1882].

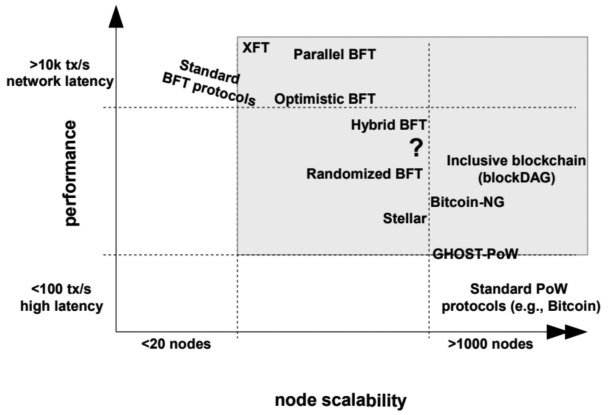

Fig. 5.4: Illustration of performance and scalability of different families of PoW and BFT protocols as discussed in [Vukolić, 2016]

Bitcoin system through its proof-of-work algorithm solved this long standing problem of consensus in distributed system. Bitcoin is at its core, a technology that enables a series of achievements that were not possible before, and not just a global cryptocurrency. Decentralized consensus can create more robust systems in a multitude of ownership or attestation related roles. Currency should be considered as the first application of this technology. Since BGP is a general problem in distributed systems, the same concept can be employed for other purposes. Motivated by Bitcoin, there is a flurry of projects tweaking components of the system and solving different problem of practical importance, which were not addressable before due to lack of a practical consensus method. We shall not get into the details of the tweaks but broadly categorize them into two verticals: permissioned and permissionless — both as types of trust management system with an increasing degree of underlying trust. Some variants built for the want of speed of transaction at the cost of trust, some built for the want of capturing value representation other than currency like land records. This whole family of variants is conveniently called as blockchains, each differing from the other based on the underlying consensus mechanism. There is a subset of variants that use BFT (Byzantine Fault Tolerance) algorithm to construct their consensus algorithm. We briefly mention the prominent ones below.

So far, Bitcoin is the most successful deployment of blockchain protocol with proof-of-work (PoW) as its consensus algorithm. Similar to bitcoin, several alternative cryptocurrencies (altcoins.com) were deployed with slight improvements in objectives. Projects like Stellar (stellar.org), Ripple (ripple.com) are using concept of blockchain to perform global inter-bank settlements with their own private cryptocurrencies; lumens and XRP respectively. An interesting proposal of programmable (Turing-complete; unlike Bitcoin, which has limited set of operations) blockchain called Ethereum [Buterin 2013, Wood 2014] was floated in year 2013, which is gathering momentum recently in business domain [ConsenSys (consensys.net), Corda (corda.net), Augur (augur.net), *et al*.] Ethereum is inspired by Bitcoin and presented an alternative consensus forming algorithm called proof-of-stake (PoS) to assuage the concerns of power consumption and latency in verification of transactions in Bitcoin. A prominent permissioned variant called Hyperledger Fabric (https://www.hyperledger.org) is an open-source project championed by IBM et al that uses PBFT (practical Byzantine fault tolerance) [Castro and Liskov, 1999] as its consensus algorithm. Several other noteworthy consensus algorithms in this space are: Paxos/RAFT [Ongaro and Ousterhout, 2014], Hashgraph [Baird, 2016], Algorand [Micali, 2016], PoET (Proof of Elapsed Time), Blockstack [Ali *et al*., 2016]. Fig. 5.4 illustrates a comparison between Proof-of-Work and BFT (Byzantine fault tolerance) types of consensus algorithms for performance and scalability. And, in Table 5.1 their high level feature-wise comparison is presented.

Bitcoin ushered a completely revolutionary consensus protocol through blockchain. It is revolutionary because it showed a way to handle trust without TTPs and suddenly there is an invigorating stock-taking of all prevalent trust management frameworks (in business, society, or with the institutions that govern us). Old ways of doing transactions are being re-engineered and a completely new set of applications are being engineered — with blockchain, at their core, as a service that offers trust, similar to cloud service that offers on-demand compute, storage, network. In the following we take an abstract view of blockchain and treat it as a machine that provides trust as a service!

Blockchain: The Trust Machine

Conceptually, a blockchain as a machine;

1. stores data (in a shared, distributed ledger),
2. performs some computation (read data from ledger, append data to ledger),
3. reach consensus about the both (through algorithms like PoW), and
4. at each epoch changes its internal state to a new state.

Fig. 5.5 depicts the Bitcoin blockchain protocol as a simple state machine, where “code” starts with

Table 5.1: High-level comparison between PoW and BFT blockchain consensus families for a set of important blockchain properties. Entries in bold suggest desirable features and highlight advantages of one consensus family over the other [Vukolić, 2016]

	PoW consensus	BFT consensus
Node identity management	**open, entirely decentralized**	permissioned, nodes need to know IDs of all nodes
Consensus finality	no	**yes**
Scalability (# of nodes)	**excellent (thousand of nodes)**	limited, not well explore
Scalability (# of clients)	excellent (thousands of clients)	excellent (thousands of clients)
Performance (throughput)	limited (due to possibility of chain forks)	excellent **(tens of thousands tx/sec)**
Performance (latency)	high (due to multi-block confirmations)	**excellent (matches network latency)**
Computational requirement	high	**moderate**
Network synchrony assumptions	physical clock timestamps (e.g., for block validity)	none for consensus safety **(synchrony needed for liveness)**
Correctness proofs	no	**yes**

