Bus Inf Syst Eng 59(3):183–187 (2017)
DOI 10.1007/s12599-017-0467-3

CATCHWORD

Blockchain

Michael Nofer · Peter Gomber · Oliver Hinz · Dirk Schiereck

Received: 20 January 2017 / Accepted: 20 February 2017 / Published online: 20 March 2017

Keywords Blockchain · Block chain · Business models · Disintegration · Digital currency

1 Blockchain – A Disruptive Technology

Blockchain technology and distributed ledgers are attracting massive attention and trigger multiple projects in different industries. However, the financial industry is seen as a primary user of the blockchain concept. This is not only due to the fact that the most well-known application of this technology is the crypto-currency Bitcoin, but it is also driven by substantial process inefficiencies and a massive cost base issue specifically in this industry. On top of this, the financial crisis revealed that even in financial services it is not always possible to identify the correct present owner of an asset. It is even more of a problem to retrace ownership over a longer chain of changing buyers in global financial transaction services: when, e.g., the US investment bank Bear Stearns failed in 2008 and was completely acquired by JP Morgan Chase, the number of shares offered to the acquirer was larger than the shares outstanding in the books of Bear Stearns. It was not possible to clarify the accounting errors and JP Morgan Chase had to bear the damage from excess (digital) shares.

While the problem of tracing back ownership in long transaction chains is already a critical aspect in financial markets, it is also important for physical goods, e.g., (blood) diamonds or broccoli. US retailer Wal-Mart with more than 260 million customers per week is in search for a technology that helps to identify precisely those batches of vegetables that in a given case, e.g., are infected by coliform bacteria.

Intermediation is today's dominating solution for verifying ownership of assets and transaction processing. Intermediaries perform the careful checking of each involved party along a chain of intermediaries. However, this is not only time consuming and costly but also bears a credit risk in case an intermediary fails. The blockchain technology promises to overcome these critical aspects, representing "a shift from trusting people to trusting math" (Antonopoulos 2014) since human interventions are no longer necessary.

2 Blockchain Functionalities and Implications

A typical example for a blockchain is illustrated in Fig. 1. A blockchain consists of data sets which are composed of a chain of data packages (blocks) where a block comprises multiple transactions (TX1-n, see Fig. 1). The blockchain is extended by each additional block and hence represents a complete ledger of the transaction history. Blocks can be

Accepted after one revision by Prof. Dr. Sinz.

Dr. M. Nofer · Prof. Dr. O. Hinz (✉)
Electronic Markets, Fachgebiet Wirtschaftsinformatik, TU Darmstadt, Hochschulstr. 1, 64289 Darmstadt, Germany
e-mail: hinz@wi.tu-darmstadt.de

M. Nofer
e-mail: nofer@emarkets.tu-darmstadt.de

Prof. Dr. P. Gomber
E-Finance, Goethe-Universität Frankfurt, Theodor-W.-Adorno-Platz 4, 60629 Frankfurt am Main, Germany
e-mail: gomber@wiwi.uni-frankfurt.de

Prof. Dr. D. Schiereck
Corporate Finance, TU Darmstadt, Hochschulstr. 1, 64289 Darmstadt, Germany
e-mail: schiereck@bwl.tu-darmstadt.de

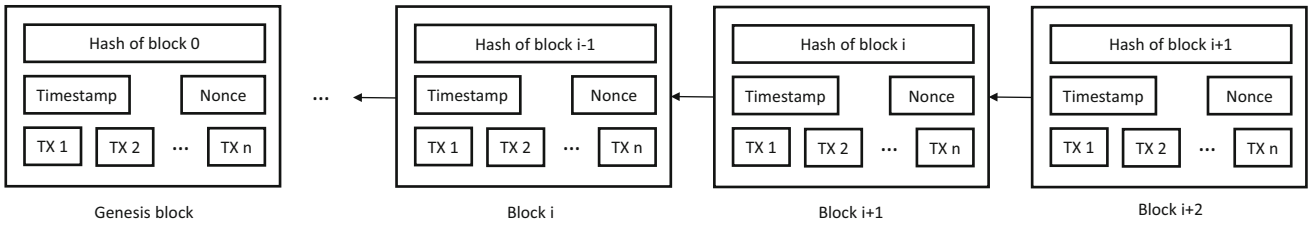

Fig. 1 Example of a blockchain (Zheng et al. 2016)

