Blockchains: What are they, and how can they be applied to business problems?

Contents

1. Overview

A blockchain is a single-version record system that grows continuously. New records, called blocks, are added to the chain as new information propagates through the peer network. This whitepaper is intended to provide a brief overview of the state of existing blockchain technologies, as well as a technical overview of the features that have caused this technology to gain so much momentum since the turn of the 21st century.

2. Technical Review

While the primary application of blockchain has so far been in the realm of currency development, there is high potential for other applications. The following features have already begun to be adopted in sectors from healthcare to energy production and manufacturing.

2.1. Decentralization

A decentralized network uses client software on participating devices to synchronize and communicate information on a mutual forum. [6] New information is transmitted out to any listening nodes, which update their copy of the new data. Each node then competes to organize the new data into an appropriate block to satisfy the constraints of the system. Once a new block is confirmed, all nodes across the system transmit the new version of the block chain, and the nodes that contributed to solving the block are rewarded in a related currency.

2.2. Trustless Systems

Because all nodes have to run the same software in order to be allowed to participate, the network is always entirely decentralized. All nodes are open sourced; so all participants can be assured that everyone is playing by the rules. Furthermore, the entire history of the network is available at all times, which means that any malicious activity can be resolved and corrected. [7]

Open source software and public records cannot be bypassed without destroying the underlying system, since any malicious attacker would need to take over the majority of the nodes in the system. [8] The larger the community becomes, the more difficult it is to subvert.

2.3. Forks

If the network is ever corrupted, or errors in the public record or software are identified, a fork can occur where a portion of the nodes choose to adopt a change to the system, creating an entirely new network. At the time this report was published, there have been forks in both of the major blockchains, Bitcoin and Ethereum, and they've been well handled by the community without disruptions to either value or liquidity. [9]

2.4. Distributed Applications (smart contracts)

Recent improvements in the Ethereum blockchain have added the option for nodes to upload programs to the blockchain, which can be executed by other nodes. [10] These smart contracts are now being used to develop entirely distributed applications that exist as truly trustless systems.

2.5. ICO

An ICO or Initial Coin Offering is a process used to crowd fund a distributed application by selling a predefined amount of the currency that it will use to do business. This presell of the currency provides a non-controlling stake which appreciates in value relative to the application firm. ICOs allow the network to have initial volume and liquidity, ensuring stable growth. [11]

3. Business Applications

The inherent stability and transparency of blockchain systems in addition to the new potential of smart contracts has triggered a boom in blockchain applications for everyone from small to medium enterprises to major corporations.

3.1. International Transaction Cost Reduction

One of the primary advantages of blockchain currencies is that transaction fees are set from the creation of a network, and generally fall as low as 1 %. [2] This means that it can often be less expensive to convert international currencies to blockchain currencies and then back again, rather than paying international exchange rates or transfer fees on wire transfers.

Solutions now exist that allow you to even send a money transfer via crypto currency, so that the end user receives an email asking whether they'd like to convert the funds to another currency or transfer them to another crypto wallet. [4]

3.2. Process Automation

One of the primary uses of smart contracts at this time has been as escrow accounts for the use of money transfers and conditional payment. [12] Smart contracts can be designed to queue off of an external trigger, time based event, or node contact, which has provided a wide range of distributed applications.

3.3. Data Security

While blockchain data is publicly visible, the content can be encrypted using a private key, which renders it entirely unreadable to any other users. This simultaneously assures that the data is secure, and that it cannot be edited. Furthermore, because the data is distributed, it is exceedingly difficult for any attacker to hold the files to ransom, and maximizes access and uptime. [5]

3.4. Fraud Protection

There has been substantial discussion in the media regarding the potential for crypto currencies to be used for illicit money management practices and illegal activity, but these are in fact entirely incorrect. [7] Because of the open ledger, all transactions on a block chain can be traced, so the only limitation is the accounting of conversion from blockchain to fiat currency.

Furthermore, the same feature makes blockchain the perfect option for internal data storage within organizations. If there is already a wide network of devices, the distribution of key data across devices, rather than centrally, is the optimal method of securing data and ensuring that tampering and fraud cannot occur. [6]

Citations

1. David Parkins, “The great chain of being sure about things”, The Economist, https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

2. Bitcoin wiki, s.v. “Address,” accessed July 30, 2013, https://en.bitcoin.it/wiki /Address.

3. Jerry Brito and Andrea Castillo, “Bitcoin, A Primer for Policy Makers”, Mercatus Center, George Mason University, https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf

4. Fergal Reid and Martin Harrigan, “An Analysis of Anonymity in the Bitcoin System,” in Security and Privacy in Social Networks, ed. Yaniv Altshuler et al. (New York: Springer, 2013), http://arxiv.org/pdf/1107.4524v2.pdf

5. MoneyBadger, “How does it work”, https://moneybadger.io/#how

6. Jon Crowcroft, Tim Moreton, Ian Pratt, Andrew Twigg, University of Cambridge Computer Laboratory, “Peer-to-Peer Systems and the Grid”, http://www.cl.cam.ac.uk/teaching/2003/AdvSysTop/grid-p2p-paper.pdf

7. Kevin D. Werbach, “Trustless Trust“, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2844409

8. Martijn Bastiaan, University of Twente, “Preventing the 51%-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin”, http://referaat.cs.utwente.nl/conference/22/paper/7473/preventing-the-51-attack-a-stochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf

9. Coindesk, “A short guide to Bitcoin Forks”, https://www.coindesk.com/short-guide-bitcoin-forks-explained/

10. Ethereum, https://ethereum.org/

11. Andrew Marshall, CoinTelegraph, “How to Launch a Successful ICO, Explained” https://cointelegraph.com/explained/how-to-launch-a-successful-ico-explained\

12. CapGemini Consulting, Smart Contracts in Financial Services: Getting from Hype to Reality, https://www.capgemini-consulting.com/resource-file-access/resource/pdf/smart-contracts.pdf

13. Nick Szabo, “Smart Contracts: 12 Use Cases for Business & Beyond” http://bloq.com/assets/smart-contracts-white-paper.pdf