Smart contract

A **smart contract** is a computer program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement.[1][2][3][4] The objectives of smart contracts are the reduction of need in trusted intermediators, arbitrations and enforcement costs, fraud losses, as well as the reduction of malicious and accidental exceptions.[5][2]

Vending machines are mentioned as the oldest piece of technology equivalent to smart contract implementation.[3] 2014's white paper about the cryptocurrency Ethereum[6] describes the Bitcoin protocol as a weak version of the smart contract concept as defined by computer scientist, lawyer and cryptographer Nick Szabo. Since Ethereum, various cryptocurrencies support scripting languages which allow for more advanced smart contracts between untrusted parties.[7] Smart contracts should be distinguished from smart legal contracts. The latter refers to a traditional natural language legally-binding agreement which has certain terms expressed and implemented in machine-readable code.[8][9][10]

Contents

Etymology

Smart contracts were first proposed in the early 1990s by Nick Szabo, who coined the term, using it to refer to "a set of promises, specified in digital form, including protocols within which the parties perform on these promises".[11][12] In 1998, the term was used to describe objects in rights management service layer of the system *The Stanford Infobus*, which was a part of Stanford Digital Library Project.[1]

Legal status of smart contracts

A smart contract does not necessarily constitute a valid binding agreement at law. Some legal academics claim that smart contracts are not legal agreements, but rather means of performing obligations deriving from other agreements[13] such as technological means for the automation of payment obligations[14] or obligations consisting in the transfer of tokens or cryptocurrencies. Additionally, other scholars have argued that the imperative or declarative nature of programming languages can impact the legal validity of smart contracts.[15]

Since the 2015 launch of the Ethereum blockchain,[16] the term "smart contract" has been more specifically applied toward the notion of general purpose computation that takes place on a blockchain or distributed ledger. The US National Institute of Standards and Technology describes a "smart contract" as a "collection of code and data (sometimes referred to as functions and state) that is deployed using cryptographically signed transactions on the blockchain network".[17] In this interpretation, used for example by the Ethereum Foundation[6] or IBM,[18] a smart contract is not necessarily related to the classical concept of a contract, but can be any kind of computer program. A smart contract also can be regarded as a secured stored procedure as its execution and codified effects like the transfer of some value between parties are strictly enforced and can not be manipulated, after a transaction with specific contract details is stored into a blockchain or distributed ledger. That's because the actual execution of contracts is controlled and audited by the platform, not by any arbitrary server-side programs connecting to the platform.[19][20]

In 2017, by implementing the Decree on Development of Digital Economy, Belarus has become the first-ever country to legalize smart contracts. Belarusian lawyer Denis Aleinikov is considered to be the author of a smart contract legal concept introduced by the decree.[21]

In 2018, a US Senate report said: "While smart contracts might sound new, the concept is rooted in basic contract law. Usually, the judicial system adjudicates contractual disputes and enforces terms, but it is also common to have another arbitration method, especially for international transactions. With smart contracts, a program enforces the contract built into the code."[22] A number of states in the US have passed legislation on the use of smart contracts, such as Arizona,[23] Nevada,[24] Tennessee,[25] and Wyoming.[26] And in April 2020, Iowa's House of Representatives passed a bill legally recognizing smart contacts in the state.[27]

In April 2021, the UK Jurisdiction Taskforce (UKJT) published the Digital Dispute Resolution Rules (the Digital DR Rules) to help enable the rapid resolution of blockchain and crypto legal disputes in Britain.[28]

Workings

Similar to a transfer of value on a blockchain, deployment of a smart contract on a blockchain occurs by sending a transaction from a wallet for the blockchain.[29] The transaction includes the compiled code for the smart contract as well as a special receiver address.[29] That transaction must then be included in a block that is added to the blockchain, at which point the smart contract's code will execute to establish the initial state of the smart contract.[29] Byzantine fault-tolerant algorithms secure the smart contract in a decentralized way from attempts to tamper with it. Once a smart contract is deployed, it cannot be updated.[30] Smart contracts on a blockchain can store arbitrary state and execute arbitrary computations. End clients interact with a smart contract through transactions. Such transactions with a smart contract can invoke other smart contracts. These transactions might result in changing the state and sending coins from one smart contract to another or from one account to another.[30]