validated by the network using cryptographic means. In addition to the transactions, each block contains a timestamp, the hash value of the previous block ("parent"), and a nonce, which is a random number for verifying the hash. This concept ensures the integrity of the entire blockchain through to the first block ("genesis block"). Hash values are unique and fraud can be effectively prevented since changes of a block in the chain would immediately change the respective hash value. If the majority of nodes in the network agree by a consensus mechanism on the validity of transactions in a block and on the validity of the block itself, the block can be added to the chain. According to Swanson (2015), this consensus mechanism "is the process in which a majority (or in some cases all) of network validators come to agreement on the state of a ledger. It is a set of rules and procedures that allows maintaining coherent set of facts between multiple participating nodes". Therefore new transactions are not automatically added to the ledger. Rather, the consensus process ensures that these transactions are stored in a block for a certain time (e.g., 10 min in the Bitcoin blockchain) before being transferred to the ledger. Afterwards, the information in the blockchain can no longer be changed. In the case of Bitcoin, blocks are created by so-called miners who are rewarded with Bitcoins for validating the blocks. The example of Bitcoin illustrates that the principle of the blockchain cannot only change the process of money transactions. Using cryptography, people all over the world can trust each other and transfer different kinds of assets peer-to-peer over the internet.

The distributed ledger system described above offers many benefits. In contrast to centralized systems, the functionalities of the network persist even if particular nodes break down. This increases trust since people do not have to assess the trustworthiness of the intermediary or other participants in the network. It is sufficient if people solely build trust in the system as a whole. The absence of intermediaries also fosters data security. As discussed by Zyskind et al. (2015), the current practice of third parties collecting personal data implies the risk of security breaches. By utilizing the blockchain third parties can become obsolete, ultimately increasing user's security.

In computer science, various papers around blockchains have been published in recent years and have, e.g., analyzed consensus algorithms (e.g., Eyal and Sirer 2014) or proposed novel concepts to tackle issues regarding privacy of smart contracts (e.g., Kosba et al. 2016). However, besides a lot of industry whitepapers on blockchains, academic papers in information systems around blockchain currently primarily focus on cryptocurrencies. Besides significant benefits, there are also drawbacks and potential risks which are discussed in this stream of literature. Barber et al. (2012) highlight several weaknesses of Bitcoin, such as theft or loss of Bitcoins (malware attacks, accidental loss), scalability issues (e.g., delayed transaction confirmation, data retention, and communication failures), and structural problems (e.g., deflationary spiral). At the same time, Barber et al. (2012) suggest solutions for improving the existing Bitcoin technology. For instance, a "fair exchange protocol" might improve the user's anonymity. Privacy implications of Bitcoin have also been discussed by other authors (e.g., Androulaki et al. 2013; Bonneau et al. 2014; Miers et al. 2013). In the current Bitcoin world, privacy can only be protected by using pseudonyms. As an extension to Bitcoin, Miers et al. (2013) therefore developed Zerocoin, which allows for trading cryptocurrencies completely anonymously. In 2016, Zcash, the successor of Zerocoin was launched.

The process of generating new blocks implies performance problems if blocks are added to the network at a high rate. As an alternative to the existing blockchain structure, Lewenberg et al. (2015) introduce "Inclusive Block Chain Protocols" to increase the transaction speed. It will be interesting to observe whether performance problems can be overcome by this new technology. An analysis regarding the scalability of Bitcoin is provided by Croman et al. (2016).

3 Blockchain and Smart Contracts

The rise of the blockchain technology in recent years also supports other concepts that have been suggested in

literature. Szabo (1997) introduced the concept of "Smart Contracts", which combine computer protocols with user interfaces to execute the terms of a contract. Due to the blockchain, Smart Contracts are becoming more popular since they can be utilized more easily by applying blockchains in comparison to the technology available at the time of their invention 20 years ago. This innovative approach might, for example, replace lawyers and banks that have been involved in contracts for asset deals depending on predefined aspects (Fairfield 2014). Smart Contracts can also be used to control the ownership of properties. These properties might be tangible (e.g., houses, automobiles) or intangible (e.g., shares, access rights). A prominent example for blockchain technology that treats smart contracts as first class citizens is Ethereum, which is a decentralized system originally proposed by Buterin (2014). A taxonomy of decentralised consensus systems and an overview of different types of systems is provided by Glaser and Bezzenberger (2015). Ethereum can be seen as an extension of the Bitcoin blockchain to support a broader scope of applications. Thus, blockchain technology allows to establish contracts using cryptography and to replace third parties (e.g., a notary) that have been necessary to establish trust in the past. Blockchain might disrupt the entire transaction process by automatically executing contracts in a cost-effective, transparent and secure manner (Fairfield 2014). The architectural components of blockchain technology, their interaction as well as a framework for implication analysis of blockchain systems for digital ecosystems is proposed by Glaser (2017).