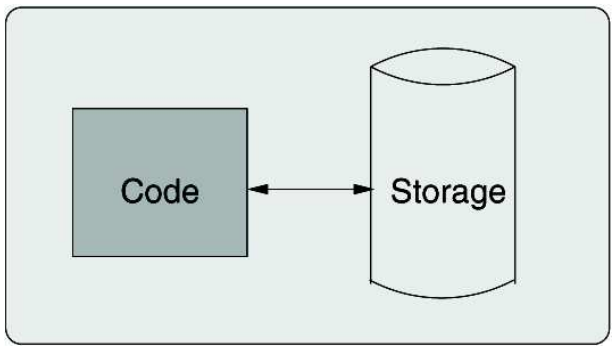

Fig. 5.5: Bitcoin code interacting with immutable storage

a state fetched from the "storage" and the new state is written back (i.e., appended) to the "storage." Fig. 5.6 shows a simplified version of the bitcoin script responsible to transfer value from sender "S" to receiver "R". In an abstract way, blockchain is trusted for correctness but not for privacy since it exposes internal state to everyone, at least in its primitive form.

Bitcoin can be said as a special purpose program running on blockchain. Functionally it serves only one purpose — transfer of value. The underlying technology blockchain ensures users' trust in the system by thwarting double-spending attempts from malicious users. In Bitcoin system, *bitcoin* (the currency) and *blockchain* (the algorithm) are inseparable. Bitcoin (the currency) creation requires blockchain and blockchain requires bitcoins to incentivize PoW. The elegance of the protocol is in delivering trust without a TTP. It is a self-sustained, self-regulating, transparent "trust machine." Anyone can rely on it but for only one functionality, that is, transfer of value.

In year 2013, Ethereum was proposed as a new general purpose blockchain that promised more than "transfer of value". It proposed a Turing-complete language to write code that not only does "transfer of value" but also any functionality that can be digitally controlled/interfaced (e.g., transfer of shares, real-estate, etc.).

To put Bitcoin and Ethereum in perspective; Bitcoin is a special-purpose blockchain (like a stand alone Calculator) whereas Ethereum is a general-purpose blockchain (like Android - on which Calculator is an app along with many other apps). Ethereum uses Proof-of-Stake as its consensus algorithm, which is bootstrapped from Proof-of-Work initially. Ether is the currency on Ethereum platform that can be used to buy "*stake*". Stake provides proportionate voting (consensus) rights. *Gas* is another concept introduced in Ethereum. A pre-defined amount of gas is required to execute a smart contract, which is nothing but a program having its own code and storage, that is, its own state. Gas measures how much "work" an action or set of actions takes to perform. Every operation that can be performed by a transaction or contract on the Ethereum platform costs a certain amount of gas, with operations that require more computational resources costing more gas than operations that require few computational resources. The reason gas is important is that it helps to ensure an appropriate fee is being paid by transactions submitted to the network. By requiring that a transaction pay for each operation it performs (or causes a contract to perform), we ensure that network doesn't become bogged down with performing a lot of intensive work that isn't valuable to anyone. This is a different strategy than the Bitcoin transaction fee, which is based only on the size in kilobytes of a transaction. Since Ethereum allows arbitrarily complex computer code to be run, a short length of code can actually result in a lot of computational work being done. So it's important to measure the work done directly instead of just choosing a fee based on the length of a transaction or contract.

Fig. 5.7 shows a simplified notion of two states in Ethereum "trust machine". Smart contracts have their local state, which is also recorded in the underlying blockchain and the system as a whole has a global state on which all other smart contracts rely upon.

Smart Contracts — the Code on the Machine

A Smart Contract is a contractual agreement that is implemented using software. Unlike a traditional

$\mathcal{F}_{\text{bitcoin}}$: a global ledger

```
Transfer: On receive ("transfer", $amt, R) from S,
          Notify adversary A of event
          Assert ledger[S] >= $amt
          ledger[S] := ledger[S] – $amt
          ledger[R] := ledger[R] + $amt

        /* all internal states exposed */
```

Fig. 5.6: Change of state upon incovation of Transfer function

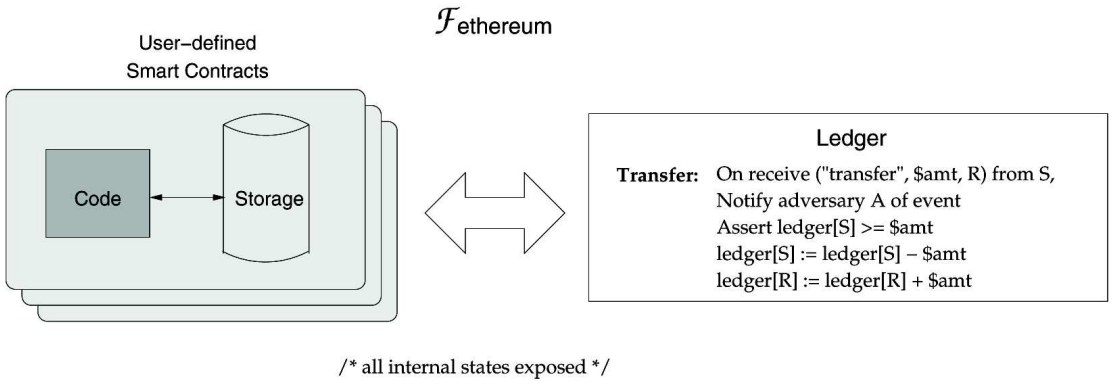

Fig. 5.7: Ethereum Trust Machine: local and global state interaction

contract where parties may seek remedial action through the legal system, a smart contract is self-enforced (possibly also self-executed), depending on whether specific conditions, that are monitored through software, are met. Smart contracts may provide several benefits, for instance:

- automatically enforce power equality of all parties involved,
- protect an individual's rights by enforcing reasonable expectations for the signee,
- eliminate the possibility of any signatory defaulting on their obligations.