The most popular blockchain for running smart contracts is Ethereum.[31] On Ethereum, smart contracts are typically written in a Turing-complete programming language called Solidity,[32] and compiled into low-level bytecode to be executed by the Ethereum Virtual Machine.[33] Due to the halting problem and other security problems, Turing-completeness is considered to be a risk and is deliberately avoided by languages like Vyper.[34][35] Some of the other smart contract programming languages missing Turing-completeness are Simplicity, Scilla, Ivy and Bitcoin Script.[35] However, measurements using regular expressions showed that only 35.3% of 53,757 Ethereum smart contracts included recursions and loops — constructs connected to the halting problem.[36]

Several languages are designed to enable formal verification: Bamboo, IELE, Simplicity, Michelson (can be verified with Coq),[35] Liquidity (compiles to Michelson), Scilla, DAML and Pact.[34]

Notable examples of blockchain platforms supporting smart contracts include the following:

Name	Description
Bitcoin	Provides a Turing-incomplete script language that allows the creation of custom smart contracts on top of Bitcoin like multisignature accounts, payment channels, escrows, time locks, atomic cross-chain trading, oracles, or multi-party lottery with no operator.[37]
Cardano	A blockchain platform for smart contracts, using proof of stake
Ethereum	Implements a Turing-complete language on its blockchain, a prominent smart contract framework[38]
EOS.IO	A blockchain platform for smart contracts
Tezos	A blockchain platform modifying its own set of rules with minimal disruption to the network through an on-chain governance model

Processes on a blockchain are generally deterministic in order to ensure Byzantine fault-tolerance.[39] Nevertheless, real world application of smart contracts, such as lotteries and casinos, require secure randomness.[40] In fact, blockchain technology reduces the costs for conducting of a lottery and is therefore beneficial for the participants. Randomness on blockchain can be implemented by using block hashes or timestamps, oracles, commitment schemes, special smart contracts like RANDAO[41][42] and Quanta as well as sequences from mixed strategy Nash equilibria.[39]

Applications

In 1998, Szabo proposed that smart contract infrastructure can be implemented by replicated asset registries and contract execution using cryptographic hash chains and Byzantine fault-tolerant replication.[43] Askemos implemented this approach in 2002[44][45] using Scheme (later adding SQLite[46][47]) as contract script language.[48]

One proposal for using bitcoin for replicated asset registration and contract execution is called "colored coins".[49] Replicated titles for potentially arbitrary forms of property, along with replicated contract execution, are implemented in different projects.

As of 2015, UBS was experimenting with "smart bonds" that use the bitcoin blockchain[50] in which payment streams could hypothetically be fully automated, creating a self-paying instrument.[51]

Inheritance wishes could hypothetically be implemented automatically upon registration of a death certificate by means of smart contracts.[52][53] Birth certificates can also work together with smart contracts.[54][55]

Smart contracts can also be used to handle real estate transactions [56] (i.e. via Propy, ...)[57] [58] and blockchain solutions are also proliferating on the field of title records and in the public register.[59][60][61][62][63]

Smart contracts can also be used in employment contracts, especially temporary employment contracts, offering benefits for both employer and employee.[64][65]

Security issues

A blockchain-based smart contract is visible to all users of said blockchain. However, this leads to a situation where bugs, including security holes, are visible to all yet may not be quickly fixed.[66] Such an attack, difficult to fix quickly, was successfully executed on The DAO in June 2016, draining approximately US$50 million worth of Ether at the time, while developers attempted to come to a solution

that would gain consensus.[67] The DAO program had a time delay in place before the hacker could remove the funds; a hard fork of the Ethereum software was done to claw back the funds from the attacker before the time limit expired.[68] Other high-profile attacks include the Parity multisignature wallet attacks, and an integer underflow/overflow attack (2018), totaling over US$184 million.[69]

Issues in Ethereum smart contracts, in particular, include ambiguities and easy-but-insecure constructs in its contract language Solidity, compiler bugs, Ethereum Virtual Machine bugs, attacks on the blockchain network, the immutability of bugs and that there is no central source documenting known vulnerabilities, attacks and problematic constructs.[38]

Difference from smart legal contracts

Smart legal contracts are distinct from smart contracts. As mentioned above, a smart contract is not necessarily legally enforceable as a contract. On the other hand, a smart legal contract has all the elements of a legally enforceable contract in the jurisdiction in which it can be enforced and it can be enforced by a court or tribunal. Therefore, while every smart legal contract will contain some elements of a smart contract, not every smart contract will be a smart legal contract.[70]

There is no formal definition of a smart legal contract in the legal industry.[71]

A Ricardian contract is a type of smart legal contract.

