More than Money

Get the gist on bitcoins, blockchains, & smart contracts

April 2016 Foresight Gist brought to you by:

SHAPING TOMORROW

MAKING BETTER DECISIONS TODAY

Edited by Dennis D. Draeger

Table of Contents

Preface

What is a Gist report?

Gist reports provide a brief overview of the current and future status of each topic and are intended to help readers quickly and conveniently appraise the future of an issue. Each 5 to 10-page Gist report includes an introduction to the topic, a literature review using our auto-extracted Forecasts, and our own method of analysis. The Gists quickly and conveniently get every team member on the same page so that meetings may be conducted more efficiently and with deeper insight. The Gists then become a launching pad for organizations to develop their own analysis and strategy.

A Gist report tells only part of the story. If you wish to explore the potential of these technologies in greater detail for your industry, please contact us for a more comprehensive product. To see a brief description of other issues such as the futures of work, cities, energy, Asia, and more; please see our other Gists and options for ordering custom Gists specific for your organization. To see a full list of our Forecasts, please register for our service and enjoy our weekly newsletter.

Methodology

Shaping Tomorrow's system is able to add sources to it database automatically depending on the sources and key search terms specified by Shaping Tomorrow's users. The system then auto-extracts any forecasts from the sources. As users search these Forecasts, the system can summarize the Forecasts to simplify their research. Shaping Tomorrow has extracted more than 105,000 Forecasts (one-sentence, future relevant statements) out of Shaping Tomorrow's 125,000+ Insights (sources). Shaping Tomorrow offers clients the service of searching these Forecasts at their convenience giving clients greater flexibility for strategy development. The Forecasts used for this Gist were summarized to indicate the future of cryptocurrencies, blockchains, and smart contracts. The Forecasts were then paraphrased and edited for reader convenience. An introduction was then added to clarify terms, explain the current changes in the market, and pinpoint the implications. A brief baseline scenario is also provided to add perspective for how the technology could evolve long term. The report ends with strategic questions, also automatically extracted by Shaping Tomorrow, to give insight for the questions already being discussed online.

Introduction

Proponents say Bitcoin will decentralize power away from banks and other institutions while distributing it across whole communities. If these promises hold true, Bitcoin will only be the beginning. Bitcoin's related technologies, the blockchain (also known as a distributed ledger) and smart contracts, are primed to move beyond money to other real world applications. Eventually, these technologies could move automation straight up the corporate ladder to the executive level, making even CEOs redundant, with similar far future implications for public organizations.

In many ways these technologies are similar to the internet in the early 90s. They are too complicated for average consumers to understand, but developers and investors are flooding them with resources. Average consumers fail to understand how Bitcoin or any other virtual currency can be successful without any physical representation of the currency's value, but banks handled $410 trillion (more than 5 times global GDP) in non-cash transactions in 2013. The following year in 2014, the banks earned $1.1 trillion of revenue from these non-cash transactions.

More concerning is the amount of money lost through bank fraud each year. In 2013, a total of $9 billion was lost just in card-not-present transactions which are performed via online hacks, telephone scams, or mail order cons. The total is expected to reach $19 billion by 2018. Many banks, 62% of those surveyed by Bank Info Security in 2014, say they often do not know about fraud until their customers inform them.

Cryptocurrency, blockchain and smart contract proponents promise that these technologies will offer more secure, more efficient, and less expensive services for financial transactions. If these technologies can reduce bank fraud, perhaps they can eventually protect against voter fraud, simplify medical record management, increase electric grid efficiency, and much more than just money.

Clarifying Terms

What are bitcoins and cryptocurrencies? Bitcoin has been a growing phenomenon since it was released as open source software in 2009. It is the most successful example to date of digital currency (virtual money which can be used to purchase physical goods such as real estate) and the first cryptocurrency (money that relies on encryption instead of the processes of central banks for creation and transferal). However, Bitcoin is not the only cryptocurrency, and several similar communities are popping up.

No cryptocurrency is currently backed by any centralized institution, and they are generated and governed electronically using algorithms that solve mathematical equations. They are controlled by a distributed community which anyone is capable of joining, and cryptocurrencies are produced electronically by individuals and businesses all over the world. The computer systems required for creating and validating them are growing ever more expensive even as the value of cryptocurrencies fluctuate.