Most financial instruments are essentially contracts between two or more parties with a set of rules or dependencies agreed upon by them. In regulated markets, authorities monitor the compliance of the contract/instrument to the rules-set. What if we could back these contract clauses with cryptographic guarantees? Oracles [Buterin, 2013], in this case, can act as the authority that determines compliance and adherence to the rules set — done objectively, transparently and without trust between contractual parties.

Like Bitcoin, Ethereum uses a blockchain that has its own currency, called *ethers*. Unlike Bitcoin, Ethereum uses transactions that are miniprograms, called smart contracts, that can be written with an unlimited amount of complexity. Users can then interact with programs by sending them transactions loaded with instructions, which miners then process. In practice, this means that anyone can embed a software program into a transaction and know that it will remain there, unaltered and accessible for the life span of the blockchain.

In other words, a smart contract is an event driven program, with state, which runs on a distributed, shared ledger and which can take custody of assets on that ledger [Weber *et al*., 2016]. An abstract smart contract model under Ethereum has:

1. Shared public ledger
2. Replicated states (smart contracts)
3. Cryptocurrency as reward for contract execution
4. Contracts that involve financial gains or losses
5. Event driven execution flow
6. Consensus (smart contract state change and recording in global ledger)
7. Participants are not trusted (can read contract before execution)
8. Inter-dependent contracts communicating via the global ledger

Business processes vying for efficiency, transparency, reliability of actions and deliverables upon fulfilling a task are exploring this space. In our globalized economy, almost all workflows span across boundaries of disparate collaborating organizations. The whole workflow loses its efficiency if any of the participating entity acts maliciously or does not perform as expected. It causes litigation and have cascading effects on other organizations. The logic of existing business processes/workflows can be

captured and automated through smart contracts and the underlying "trust machine" keeps track of state changes for continuous auditable visibility of the workflow for all users of the machine.

Smart contracts promise to change the economy more than any other feature of the blockchain. They could take over most routine business processes. Some companies could be no more than a bundle of smart contracts, forming true virtual firms that live only on a blockchain [Economist, 2017]. DAO (decentralized autonomous organization) is an example of formation of such virtual venture-capital fund where stakes in the firm can be purchased using ether. ICOs (initial coin offerings) is yet another simpler version of such structures of automated crowd-funding for startups whose functionality is publicized as a whitepaper or prospectus for investors in the form of smart contracts. Investors can then send ether to the smart contract, which automatically creates "tokens" that can be traded like shares.

DAOs and ICOs are a type of permissioned or private blockchains that can be realized on permissionless Ethereum platform. There is another form of private or permissioned blockchain that can be realized using Ethereum source code in which the genesis block (zeroth block) of the realized blockchain is shared among select group of participants.

Triggers & Signals – the Interrupts to the Machine

Smart contracts are capable of taking inputs from external sources. This makes them extremely useful in addressing and integrating external data sets and proprietary business interfaces that cannot be readily ported to the trust machine either due to legacy issues or privacy concerns. Programmers have to be aware of the fact that each action listed in the code of a smart contract has an associated execution cost. If all of the business logic is as it is imported into the smart contract the gas cost of running the contract increases. Smart contracts should be used as special code snippets of business logic that are critical in communicating state change in the workflow to all other stakeholders in a verifiable, non-repudiable fashion. Non-critical part of the business logic should be off-loaded from the blockchain to reduce the cost of running a smart contract on the "trust machine".

The shared global ledger among the participants acts as a shared communication bus from/to which each participant receives/sends triggers to others via recording a local state change. Fig. 5.8 depicts the inter-contract communication using shared ledger. Special smart contracts can be written that specifically act as triggers to other contracts by capturing events in the environment in which they are deployed [Weber *et al*., 2016]. For example, a stock price tracking contract can trigger a sell/buy contract automatically. In [Azaria *et al*., 2016], smart contracts on blockchain are used to specify access control policies for medical records of patients. Actual medical records are stored in an encrypted fashion off-blockchain to reduce cost, latency and for privacy preservation. Whereas who can access the data and the keys to decipher are delivered via blockchain as "signals" to the legacy database systems holding actual medical records.

Ability of smart contracts to integrate traditional IT system interfaces into the "trust machine" has brought benefits of automation, efficiency, integrity, continuous auditability, transparency, optimization, etc. to traditional IT systems. IoTs can pave way for similar impact on cyber-physical systems like physical

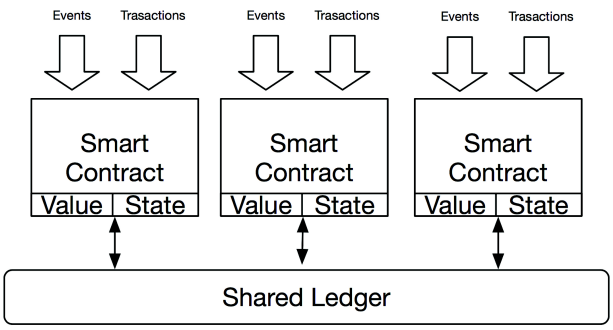

Fig. 5.8: Ethereum Inter-Contract Communication

assets (vehicles, houses, smart-grid) by facilitating the trigger & signaling interface to the "trust machine".