See also

- *Code and Other Laws of Cyberspace*
- Decentralized application
- Ethereum
- Regulation by algorithms
- Regulation of algorithms
- Ricardian contract (a design pattern to capture the intent of the agreement of parties)
- Loan
- Secure multiparty computation
- Transparency

References

1. Röscheisen, Martin; Baldonado, Michelle; Chang, Kevin; Gravano, Luis; Ketchpel, Steven; Paepcke, Andreas (1998). "The Stanford InfoBus and its service layers: Augmenting the internet with higher-level information management protocols". *Digital Libraries in Computer Science: The MeDoc Approach*. Lecture Notes in Computer Science. Springer. **1392**: 213–230. doi:10.1007/bfb0052526 (https://doi.org/10.1007%2Fbfb0052526). ISBN 978-3-540-64493-4.
2. Fries, Martin; P. Paal, Boris (2019). *Smart Contracts* (in German). Mohr Siebeck. ISBN 978-3-16-156911-1. JSTOR j.ctvn96h9r (https://www.jstor.org/stable/j.ctvn96h9r).
3. Savelyev, Alexander (14 December 2016). "Contract Law 2.0: "Smart" Contracts As the Beginning of the End of Classic Contract Law". Social Science Research Network. SSRN 2885241 (https://ssrn.com/abstract=2885241).
4. Tapscott, Don; Tapscott, Alex (May 2016). *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. pp. 72, 83, 101, 127. ISBN 978-0670069972.

5. Szabo, Nick (1997). "View of Formalizing and Securing Relationships on Public Networks | First Monday" (https://firstmonday.org/article/view/548/469). *firstmonday.org*.
6. "White Paper· ethereum/wiki Wiki · GitHub" (https://github.com/ethereum/wiki/wiki/White-Paper). Archived (https://web.archive.org/web/20140111180823/http://ethereum.org/ethereum.html) from the original on 11 January 2014.
7. Alharby, Maher; van Moorsel, Aad (26 August 2017). "Blockchain-based Smart Contracts: A Systematic Mapping Study". *Computer Science & Information Technology*: 125–140. arXiv:1710.06372 (https://arxiv.org/abs/1710.06372). doi:10.5121/csit.2017.71011 (https://doi.org/10.5121%2Fcsit.2017.71011). ISBN 9781921987700. S2CID 725413 (https://api.semanticscholar.org/CorpusID:725413).
8. Cannarsa, Michel (1 December 2018). "Interpretation of Contracts and Smart Contracts: Smart Interpretation or Interpretation of Smart Contracts?" (https://kluwerlawonline.com/journalarticle/European+Review+of+Private+Law/26.6/ERPL2018054). *European Review of Private Law*. **26** (6).
9. Drummer, Daniel; Neumann, Dirk (5 August 2020). "Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts" (https://journals.sagepub.com/doi/abs/10.1177/0268396220924669). *Journal of Information Technology*. **35** (4): 337–360. doi:10.1177/0268396220924669 (https://doi.org/10.1177%2F0268396220924669). ISSN 0268-3962 (https://www.worldcat.org/issn/0268-3962). S2CID 225409384 (https://api.semanticscholar.org/CorpusID:225409384).
10. Filatova, Nataliia (1 September 2020). "Smart contracts from the contract law perspective: outlining new regulative strategies" (https://academic.oup.com/ijlit/article-abstract/28/3/217/5897086). *International Journal of Law and Information Technology*. **28** (3): 217–242. doi:10.1093/ijlit/eaaa015 (https://doi.org/10.1093%2Fijlit%2Feaaa015). ISSN 0967-0769 (https://www.worldcat.org/issn/0967-0769).
11. Morris, David Z. (21 January 2014). "Bitcoin is not just digital currency. It's Napster for finance" (http://fortune.com/2014/01/21/bitcoin-is-not-just-digital-currency-its-napster-for-finance/). *Fortune*. Retrieved 7 November 2018.
12. Schulpen, Ruben R.W.H.G. (1 August 2018). "Smart contracts in the Netherlands - University of Tilburg" (http://arno.uvt.nl/show.cgi?fid=146860). *uvt.nl*. Twente University. Retrieved 26 October 2019.
13. Mik, Eliza, Smart Contracts: A Requiem (December 7, 2019). Journal of Contract Law (2019) Volume 36 Part 1 at p 72
14. J Cieplak, S Leefatt, 'Smart Contracts: A Smart Way To Automate Performance' (2017) 1 Georgia L & Tech Rev 417
15. Governatori, Guido; Idelberger, Florian; Milosevic, Zoran; Riveret, Regis; Sartor, Giovanni; Xu, Xiwei (2018). "On legal contracts, imperative and declarative smart contracts, and blockchain systems". *Artificial Intelligence and Law*. **26** (4): 33. doi:10.1007/s10506-018-9223-3 (https://doi.org/10.1007%2Fs10506-018-9223-3). S2CID 3663005 (https://api.semanticscholar.org/CorpusID:3663005).
16. Buterin, Vitalik (August 7, 2015). "Ethereum - On Public and Public Blockchains" (https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/). *Ethereum.Org*.
17. D J Yaga et al., Blockchain Technology Overview, National Institute of Standards and Technology Internal/Interagency Report 8202, 2018, p 54, cited in Mik, Eliza, Smart Contracts: A Requiem (December 7, 2019). Journal of Contract Law (2019) Volume 36 Part 1 at p 71
18. Cachin, Christian. "Architecture of the Hyperledger Blockchain Fabric" (https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf) (PDF). *ibm.com*.