What is a blockchain? It is a public database of transactions that is similar to an Excel spreadsheet, but it is not owned or monitored by any single individual or organization. The ownership is instead distributed to the decentralized members of a disparate community (Bitcoin or otherwise).

Although Bitcoin's blockchain can be anonymous regarding the real world people using an account, the account itself is public. A private key is assigned to the user of each unique account to allow for increased security over passwords. The most important part is that the blockchain is capable of securely identifying the online persona of the account holder operating it with the private key. Once the real world individual connects their real life identity via a credit card, fingerprint, or other unique identifier; the blockchain can securely identify who is using it. However, that means the anonymous nature that many value in the technology is then lost.

The blockchain also adds another level of security that many other online technologies do not have, consensus and permanence. The blockchain's community must provide a majority consensus on every transaction and any other changes made on the blockchain. Since every update to the blockchain is incapable of being deleted, the blockchain allows for audits to be completed with increased trust.

What are smart contracts? They are codes that allow an exchange once pre-set conditions are met (i.e. if this happens, then that happens). Smart contracts are largely what is driving the internet of things. If a homeowner's car is within 10km of home, then the lights turn on and the heating/ air conditioning is optimized. However, smart contracts can also act based on information provided in a blockchain to automate tasks.

The blockchain enables real world data management to function more like a computer with the automation of tedious tasks such as processing payments. If a borrower's monthly payment adds up to the total of the mortgage, then the borrower is automatically registered as the full owner of the house. Smart contracts can automate escrow processes. If a bet is made, then the money is held by a third party account which the smart contract accesses to pay the winner. Derivatives and insurance are therefore obvious applications for automation via smart contracts.

What is a Decentralized Autonomous Organization (DAO)? As the distributed model that the blockchain offers combines with the automation of smart contracts and other technologies, organizations may be capable of automating their operations and distributing their governance. Even if the centralized company dissolves, the service would remain and function as normal since all of the systems and processes are distributed and autonomous. A sole proprietor could more easily run a multimillion dollar service.

What is Changing?

Financial institutions are investing in the blockchain to make their job easier and more secure. R3 CEV is a company specifically set up to help banks trial blockchain technology. They lead a consortium of 42 banks who want to see how blockchain technology could change their industry, the potential of which R3 compares to how the internet changed the music and media industries.

The Z/Yen Group researched blockchain technology and its potential effects for the insurance industry. They expressed a number of concerns especially over government regulations as well as mining decentralization and scalability. However, they think the positives outweigh the negatives saying that blockchain technology would improve both integrity and security which are essential for financial services.

Slock.it is attempting to be the first real world Decentralized Autonomous Organization (DAO). Slock.it's service connects the internet of things to the sharing economy via the blockchain and smart contracts. Once a user pays to rent a bicycle or house or any other property, the physical lock on the property is automatically unlocked and ready for use without any middleman such as Uber or Airbnb. Front door deadbolts, padlocks, and car doors are all capable of being connected to the internet and controlled by smart contracts.

However, the blockchain could be useful for so much more than just financial transactions. Ubitquity has developed a blockchain platform specifically for the real estate industry. The company says the new platform will improve the title transfer process by making it faster, more accurate, and more transparent for fraud prevention. And they say it will improve the due diligence process for the industry.

Governments are also exploring the benefits of blockchain and smart contracts. Honduras has long had to contend with fraud from bureaucrats exploiting hacks in the system to acquire beachfront property, but the Central American nation is considering a real estate blockchain similar to Ubitquity. The UK government is looking at blockchain to improve the transparency and accuracy of its record keeping. The Isle of Man is trialling a technical experiment, the first government agency anywhere to attempt such work. China has partnered with Factom to apply blockchain and smart contracts to their smart cities initiative.

Going a step further, the self-proclaimed micronation of Liberland in the Balkans is in talks with Pax, a blockchain based "virtual nation" of volunteer citizens upholding its laws. Pax is a peer-to-peer legal system that some believe will change the way society thinks about government and potentially decentralize and distribute many government services around the globe.

Multiple organizations are working to use blockchain tech to make voting more secure, and anonymous. In 2014 a major political party in Denmark, the Liberal Alliance, used blockchain tech for its own internal party voting. Since the blockchain relies on consensus anyway, it is inherently a voting platform and could one day be modified by government entities for such purpose.