IoT – The Peripherals of the Machine

The advances in networking protocols and miniature, power-efficient computational chips have made our ambience intelligent and interactive through IoTs. Current deployments (c.f. Fig. 5.9) are cloud-centric [Purueswaran and Brody, 2015] and derive their intelligence from cloud, which is by design privacy invasive. This is largely because of lack of alternatives to deploy and manage IoTs in a naturally ambient

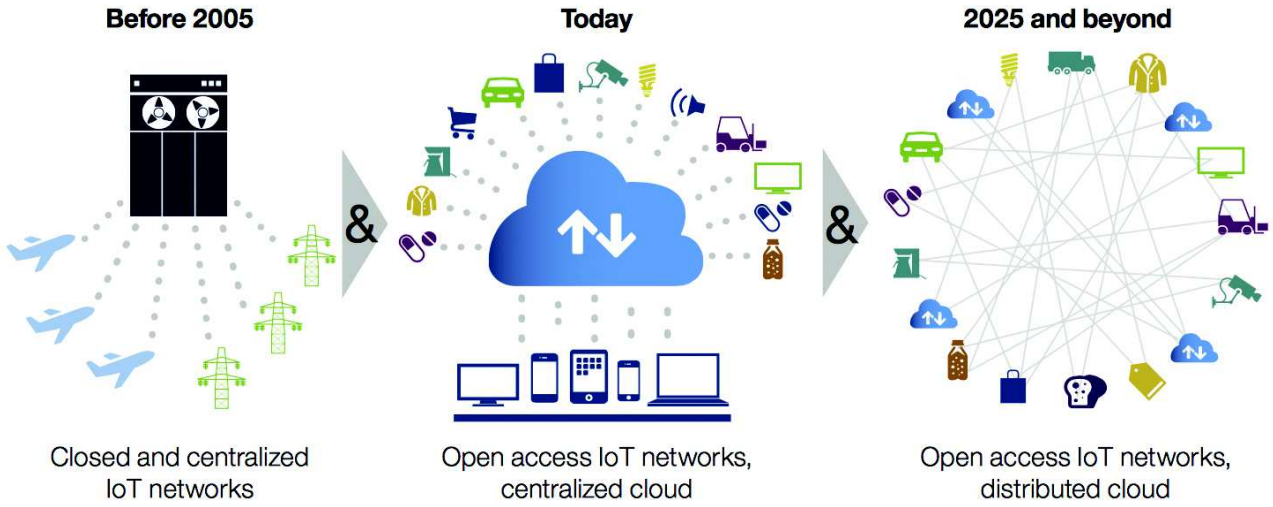

Fig. 5.9: IoT progressing towards decentralization [Pureswaran and Brody, 2015]

fashion. The potential of disruption because of this technology alone is summarized in Fig. 5.10 by IBM [Purueswaran and Brody, 2015].

The sort of programmability Ethereum offers does not just allow people's property to be tracked and registered. It allows it to be re-engineered in new ways. Imagine a digitized car-key (password that is needed to start the engine) embedded in the Ethereum blockchain could be sold or rented out in all manner of rule-based ways — enabling new P2P schemes for renting or sharing cars (bypassing TTPs like Avis, Hertz.) Imagining further, smart contract enabled self-driving cars can be self-owning [Economist, 2015 a]. Such vehicles could stash away some of the digital money they earn from renting out their keys to pay for fuel, repairs and parking spaces; all according to preprogrammed rules as smart contracts, where IoTs are acting as peripheral devices (interfaces to) connected to the "trust machine".

With respect to the future of IoT, as highlighted in [Purueswaran and Brody, 2015], blockchain is a suitable platform for facilitating transaction processing and coordination among interacting devices. Each managing its own role and behavior, resulting in an "Internet of Decentralized, Autonomous Things" — and thus the democratization of the digital world and cutting the cloud's disproportionate control over ubiquitous, autonomic computing. As a consequence, plausibly reigning back privacy; since IoTs are going to be the most ingrained computational sensors in our immediate surroundings in near future.

Applications of the Trust Machine

Blockchains are clunky databases, so why would you want to use one? Traditional systems have inherent flaws that make them easy targets for corruption of data either by technical error or by human intention. When financial firms do business with each other, the hard work of synchronizing their internal ledgers can take several days, which ties up capital and increases risk. All sorts of companies and public bodies suffer from hard-to-maintain and often incompatible databases and the high transaction costs of getting them to talk to each other. Distributed ledgers that settle transactions in minutes or seconds could go a long way to solving such problems and fulfilling the greater promise of digitization and automation with trust and transparency.

A list of efforts to solve business and social use cases is enumerated at: http://dcg.co/portfolio/. These efforts give a taste of what will be possible. Table 5.2 gives a domain-wise list of applications where the "trust machine" has a promise to play revolutionary role.

Blockchain Applicability Test

Can't computers already execute transactions based upon pre-programmed conditions? Indeed they can; however, several intermediaries are often needed to verify and validate the details of the transaction. If the intermediaries fall under a single administrative domain, they inherit trust from the same source. If the intermediaries are from disparate administrative

Vectors of disruption	Liquification of the physical world
Unlock excess capacity of physical assets	Instantly search, use and pay for available physical assets
Create liquid, transparent marketplaces	Real-time matching of supply and demand for physical goods and services
Enable radical re-pricing of credit and risk	Digitally manage risk and assess credit, virtually repossess and reduce moral hazard
Improve operational efficiency	Allow unsupervised usage of systems and devices, reduce transaction and marketing costs
Digitally integrate value chains	Enable business partners to optimize in real-time, crowdsource and collaborate

Fig. 5.10: Five vectors of disruption: How the IoT will increase our leverage of physical assets [Pureswaran and Brody, 2015]

domains and are susceptible to external breach, influence, malice, laxity, etc., then blockchain brings all domains to a common immutable ledger. Andreas M. Antonopoulos, the author of book "Mastering Bitcoin" [Antonopoulos, 2014], has coined a simple test to identify whether an application use case is really a blockchain use case or pure classical database use case. He states:

"If you replace the word Blockchain by Database and the implementation deliverables remain the same, then the use case does not require a Blockchain".