19. Vo, Hoang Tam; Kundu, Ashish; Mohania, Mukesh (2018). "Research Directions in Blockchain Data Management and Analytics" (https://openproceedings.org/2018/conf/edbt/paper-227.pdf) (PDF). *Advances in Database Technology - Extending Database Technology (EDBT)*. OpenProceedings. **21**: 446. "Some distributed ledger technologies support an additional capability called a smart contract, which is similar to the concept of stored procedure in classical relational databases to some extent. Smart contracts allow the shared business processes within a business network to be standardised, automated and enforced via computer programs to increase the integrity of the ledger."
20. Huckle, Steve; Bhattacharya, Rituparna; White, Martin; Beloff, Natalia (2016). "Internet of Things, Blockchain and Shared Economy Applications" (https://doi.org/10.1016%2Fj.procs.2016.09.074). *Procedia Computer Science*. Elsevier B.V. **98**: 463. doi:10.1016/j.procs.2016.09.074 (https://doi.org/10.1016%2Fj.procs.2016.09.074). "Firstly, that total quantity of BTC in a transaction's inputs must cover the total number of BTC in the outputs. That rule behaves similarly to a database stored procedure, except that it is impossible to circumvent. Secondly, BTC transactions use public-private key cryptography. That makes BTC act like a database with a publicly auditable per-row permission scheme."
21. Makhovsky, Andrei (December 22, 2017). "Belarus adopts crypto-currency law to woo foreign investors" (https://www.reuters.com/article/us-belarus-cryptocurrency-idUSKBN1EG0XO). *Reuters*.
22. Chapter 9: Building a Secure Future, One blockchain at a time (https://www.jec.senate.gov/public/_cache/files/aaac3a69-e9fb-45b6-be9f-b1fd96dd738b/chapter-9-building-a-secure-future-one-blockchain-at-a-time.pdf), US Senate Joint Economic Committee, March 2018.
23. "Arizona HB2417 - 2017 - Fifty-third Legislature 1st Regular" (https://legiscan.com/AZ/text/HB2417/id/1588180). *LegiScan*.
24. Hyman Gayle M, Digesti, Matthew P New Nevada legislation recognizes blockchain and smart contract terminologies (https://www.nvbar.org/wp-content/uploads/NevadaLawyer_Aug2017_Blockchain-1.pdf) August 2017, Nevada Lawyer
25. Tom, Daniel (22 September 2020). "Smart Contract Bill Tennessee" (http://www.capitol.tn.gov/Bills/110/Bill/SB1662.pdf) (PDF).
26. Wyoming, Legislature (26 February 2019). "Wyoming - Smart Contract" (https://wyoleg.gov/Legislation/2019/sf0125).
27. "Iowa House approves bills to facilitate broadband, cryptocurrency" (https://www.thegazette.com/government-politics/iowa-house-approves-bills-to-facilitate-broadband-cryptocurrency/). *www.thegazette.com*. Retrieved 2021-04-15.
28. Morgan, Herbert Smith Freehills LLP-Charlie; Parker, Chris; Livingston, Dorothy; Naish, Vanessa; Tevendale, Craig. "Arbitration of digital disputes in smart contracts and the release of the digital dispute resolution rules from the UK jurisdiction taskforce | Lexology" (https://www.lexology.com/library/detail.aspx?g=6ea7c284-0157-4f2c-b330-e2758d1bf7a0). *www.lexology.com*. Retrieved 2021-04-25.
29. Soloro, Kevin; Kanna, Randall; Hoover, David (December 2019). *Hands-On Smart Contract Development With Solidity and Ethereum: From Fundamentals to Deployment* (https://www.google.com/books/edition/Hands_On_Smart_Contract_Development_with/thbADwAAQBAJ?hl=en&gbpv=1&kptab=getbook). California, U.S.A.: O'Reilly. p. 73. ISBN 978-1-492-04526-7. Retrieved 1 November 2020.
30. Sergey, Ilya; Nagaraj, Vaivaswatha; Johannsen, Jacob; Kumar, Amrit; Trunov, Anton; Hao, Ken Chan Guan (10 October 2019). "Safer smart contract programming with Scilla" (https://doi.org/10.1145%2F3360611). *Proceedings of the ACM on Programming Languages*. **3** (OOPSLA): 1–30. doi:10.1145/3360611 (https://doi.org/10.1145%2F3360611). ISSN 2475-1421 (https://www.worldcat.org/issn/2475-1421).