Implications

Bitcoin and other cryptocurrencies offer a libertarian ideal that could destabilize the current infrastructure of banks and other powerful institutions. The blockchain offers distributed, secure, trusted and highly scalable architectures that conventional technologies cannot compete with. Although the banking industry is pre-empting disruption by investing in this new technology, many of their business models and revenue streams will be affected especially with increased competition from the tech industry. The opportunity for the financial industry is high, but the potential risks are also large especially for smaller players in the industry.

Since computers are now able to process payments, other contractual exchanges could be carried out automatically via smart contracts. Currently if an online store receives a payment, then the product is delivered, but humans are still involved in the process. Blockchains and smart contracts could entirely automate the processing especially as logistic automation systems improve with robots packing and shipping products eventually via a driverless vehicle.

In the public sector, digital voting has been a long held dream for decades, but the blockchain may hold the key to its eventual success if the anonymity can be maintained along with some aspect of verifying that only individuals are voting (i.e. no double votes are made). This could be achieved in a number of ways using tangible rather than digital methods such as providing each citizen with an encrypted key that they must protect like their unique identifying numbers (e.g. credit card number, US Social Security number, voter registration number).

For many digital voting advocates, the ultimate purpose is "liquid democracy". They want citizens to be able to vote on everything they wish, or citizens could allow their vote to be made by someone they feel is better qualified.

Another application for the public sector is the potential for automating the allocation of a small amount of funds based on very specific parameters. So if an earthquake of a certain magnitude were detected in a given area, the emergency relief agency could automatically allocate a small amount of funds to certain organizations in the area. Regardless of the amount, these funds could provide immediate help for the community when it is needed most even as the government agency scrambles to respond more effectively to the emergency.

Cultural Lag

Every new technology experiences an early dichotomy period where proponents see idealistic visions of the future while its detractors either mock its abilities or highlight its negative aspects. With Bitcoin, both have already happened and are beginning to wane. Just a couple of years ago, the press was focused on Bitcoin's uses by the black market—bitcoins paying for guns, drugs, etc.—due to the difficulty in positively identifying the buyer or seller in illegal transactions. Although the black market connection continues to be a concern, it is no less a concern with bitcoins than it is for cash.

Around the same time, economists were quick to point out various technical weaknesses in the Bitcoin system, and they predicted Bitcoin would never succeed as a currency. These economists completely missed the point of Bitcoin which is less about beating out any currencies and more about funding research and development in innovations that could spur the economy. Bitcoin has much to prove as a currency, but it has clearly shown its ability to succeed in the market despite a few technical issues which are being resolved by its online community.

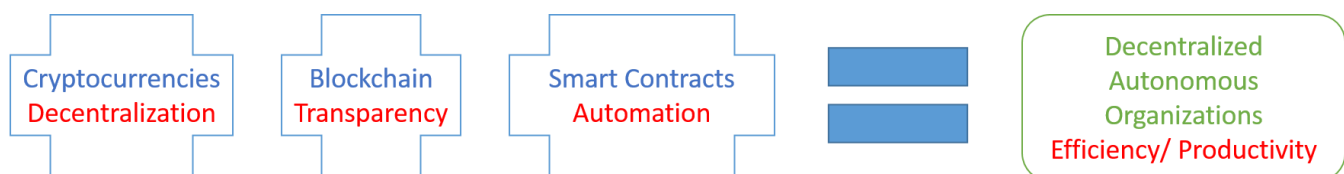| Cryptocurrencies
Decentralization | Blockchain
Transparency | Smart Contracts
Automation | | Decentralized Autonomous Organizations
Efficiency/ Productivity |

Figure 1 The basic benefits of the blockchain and its related technologies as proposed by techno-optimists

At the moment, mainstream businesses and media are more interested in the potential of the blockchain and smart contracts than the idea of a virtual currency like Bitcoin. The most likely scenario is that these technologies will be tamed by regulations just as the internet has over the course of the past 25 years. The key question in that case surrounds: what paradigms will shift in the meantime, and which sectors will be disrupted as they scramble to keep up?