The financial industry is even wondering if large parts of their current business might be replaced by the blockchain. This can be illustrated by the payment process. If people pay goods by credit card today, the settlement occurs after a delay of several days. Utilizing the blockchain, this delayed settlement would become

Table 1 Applications of blockchain

Type	Application	Description	Examples
Financial applications	Crypto-currencies	Networks and mediums of exchange using cryptography to secure transactions	Bitcoin Litecoin Ripple Monero
	Securities issuance, trading and settlement	Companies going public issue shares directly and without a bank syndicate. Private, less liquid shares can be traded in a blockchain-based secondary market. First projects try to tackle securities settlement	NASDAQ private equity Medici Blockstream Coinsetter
	Insurance	Properties (e.g., real estate, automobiles, etc.) might be registered using the blockchain technology. Insurers can check the transaction history	Everledger
Non-financial applications	Notary public	Central authorization by notary is not necessary anymore	Stampery Viacoin Ascribe
	Music industry	Determining music royalties and managing music rights ownership	Imogen heap
	Decentralized proof of existence of documents	Storing and validating the signature and timestamp of a document using blockchain	www.proofofexistence.com
	Decentralized storage	Sharing documents without the need of a third party by using a peer-to-peer distributed cloud storage platform	Storj
	Decentralized internet of things	The blockchain reliably stores the communication of smart devices within the internet of things	Filament ADEPT (developed by IBM and Samsung)
	Anti-counterfeit solutions	Authenticity of products is verified by the blockchain network consisting of all market participants in electronic commerce (producers, merchants, marketplaces)	Blockverify
	Internet applications	Instead of governments and corporations, Domain Name Servers (DNS) are controlled by every user in a decentralized way	Namecoin

redundant since payment can be done in real time by adjusting the ledger.

4 Applications of Blockchain and Future Trends

4.1 Applications

Crosby et al. (2016) distinguish between financial and non-financial applications that could potentially be addressed by the blockchain (Table 1). This disruptive innovation has not only the potential to change the nature of interactions in Finance, but also in many other areas of our everyday life. For instance, the British singer Imogen Heap sells her songs using the blockchain.

4.2 Future Trends

The application fields for blockchains seem to be manifold, especially in areas that have historically relied on third parties to establish a certain amount of trust. Atzori (2015) suggests that politics and the entire society might be restructured by the blockchain. Many functions might become obsolete if people started to organize and protect the society using decentralized platforms. He concludes that "decentralization of government services through permissioned blockchains is possible and desirable, since it can significantly increase public administration functionality". Reorganizing societies is of prime importance in poor countries. Wealth can be protected more effectively using the blockchain. Especially in the third world, landowners have problems to prove the ownership if for example the local government aims to expropriate the population. These existential threats can be controlled by integrating land titles into the blockchain. However, as pointed out by Glaser (2017), the interface between the digital realm and the physical world could turn out to be the weak link which damages the digital trust established by a blockchain system.

There is also currently a debate among researchers and regulators if crypto-currencies relying on the blockchain can fulfill the functions of real money (European Central Bank 2012; Federal Bureau of Investigation 2012). Money has been defined by Mishkin (2004) as "anything that is generally accepted in payment for goods or services or in the repayment of debts". Luther and White (2014) argue that today crypto-currencies are only rarely used as a medium of exchange. Glaser et al. (2014) provide empirical insights that Bitcoin is indeed primarily used as a speculative asset. However, spending and accepting might become easier due to innovative approaches by entrepreneurs, establishing crypto-currencies as a substitute for fiat money. The blockchain might therefore contribute to change the way people pay for goods in the real world. Homeowners face significant transaction costs when buying property. According to Goldman Sachs, "blockchain could reduce title insurance premiums and generate $2–$4 billion in cost savings in the US by reducing errors and manual effort" (Goldman Sachs 2016).