Blockchain practitioners should use this test, further elaborated in Fig. 5.11, as a guiding principle, while evaluating blockchain as a solution to the problem at hand, apart from the judicious consideration of other aspects like efficiency, integrity, non-repudiation, and potential for collusion in the proposed solution.

Challenges in Deploying the Blockchains

As blockchain applications have evolved from potential to actual use cases, we can see that particular use cases will raise specific governance questions best answered at the level of each use case (e.g., payments, contracts, securities clearance, insurance, etc.) There will not be a single blockchain but many, some of which may serve specific industries and/or geographies.

Table 5.2: Blockchain (the Trust Machine) Applications

Domain/Class	Examples
General	Escrow transactions, bonded contracts, third-party arbitration, multiparty signature transactions, messaging (Whisper), carbon credit, personal data ecosystem
Financial transaction	Remittance, trade settlement, stock, KYC/AML, private equity, crowdfunding, micro-lending, P2P lending, bonds, mutual funds, derivatives, prediction market, annuities, pensions, insurance
Businesses	Transparent and efficient workflow composition, trade settlement, shareholder agreements, continuous compliance and audit, efficient deterministic composition of services and business processes
Governance	Tendering, auctions, judiciary, regulation, agile taxation (GST), national digital currency economist-national-currency, accountability and transparency (RTI), platform for citizen engagement
Public services	Smart-grid metering, traffic congestion management, direct benefit transfer, dynamic pricing of services
Agriculture	Livestock digitization for collateral, organic food provenance, supply chain formation, community-driven shared resources (equipments, warehouses), crop insurance, targeted subsidy disbursement, soil & crop management
Public records	Land and property titles [Economist, 2015a], vehicle registrations, business licenses, marriage certificates, death certificates
Semi-public records	Degree, vocational certifications, learning outcomes, grades, HR records (salary, performance reviews, accomplishment), healthcare (performance tracking of doctors)
Private records	IOUs, loans, contracts, bets, wills, trusts, escrows, tax returns, credit score, medical records
Identification	Driver's licenses, identity cards, passports, voter registrations, federated authentication platform (Aadhaar V2)
Attestation	Proof of insurance, proof of ownership, notarization
Physical asset keys	Home (Airbnb), hotel rooms, rental cars, automobile repair access
Intangible assets	Patents, trademarks, copyrights, reservations, domain names