To that end, techno-optimists foresee a future of rampant decentralization and democratization, and they foresee that whole firms will become completely autonomous. Not only will automation

cause lower level employees to lose their jobs, but DAOs will jeopardize the positions of the C-suite, management, and various government employees as well. Multi-million dollar services could operate by a small group of owners—who might eventually make themselves redundant—with a distributed community of users and developers.

Forecasts

As described in the Preface, below are auto-summarized lists of auto-extracted Forecasts for cryptocurrencies, blockchains, and smart contracts. They are numbered for easy reference, and each forecast is hyperlinked to its source to access more research.

Cryptocurrencies

1. By 2027, 10% of global GDP will be stored on a blockchain network.
2. Multiple bitcoin and blockchain companies will raise $100m rounds and reach $1bn valuations next year (2016).
3. Several studies indicate that in the next four years the global market for digital transactions will reach $9.5 billion while global blockchain technology investments will reach $300 billion.
4. Micropayments are expected to reach $13 billion over the next three years as cryptocurrencies gain greater acceptance.
5. Decentralized payments technologies could transform the "business architecture" for money transfers.
6. Blockchain could eventually cut costs for financial services such as credit cards, remittances and money transfers.
7. Bitcoin technology could potentially be as disruptive as the internet itself.
8. A system like this could transform the way people consume media online and enable content creators to receive payment directly on a pay-per-use basis.
9. Brand equity in the industry will likely flow from partnerships with others in the ecosystem as banks play catch up with super-consumer brands such as Google and Apple.
10. Reliance on third parties for noncore infrastructure and talent will be a common phenomenon as banks become increasingly connected via a complex network or web of vendors and third parties.
11. The widespread use of bitcoin technology in finance could end up sucking deposits away from commercial banks and hitting lending in the real economy.
12. The settlement technology behind digital currencies could become a parallel form of distributing funds and making financial transactions with the Bank acting as a backstop.
13. The Bank of England (BoE) could become the hub of a bitcoin-style digital currency that side-lines high-street banks and cuts the costs of financial transactions.
14. African banks could actually become pioneers in developing new financial technologies like the blockchain and bitcoin.
15. The Open Banking API Standard could revolutionize how consumers manage their finances.
16. Cryptocurrencies distributed through competitive mining involve no investment of money or potential loss of a "purchase" and provide limited opportunity for profit to developers.
17. Bringing the option of receiving blockchain payments to Vietnamese merchants will dramatically improve the lack of trust and security which are swirling around legacy payment options like credit cards, PayPal and similar offerings.

18. Hundreds of millions of users will be sending money on the internet as easily as they send chats.

Legal Ramifications

19. Code will be the new financial law.
20. A US court will tackle the issue of the application of the Fifth Amendment to bitcoin private keys in a case that undoubtedly will be closely watched.
21. Bitcoin exchanges will have to comply with tougher anti-money laundering (AML) regulations.
22. Regulators will benefit from an improved audit trail and will be able to see activity in the market in near real time.
23. There seems to be a risk that virtual currencies may be used by terrorist organizations to conceal financial transactions.
24. Decentralized cryptocurrencies like Bitcoin do not readily fit the definition of a security and do not present risks generally addressed by securities regulation.
25. The IMF is worried about the fact that virtual currencies like bitcoin have potential risks that make money laundering, terrorist financing, tax evasion and fraud easier to execute.
26. Users are not guaranteed anonymity and if they want to convert their bitcoins into pounds, dollars or euros then the exchange systems are expected to enforce relevant regulations regarding identity, money laundering and terrorist financing.
27. Blockchain will help to nail money launderers and fraudsters through its distributed ledger and the historic traceability of funds.