While computer scientists mainly focus on the technical and cryptographic challenges in this area, researchers from the Business and Information Systems Engineering field have the opportunity to focus on market design, questions of trust and privacy, and the adoption respective non-adoption of the new technology. Moreover, this disruptive innovation might change many existing business models, create new ones and might have severe impacts on entire industries. Therefore, research at the intersection of technology, markets and business models is certainly valuable.

References

Androulaki E, Karame GO, Roeschlin M, Scherer T, Capkun S (2013) Evaluating user privacy in bitcoin. In: International Conference on Financial Cryptography and Data Security. Springer, Heidelberg, pp 34–51

Antonopoulos A (2014) Bitcoin security model: trust by computation. O'Reilly- Radar. http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-bycomputation.html. Accessed 30 Nov 2016

Atzori M (2015) Blockchain technology and decentralized governance: Is the state still necessary? Work Pap

Barber S, Boyen X, Shi E, Uzun E (2012) Bitter to better—how to make bitcoin a better currency. International Conference on Financial Cryptography and Data Security. Springer, Heidelberg, pp 399–414

Bonneau J, Narayanan A, Miller A, Clark J, Kroll JA, Felten EW (2014) Mixcoin: Anonymity for Bitcoin with accountable mixes. In International Conference on Financial Cryptography and Data Security. Springer, Heidelberg, pp 486–504

Buterin V (2014) A next-generation smart contract and decentralized application platform. White Pap

Croman K, Decker C, Eyal I, Gencer AE, Juels A, Kosba A, Miller A, Saxena P, Shi E, Gun Sirer E, Song D, Wattenhofer R (2016) On scaling decentralized blockchains. 3rd Workshop on Bitcoin Research (BITCOIN), Barbados

Crosby M, Nachiappan Pattanayak P, Verma S, Kalyanaraman V (2016) Blockchain technology: Beyond bitcoin. Appl Innov Rev 2:6–19

European Central Bank (2012) Virtual Currency Schemes. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf. Accessed 30 Nov 2016

Eyal I, Sirer EG (2014) Majority is not enough: Bitcoin mining is vulnerable. In: Proceedings of Financial Cryptography, Barbados

Fairfield J (2014) Smart contracts, Bitcoin bots, and consumer protection. Wash Lee L Rev Online 71:35–299

Federal Bureau of Investigation (2012) Bitcoin virtual currency: intelligence unique features present distinct challenges for deterring illicit activity. https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf. Accessed 30 Nov 2016

Glaser F (2017) Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis.

In: Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS 2017), Waikoloa Village, Hawaii

Glaser F, Bezzenberger L (2015) Beyond Cryptocurrencies-A Taxonomy of Decentralized Consensus Systems. In: Proceedings of the 23rd European Conference on Information Systems (ECIS 2015), Muenster, Germany

Glaser F, Zimmermann K, Haferkorn M, Weber M, Siering M (2014) Bitcoin-asset or currency? Revealing users' hidden intentions. In: Proceedings of the 22nd European Conference on Information Systems (ECIS 2014); Tel Aviv, Israel

Goldman Sachs (2016) Profiles in Innovation – Blockchain. http://www.the-blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf. Accessed 30 Nov 2016

Kosba A, Miller A, Shi E, Wen Z, Papamanthou C (2016) Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: IEEE Symposium on Security and Privacy (SP), pp 839–858

Lewenberg Y, Sompolinsky Y, Zohar A (2015) Inclusive block chain protocols. In: International Conference on Financial Cryptography and Data Security. Springer, Heidelberg, pp 528–547

Luther WJ, White LH (2014) Can bitcoin become a major currency? Working Paper

Miers I, Garman C, Green M, Rubin AD (2013) Zerocoin: Anonymous distributed e-cash from bitcoin. IEEE Symposium on Security and Privac. IEEE pp 397–411

Mishkin FS (2004) The economics of money and financial markets, 7th edn. Pearson, Boston

Swanson T (2015) Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. Work Pap

Szabo N (1997) Smart contracts: formalizing and securing relationships on public networks. First Monday 2(9). doi:10.5210/fm.v2i9.548

Zheng Z, Xie S, Dai HN, Wang H (2016) Blockchain Challenges and Opportunities: A Survey. Work Pap

Zyskind G, Nathan O, Pentland A (2015) Decentralizing privacy: Using blockchain to protect personal data. In Security and Privacy Workshops (SPW), IEEE 180–184