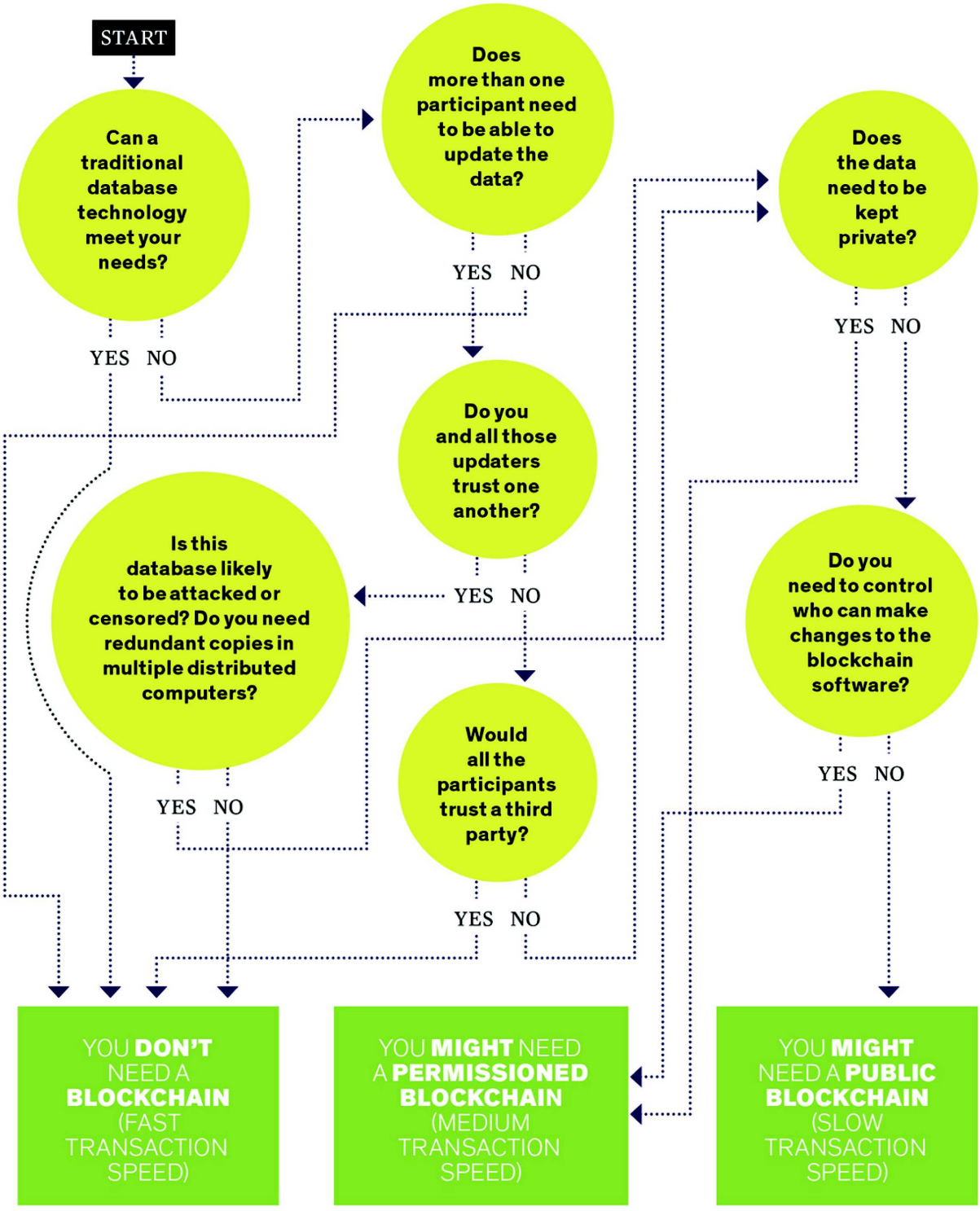

Fig. 5.11: Blockchain Applicability Test [Peck, 2017]

1. Interoperability: At the highest level, we need to focus on interoperability. Commercial blockchain applications are taking off, and governance will be critical to their success. For example, Ripple's global payments steering group, a blockchain bankers network with defined rules and governance, has been a major step forward in terms of adoption and industry acceptance. In

case of organizations from different functional domains where their collaboration is ad-hoc, a token based approach to interoperability will help [Tapscott and Tapscott, 2017].

2. Privacy: Blockchains are open ledgers where all past transactions are recorded thus posing a dilemma of constructing transactions in either a transparent way or obfuscated way. In case of smart contracts closely resembling an organizations business process flow and logic, which at times is a trade secret, the issue of privacy becomes a serious challenge. Privacy and transparency run orthogonal to each other. Deriving trust while balancing privacy and transparency will be a challenge worth addressing.

3. Regulation: Drawing up regulations for blockchains at this early stage would be a mistake: the history of peer-to-peer technology suggests that it is likely to be several years before the technology's full potential becomes clear. In the meantime regulators should stay their hands, or find ways to accommodate new approaches within existing frameworks, rather than risk stifling a fast-evolving idea with overly prescriptive rules [Economist, 2015b].

4. Testing: These technologies introduce a novel programming framework and execution environment, which are not satisfactory understood at the moment and have faced some major glitches in their nascent lifespan [Economist, 2016a, Atzei *et al*., 2017]. Multidisciplinary and multifactorial aspects affect correctness, safety, privacy, authentication, efficiency, sustainability, resilience and trust in smart contracts. Existing frameworks, which are competing for their market share, adopt different solutions to issues like the above ones. Merits of proposed solutions are still to be fully evaluated and compared by means of systematic scientific investigation, and further research is needed towards laying the foundations of Trusted Smart Contracts (http://fc17.ifca.ai/wtsc/).

5. Scalability: Industries also differ in their need for speed. For the bitcoin blockchain network, the process of clearing and settling transactions takes about 10 minutes, which is far faster end to end than most payment (e.g., remittance) mechanisms today. But clearing transactions at the point of sale instantaneously is not the issue; the real problem is that 10 minutes is simply too long for the IoT where devices need to interact continuously. Former core developer Gavin Andresen said solving for a trillion connected objects is a different design space from bitcoin, a space where low latency is more critical and fraud is less of an issue or where parties could establish an acceptable level of trust without the bitcoin network [Tapscott and Tapscott, 2016].

6. Standardization: Like Internet, blockchain is being treated as a global resource. There are already efforts underway to steward this resource for standardization on the lines of what IETF/ICANN does for the Internet. Without standardization and stewardship invisible powers could emerge.

7. Digitization of Resources: Full potential of this technology cannot be reaped unless the resources around us can interact with the digital world. In many of the developing and under-developed countries, where this technology will have the highest impact, yet do not have governmental records in digital form. Without this availability of resources in digitized form it will be extremely difficult to realize the full potential of this technology.

8. User Interface: User interface will remain as Achilles heel given the fact that even a sophisticated user finds using crypto-wallets as a daunting task.

Blockchain in Indian Context

Investments in blockchain start-ups are similar in scale to that happened for dot-coms in the 1990s. While the invention was for creating a currency, there has been a widespread belief that the underlying trust protocol lends itself for reconfiguring our institutions and economy. Though there are certainly great challenges in creating such a future for which some of the emerged principles over this short period are: (i) networked integrity, (ii) distributed power (by consensus), (iii) value as incentive, (iv) security-by-design, (v) pseudonymity, (vi) preservation of rights,

and (vii) democratic platform for inclusion with efficiency and transparency. Breakthroughs in these will lead to a great impact on building viable democratic societal applications, and a smart economy.

Sector-wise Potential

Some of the sectors that will have a positive impact of using such a technology are briefed below:

1. Policy: Management thinker Peter Drucker is often quoted as saying that "you cannot manage what you cannot measure." Drucker means that you can't know whether or not you are successful unless success is defined and tracked. What best can give a platform other than blockchain to define KPIs and triggers/conditions to track their progress in real-time?