31. Alharby, Maher; van Moorsel, Aad (26 August 2017). "Blockchain-based Smart Contracts: A Systematic Mapping Study" (https://doi.org/10.5121%2Fcsit.2017.71011). *Computer Science & Information Technology (CS & IT)*: 125–140. arXiv:1710.06372 (https://arxiv.org/abs/1710.06372). doi:10.5121/csit.2017.71011 (https://doi.org/10.5121%2Fcsit.2017.71011). ISBN 9781921987700.
32. Wohrer, Maximilian; Zdun, Uwe (20 March 2018). "Smart contracts: security patterns in the ethereum ecosystem and solidity" (https://ieeexplore.ieee.org/document/8327565). *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*: 2–8. doi:10.1109/IWBOSE.2018.8327565 (https://doi.org/10.1109%2FIWBOSE.2018.8327565). ISBN 978-1-5386-5986-1. S2CID 4567923 (https://api.semanticscholar.org/CorpusID:4567923).
33. Perez, Daniel; Livshits, Benjamin (17 October 2020). "Smart Contract Vulnerabilities: Vulnerable Does Not Imply Exploited". arXiv:1902.06710 (https://arxiv.org/abs/1902.06710) [cs.CR (https://arxiv.org/archive/cs.CR)].
34. Harz, Dominik; Knottenbelt, William (31 October 2018). "Towards Safer Smart Contracts: A Survey of Languages and Verification Methods". arXiv:1809.09805 (https://arxiv.org/abs/1809.09805) [cs.CR (https://arxiv.org/archive/cs.CR)].
35. Tyurin, A.V.; Tyuluandin, I.V.; Maltsev, V.S.; Kirilenko, I.A.; Berezun, D.A. (2019). "Overview of the Languages for Safe Smart Contract Programming" (https://doi.org/10.15514%2Fispras-2019-31%283%29-13). *Proceedings of the Institute for System Programming of the RAS*. **31** (3): 157–176. doi:10.15514/ispras-2019-31(3)-13 (https://doi.org/10.15514%2Fispras-2019-31%283%29-13). S2CID 203179644 (https://api.semanticscholar.org/CorpusID:203179644).
36. Jansen, Marc; Hdhili, Farouk; Gouiaa, Ramy; Qasem, Ziyaad (2020). "Do Smart Contract Languages Need to Be Turing Complete?". *Blockchain and Applications*. Advances in Intelligent Systems and Computing. Springer International Publishing. **1010**: 19–26. doi:10.1007/978-3-030-23813-1_3 (https://doi.org/10.1007%2F978-3-030-23813-1_3). ISBN 978-3-030-23812-4. S2CID 195656195 (https://api.semanticscholar.org/CorpusID:195656195).
37. Atzei, Nicola; Bartoletti, Massimo; Cimoli, Tiziana; Lande, Stefano; Zunino, Roberto (2018), "SoK: unraveling Bitcoin smart contracts" (https://eprint.iacr.org/2018/192.pdf) (PDF), *7th International Conference on Principles of Security and Trust (POST)*, European Joint Conferences on Theory and Practice of Software
38. Atzei, Nicola; Bartoletti, Massimo; Cimoli, Tiziana (2017), "A survey of attacks on Ethereum smart contracts" (http://eprint.iacr.org/2016/1007.pdf) (PDF), *6th International Conference on Principles of Security and Trust (POST)*, European Joint Conferences on Theory and Practice of Software
39. Chatterjee, Krishnendu; Goharshady, Amir Kafshdar; Pourdamghani, Arash (21 February 2019). "Probabilistic Smart Contracts: Secure Randomness on the Blockchain". arXiv:1902.07986 (https://arxiv.org/abs/1902.07986) [cs.GT (https://arxiv.org/archive/cs.GT)].
40. Chen, Tai-yuan; Huang, Wei-ning; Kuo, Po-chun; Chung, Hao (6 August 2020). "Method for Generating Secure Randomness on Blockchain" (http://www.freepatentsonline.com/y2020/0252211.html). Retrieved 28 August 2020.
41. Jia, Zhifeng; Chen, Rui; Li, Jie (2019). "DeLottery: A Novel Decentralized Lottery System Based on Blockchain Technology". *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications*. pp. 20–25. doi:10.1145/3376044.3376049 (https://doi.org/10.1145%2F3376044.3376049). ISBN 9781450377430. S2CID 207880557 (https://api.semanticscholar.org/CorpusID:207880557).
42. "randao/randao" (https://github.com/randao/randao). randao. 10 July 2020. Retrieved 10 July 2020.
43. Nick Szabo (1998). "Secure Property Titles with Owner Authority" (https://web.archive.org/web/20140115142013/http://szabo.best.vwh.net/securetitle.html). Archived from the original (http://szabo.best.vwh.net/securetitle.html) on January 15, 2014. Retrieved January 12, 2014.