Blockchain

28. Blockchain will evolve from something banks are suspicious of to "the" disruptive technology that will totally transform the banking system.
29. Blockchain-related savings could have pushed up the investment banking industry's 2015 return on equity, excluding exceptionals, to 10.4 percent.
30. The current interest and investment in blockchain tech among financial firms will reveal its impact in just 12 to 18 months.
31. Work on blockchain applications will benefit from an accelerating pace of overall tech adoption that will soon put pressure on existing legacy financial solutions.
32. Blockchains could be a universal transaction system on an order never before imagined that could possibly be used to coordinate the whole of human and machine activity.
33. Blockchain will do to corporate reporting and financial transactions what the internet did for knowledge.
34. Business owners truly dedicated to cost reduction and functionality expansion will be imaginative enough to find ways to implement blockchain technology in their supply chains, payments processing and other processes.
35. The use of distributed ledger technology will achieve better data efficiencies and improve transaction processing and settlement.
36. Best practices for distributed ledger technology [for record keeping] will certainly emerge and create even more applications of the concept.
37. Employee identity management for large multinational corporations or access to patient healthcare records could utilize blockchains to eliminate redundancies and false entries to the

data and offer layered information access points to third parties without compromising information security.

38. Blockchain could be the most significant social and political innovation to impact Africa in 100 years.

39. McKinsey sees great promise in blockchain for capital markets but cautions that market participants, regulators and technology companies will have to cooperate in order to make it work.

Smart Contracts

40. A digital will or testament can automatically trigger the contract execution in favor of a primary beneficiary.

41. Highly shared smart contracts could be recognized as key infrastructure components and be formally owned and managed by some form of open software foundation (OSF).

42. The technology behind the Bitcoin digital currency could usher in an era of 'smart contracts' and enable the creation of a tamper-proof Land Registry database.

43. Carriers that are slow to integrate Internet of Things data sources into their underwriting and pricing models risk adverse selection which could put pressure on their margins.

44. Expectations are that the new FLEX options will provide insurers with an alternative hedging method in an exchange-traded environment where transparency, price discovery, and centralized clearing are attractive differentiators.

45. With increasing automation and faster clearing and settlement cycles, markets will become more efficient, and differentiation hard to find, but the role of human insight and strategic advice will become even more important in serving clients and building algorithms.

Distributed Autonomous Organizations (DAO)

46. In financial markets, one clear application of blockchain technology is algorithmic trading and back office operations. High-frequency trading could be taken to the next level implemented in smart contract DACs (decentralized autonomous corporations) and executed by semiautonomous agents with the ability to act more quickly and better crawl information sources for price, news, and sentiment changes. Similarly, whole tiers of back-office operations like clearing currently handled by people-agents could be handled by blockchain-agents.

47. Cryptographic ledgers could coordinate spot transactions (cryptocurrency) and t+n interactions with smart contracts and autonomous dapp (decentralized app), DAO, DAC (decentralized autonomous corporations).

48. Citizens could make political decisions through transparent digital processes and interfaces set up around a DAO.

49. Citizens could actually become shareholders in their local government.

50. Autonomous agents, smart programs, and (later) increased levels of artificial intelligence and AI algorithms will provide self-sustainability in operations and value creation at the centers, edges and arteries of an organization.

51. The idea of a rigid organisation or corporation will evaporate and left will be the true essence of human interaction patterns.

52. Markets and marketplaces created or maintained by decentralized autonomous organizations will not readily allow for government intervention. Forcing software developers to introduce a

particular feature into the code will only work to the extent that the userbase actually agrees to switch to the new protocol.

Security Concerns (Quantum)

The extent to which the blockchain is secure is still being examined and debated, but nothing can be 100% secure especially when money is involved. One weakness that some researchers foresee is quantum computing.

53. Quantum computing could be used in hashing.
54. Quantum computing will create issues for cryptocurrency and cryptography in general that will need to be addressed going forward.
55. The security of elliptic curve cryptography systems could be jeopardized due to the fact that a quantum computer could deduce the private key of an address if it knows the public key.

Idyllic Scenario

The techno-optimists' scenario for the blockchain and smart contracts spells out a future where money becomes a latent feature of human interaction as opposed to a dominant feature as it is today. As other issues (such as guaranteed basic income, Internet of Things, etc.) mature and converge, applications for blockchain and smart contracts will expand to underlay almost every aspects of digital life.

Guaranteed basic income has been gaining traction in several countries around the world especially as automation continues to develop. If value can be guaranteed and automated as Figure 1 suggests, then money will become obsolete and the digital world may rely more on a type of digital bartering system determined more by a reputation economy than money. And as the Internet of Things advances, a similar reputation system may influence

Figure 2 Fiat money has no more intrinsic value than virtual currency, and fiat money's value is all the more abstruse now in the age of digital communications. The internet has distributed information beyond any centralized or decentralized silos such as libraries, and blockchain and related technologies promise to do the same for value. Whether the value refers to currency or votes—as a currency for the public sector—or some other form of value, the blockchain could make that value more transparent and more secure while engendering greater trust for any system or process to which it is applied.

even real world transactions.