2. Judiciary: A growing pool of empirical studies suggests that slow court systems discourage the growth of new businesses. With 2.8 crore of pending cases, blockchain's smart contract technology can be used to resolve the cases involving economic contract breaches, as a first step to experiment with. With the advances in AI (machine learning) and NLP technologies, effort can be made to resolve cases that have a clear precedent to rely on.

3. National Identity Platform: Identity is a critical part of a modern, progressive nation. Identity plays a vital role in correct identification of individuals for various purposes: for economic, public service delivery, etc. Duplication of identities without holistic view gives rise to leakages as each department/institution maintains its own database — resulting in parallel expenses for same goal. Malfeasance to such databases create situations where genuine individuals are excluded from being identified. Issues arising out of privacy violations generate resistance to evolution of a cohesive platform. Blockchain can provide a cohesive registry of identities and associated attributes that can be accessed by authorized entities under well-defined circumstances and contexts with appropriate authentication loop involving the subject being identified. Smart contracts can help improving Aadhaar framework into an intelligent, privacy-preserving national identity platform. Such a system will save cost of doing KYC for financial institutions and provide uniform view and control over data to end users.

4. Public Distribution System & DBT: Blockchain can reduce the number nodes through which a benefit/value traverses from issuer to receiver to zero. Thus the traditional intermediate nodes in value transfer to beneficiary will have the role of actuators only in which they have to just verify the validity of eligibility conditions for a beneficiary. Eligibility of a beneficiary can be evaluated in real-time instead of current periodic evaluation. Having a inter-connected national identity platform will greatly help in accurate evaluation of any beneficiary. Blockchain plays a role of a universal, all-knowing database to which any authorized entity can make a query.

5. Governance & Service Delivery: In a democratic country like India, health of the democracy is dependent on the active participation of its populace. Government spends huge amount of money on public welfare projects where the project executioner and the project auditor are exclusive of populace supposed to be the beneficiaries of or affected by the project. We can borrow the idea championed by ixo Foundation (http://ixo.foundation) to use blockchain for measuring impact of UN SDG (sustainable development goals) by making the populace as an auditor of the projects being implemented. Upon completion of execution of a project the affected people vote or provide feedback about the quality and degree of completion of the project. Thus making it difficult for the project executioner to influence or bribe the auditor.

6. Energy: With a huge potential of roof-top solar power generation, the national power grid will have to be equipped with an ability to dynamically adjust its transmission and distribution capacities. Reporting inaccurate data by error or malice can have cascading effect on the grid's stability. It will be of paramount importance to bring unified view across the grid for import/export of electricity. IoT-enabled controllers & meters with blockchain as an underlying data reporting, billing system will be

a natural fit.

7. Agriculture: In a country like ours where a large population is engaged in agriculture, any gains in matching the produce with the best market will benefit the farmers. APEDA actively assists farmers to sell their produce in foreign markets by certifying the produce. Authenticity of these certificates and time taken to issue them is critical for perishable items. Integration of blockchain in supply chain consisting of certifiers like APEDA, cold-storage chains, port authorities, shipping lines will be a game changer. Another great benefit of blockchain in this sector would be a system that digitizes immovable assets and livestock of marginal farmers who have Jan Dhan Account but no credit profile thus excluded from formal financial services. Representation of livestock, ancestral property in shared custody of undivided joint family onto a blockchain will build their credit profile for NBFCs.

This technology has great potential to transform almost all sectors fundamentally. With a proper action plan and strategy, government can nurture and promote this technology by becoming its promoter and user.

Design & Deployment Considerations

While constructing a "trust machine" for a national (governamental) initiative a few subtle decisions need to be made in line with the spirit of Bitcoin highlighted below:

1. Permissioned vs Permissionless blockchain: It is going to be a great conundrum because by relevance it has to be a permissioned blockchain at global level, whereas it has to be a permissionless blockchain at national level. Identity-cum-authentication will help segregating the users interacting with the national level blockchain. Luckily, India has a national level identification mechanism for its citizens and businesses. It will be an interesting proposition to build such a blockchain also because businesses operating out of India will have their workflow spanned across the world. How do we provide the interoperability will be an important design criteria.

2. Evoking the Trust: Being a national blockchain, either backed by the Indian government or by a consortia of public-private partnership, the obvious fact will be the ownership of the setup. Blockchain is a P2P system in its original form with no entry or exit barrier for the nodes and no ownership of the whole. Whereas, having a owner of the permissioned setup does not bode well for evoking public trust into the system. Pragmatic approach like setting up an independent statutory body similar to Election Commission of India will assuage the concern.

3. Choice of the consensus algorithm: PoW is the only proven practical consensus algorithm that scales for a large number of nodes, as seen in case of Bitcoin. PoS of Ethereum is bootstrapped from PoW in the beginning to denote generated currency units as "Stake" or Ether. Choosing PoW type of consensus algorithm has to be extremely careful while making the choice of one way hash function to perform actual PoW construction. Bitcoin miners have reached to such gigantic levels of hashing power that the biggest miner on Bitcoin can easily overwhelm combined power of all supercomputers in the world put together. A different hash function has to be chosen while keeping in mind the sophistication of existing Bitcoin miners for SHA family of hash functions. PoS without PoW for bootstrapping could be a good option since the national blockchain will have option of using Aadhaar-unique-IDs to offer a pre-determined stake to each individual a priori.

Takeaways

Bitcoin is the first application of a technology that paves the way forward, revealing an opportunity for innovation that was not apparent before. Bitcoin is wholly open source (an important trust evoking aspect), so every element of it can be tweaked, modified, altered and tested for potentially improved iterations, just like evolution.