44. Jörg F. Wittenberger (2002). *Askemos a distributed settlement* (http://citeseerx.ist.psu.edu/viewdoc/download;?doi=10.1.1.11.5050&rep=rep1&type=pdf). Proceedings of International Conference on Advances in Infrastructure for e-Business, e-Education, e-Science, and e-Medicine on the Internet (SSGRR), L'Aquila.
45. "Proceedings of International Conference on Advances in Infrastructure for e-Business, e-Education, e-Science, and e-Medicine on the Internet" (http://www.isl.cs.waseda.ac.jp/~sugawara/pdf/kurihara-SSGRR2002.pdf) (PDF).
46. Martin Möbius (2009). "Erstellung eines Archivierungskonzepts für die Speicherung rückverfolgbarer Datenbestände im Askemos-System" (https://monami.hs-mittweida.de/frontdoor/index/index/docId/476).
47. Tom-Steve Watzke (2010). "Entwicklung einer Datenbankschnittstelle als Grundlage für Shop-Systeme unter dem Betriebssystem Askemos" (https://core.ac.uk/display/33987564).
48. RA Markus Heinker (2007). "Beweiswürdigung elektronischer Dokumente im Zivilprozess unter vergleichender Betrachtung von qualifizierten elektronischen Signaturen nach dem Signaturgesetz und dem Askemos-Verfahren" (http://askemos.org/A0e80fdd97a7b6e7af87c5d294f39a96c).
49. Hal Hodson (20 November 2013). "Bitcoin moves beyond mere money" (https://www.newscientist.com/article/dn24620-bitcoin-moves-beyond-mere-money.html). *New Scientist*. Retrieved 12 January 2014.
50. Ross, Rory (2015-09-12). "Smart Money: Blockchains Are the Future of the Internet" (http://europe.newsweek.com/smart-money-blockchains-are-future-internet-329278). *Newsweek*. Retrieved 2016-05-27.
51. Wigan, David (2015-06-11). "Bitcoin technology will disrupt derivatives, says banker" (http://www.ifrasia.com/bitcoin-technology-will-disrupt-derivatives-says-banker/21202956.article). *IFR Asia*. Retrieved 2016-05-27.
52. How blockchain technology could change our lives (https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf)
53. Blockchain and AI are coming to kill these 4 business verticals (https://www.inc.com/chris-j-snook/4-small-business-verticals-artificial-intelligence-blockchain-will-destroy-in-coming-decade.html)
54. Blockchain for Digital Governments (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC115049/blockchain_for_digital_government_online.pdf)
55. Blockchain Based Framework for Document Authentication (https://link.springer.com/chapter/10.1007/978-3-030-67490-8_19)
56. Blockchain and AI are coming to kill these 4 business verticals (https://www.inc.com/chris-j-snook/4-small-business-verticals-artificial-intelligence-blockchain-will-destroy-in-coming-decade.html)
57. Propy's Mission to Transform the Real Estate Industry (https://medium.com/@timventura/propys-mission-to-transform-the-real-estate-industry-c03b76d012ba)
58. Propy Completes the First Real Estate Deal Recorded on Blockchain (https://medium.com/@propy/propy-completes-the-1st-real-estate-deal-recorded-on-blockchain-edcec38b5f19)
59. Blockchain and AI are coming to kill these 4 business verticals (https://www.inc.com/chris-j-snook/4-small-business-verticals-artificial-intelligence-blockchain-will-destroy-in-coming-decade.html)
60. The Bitfury Group and Government of Republic of Georgia Expand Blockchain Pilot (https://bitfury.com/content/downloads/the_bitfury_group_republic_of_georgia_expand_blockchain_pilot_2_7_16.pdf)
61. A BLOCKCHAIN - Journals Gateway (https://www.mitpressjournals.org/doi/pdf/10.1162/inov_a_00276)
62. Digital Transformation: Blockchain and Land Titles (https://www.oecd.org/corruption/integrity-forum/academic-papers/Georg%20Eder-%20Blockchain%20-%20Ghana_verified.pdf)