- If a person's milk supply runs dry, their fridge can order a new litre of milk to be delivered once they finish an online survey.
- When a wealthy person's fingerprints are recognized by a store's door, the price for everything increases.
- If public surveillance ramps up, a kind act could be registered by someone's wearable camera, and a reward (tickets to a concert that the individual expressed interest for on Facebook) could be automatically allocated to the individual out of a philanthropic fund that is no longer monitored by humans.
- If someone's death is recorded at a hospital, emails are sent to pre-set loved ones with messages of love, videos, photos, etc.

All of these scenarios are entirely plausible now, but with the blockchain, the process could become automated, standardized, and nearly universal. Money and other values could become hidden in the digital architecture as soon as 20 years from now. While a virtual currency would continue to exist, value exchange at every level would become more latent than is possible today.

Strategic Questions

The following questions were auto-extracted by Shaping Tomorrow's system the same way the Forecasts were, and like the Forecasts each question includes a hyperlink to its source. Some of the sources will supply an answer to the question, but some will not. These questions represent some of the issues surrounding cryptocurrencies, blockchains, and smart contracts. Answer them as best you can for your own organization before clicking the links to deepen your understanding.

Cryptocurrencies

- What might push blockchain and cryptocurrencies in general, into the mainstream?
- What new features should be in cryptocurrency in order for it to succeed?
- What do you think will happen to Bitcoin when the next big recession hits?
- Is this about substituting bitcoin or some other virtual currency for the U.S. dollar [as the dominant currency standard]?
- Why is bitcoin adoption slow among the unbanked billions?
- How do we exchange different currencies or other financial instruments between blockchains denominated in different currencies?

Blockchain

- How will the constructs and systems created to handle civil litigation adapt to bitcoin and the blockchain?
- What happens when blockchain startups stop worrying about regulatory compliance and start intersecting with existing "real-life" systems?
- Will the modes of future media distribution also be decentralized on the blockchain?
- How could nation-states vote on blockchain based voting systems?
- How could blockchain disrupt or transform your competitor/ supplier/ customer operations?

- How big a threat could blockchain pose to human workers whose roles can be automated away as excess "middle men"?
- Where might new sources of unexpected risk emerge in a "blockchain world" that is still in its infancy and so poorly understood by all but a small group of pioneers and enthusiasts?

Smart Contracts

- How should regulators control an automated process that happens on numerous anonymous computers?
- Who is actually in charge, responsible, or accountable for smart contract operations?
- Will these mountains of chattering smart things liberate and elevate humanity or leave us device-dependent and drowning in complexity?
- How can companies leverage automation and smart technologies to improve productivity and create more meaningful and engaging work where employees "race with—not against— machines"?

Distributed Autonomous Organizations

- If their resources cannot be seized (since DAOs have full sovereignty over them) how can they be required to pay damages?
- If you used a DAO, what clauses could you include that hedge against the uncertainty of a potentially untrustworthy party?
- Should DAOs try to maintain balances in other currencies, or should they only reward behavior by issuing their own internal token?

Next Steps

We recommend developing multiple scenarios to explore how these technologies could affect your organization both positively or negatively. Considering the rate of change over the past several years, it is best to develop each scenario on at least a 10-year time horizon since these changes may occur sooner than your organization expects.

With these scenarios, you can then build a more adaptable strategic plan that can easily adjust to the actual future that unfolds. If you need any help accomplishing this, please contact us for a solution that best fits your needs.

Other Sources

The following sources were used in the Introduction and other expository sections of the Gist report.

1. Global Payments 2015: The Interactive Edition
2. Global Payments 2014: Capturing the Next Level of Value
3. Credit card fraud and ID theft statistics
4. 2014 Faces of Fraud Survey: The Impact of Retail Breaches
5. Election Fraud in America
6. Exhaustive Database of Voter Fraud Cases Turns Up Scant Evidence That It Happens
7. U.S. voter turnout trails most developed countries