1. Blockchain is an idea of making trust a matter of coding, rather than of democratic politics, legitimacy and accountability. The blockchain lets people, who have no particular confidence in each other, collaborate without having to go

through a neutral central authority. Simply put, it is a machine for creating trust. In essence it is a shared, trusted, public ledger that everyone can inspect, but which no single user controls.

2. Ledgers that no longer need to be maintained by a company or a government may in time spur new changes in how companies and governments work, in what is expected of them and in what can be done without them.

3. A realization that systems without centralized record-keeping can be just as trustworthy as those that have them may bring radical change.

4. People and institutions today can solve hard problems and change the world for the better when they have a reliable framework to build on.

5. Systems that are honest free up dead capital. The transparency provided by blockchain can help eliminate forgery and provide efficient service delivery.

6. Blockchain is an important technology of Internet era and has global appeal. Any nation embracing this technology (e.g., Estonia, Singapore, Japan) will have a competitive advantage over the laggards. Industry (through innovation) as well as government (through calculated policy oversight, being promoter of common standards for interoperability) have a responsibility to invest in this potentially revolutionary technology for trust management in our digital economy.

"One reason why this technology works is that it has socially engineered the game mechanics based on one assumption, that there are more good people than bad people. This is the underlying hope on which blockchain resides". — Pindar Wong, VeriFi.

References

Ali M, Nelson J, Shea R and Freedman M J (2016) Blockstack: A global naming and storage system secured by blockchains. In *Proceedings of the 2016 USENIX Conference on Usenix Annual Technical Conference*, USENIX ATC '16, pages 181-194. USENIX Association

Antonopoulos A M (2014) *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, Inc., 1st edition

Atzei N, Bartoletti M and Cimoli T (2017) A survey of attacks on ethereum smart contracts SoK. In *Proceedings of the 6th International Conference on Principles of Security and Trust - Volume 10204*, pages 164-186, New York, NY, USA. Springer-Verlag New York, Inc

Azaria A, Ekblaw A, Vieira T and Lipprnari A (2016) Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25-30

Backs A (August 2002) Hashcash - A Denial of Service Counter-Measure. http://www.hashcash.org/papers/hashcash.pdf. Technical Report

Baird L (2016) The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance. http://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf. SWIRLDS Tech Report

Buterin V (2013) Ethereum: A next-generation smart contract and decentralized application platform, https://github.com/ethereum/wiki/wiki/White-Paper

Castro M and Liskov B (1999) Practical byzantine fault tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, OSDI '99, pages 173-186. USENIX Association

Chaum D, Fiat A and Naor M (1988) Untraceable electronic cash. In *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, 1988, Proceedings*, pages 319-327

Dwork C and Naor M (1993) *Pricing via Processing or Combatting Junk Mail*, pages 139-147. Springer Berlin Heidelberg

Economist T (Jul 2016a) Not-so-clever contracts. The Economist

Economist T (Jul 2017) Disrupting the trust business. The Economist

Economist T (Mar 2016b) Redistributed ledger. The Economist

Economist T (Oct 2015a) The great chain of being sure about things. The Economist

Economist T (Oct 2015b) The trust machine. The Economist

Force A C T (April 2016) Financial regulations for improving financial inclusion, https://www.cgdev.org/sites/default/files/financial-access-task-force-brief_0.pdf

Lamport L, Shostak R and Pease M (1982) The byzantine generals problem. *ACM Trans Program Lang Syst* **4** 382-401

Micali S (2016) ALGORAND: The efficient and democratic ledger. *CoRR*, abs/1607.01341

Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf

RBI (2015) Financial inclusion in India - an assessment. https://rbidocs.rbi.org.in/rdocs/Speeches/PDFs/MFI101213FS.pdf

Ongaro D and Ousterhout J (2014) In search of an understandable consensus algorithm. In *Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference*, USENIX ATC'14, pages 305-320. USENIX Association

Patil V T and Shyamasundar R K (2017) Privacy as a currency: Un-regulated? In *Proceedings of the 14th International Conference on Security and Cryptography: SECRYPT*, pages 586-595. INSTICC, SciTePress

Peck M E (2017) Blockchain world - do you need a blockchain? this chart will tell you if the technology can solve your problem. *IEEE Spectrum* **54** 38-60

Pitroda S and Desai M (2010) *The March of Mobile Money: The Future of Lifestyle Management.* Harper Collins Publisher, Colliris Business

Pureswaran V and Brody P (2015) Device democracy: Saving the future of the internet of things. http://www-935.ibm.com/services/multimedia/GBE03620USEN.pdf. IBM Institute for Business Value

Snow P, Deery B, Lu J, Jolmston D and Kirby P (Nov 2014) Business processes secured by immutable audit trails on the blockchain. Factom White Paper

Swan M (2015) *Blockchain: Blueprint for a New Economy.* O'Reilly Media, Inc., 1st edition

Tapscott D and Tapscott A (2016) *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* Portfolio Penguin

Tapscott D and Tapscott A (June 2017) Realizing the potential of blockchain: A multistakeholder approach to the stewardship of blockchain and cryptocurrencies, World Economic Forum

Vigna P and Casey M J (2016) *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order.* St. Martin's Press

Vukolić M (2016) *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*, pages 112-125. Springer International Publishing, Cham

Weber I, Xu X, Riveret R, Governatori G, Ponomarev A and Mendling J (2016) *Untrusted Business Process Monitoring and Execution Using Blockchain*, pages 329-347. Springer International Publishing, Cham

Wood G (2014) Ethereum: A secure decentralised generalised transaction ledger, http://gavwood.com/paper.pdf.