63. Ukraine launches big blockchain deal with tech firm Bitfury (https://www.reuters.com/article/us-ukraine-bitfury-blockchain-idUSKBN17F0N2)
64. The Gig Economy, Smart Contracts and Disruption of traditional work arrangements (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3270867)
65. A blockchain-based decentralized system for proper handling of temporary employment contracts (https://www.researchgate.net/publication/328657407_A_Blockchain-Based_Decentralized_System_for_Proper_Handling_of_Temporary_Employment_Contracts)
66. Peck, M. (28 May 2016). "Ethereum's $150-Million Blockchain-Powered Fund Opens Just as Researchers Call For a Halt" (https://spectrum.ieee.org/tech-talk/computing/networks/ethereums-150-million-dollar-dao-opens-for-business-just-as-researchers-call-for-a-moratorium). *IEEE Spectrum*. Institute of Electrical and Electronics Engineers.
67. DuPont, Quinn (2017). "Experiments in Algorithmic Governance: A history and ethnography of "The DAO", a failed Decentralized Autonomous Organization" (https://web.archive.org/web/20170730133911/http://iqdupont.com/assets/documents/DUPONT%2D2017%2DPreprint%2DAlgorithmic%2DGovernance.pdf) (PDF). Archived from the original (http://iqdupont.com/assets/documents/DUPONT-2017-Preprint-Algorithmic-Governance.pdf) (PDF) on 2017-07-30. Retrieved 29 July 2017.
68. Coy, Peter; Kharif, Olga (25 August 2016). "This Is Your Company on Blockchain" (https://www.bloomberg.com/news/articles/2016-08-25/this-is-your-company-on-blockchain). *Bloomberg Businessweek*. Retrieved 2016-12-05.
69. Praitheeshan, Purathani; Pan, Lei; Yu, Jiangshan; Liu, Joseph; Doss, R. (2019). "Security Analysis Methods on Ethereum Smart Contract Vulnerabilities: A Survey". arXiv:1908.08605 (https://arxiv.org/abs/1908.08605) [cs.CR (https://arxiv.org/archive/cs.CR)].
70. Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective (https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf), 5.
71. Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective (https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf), 3.
