



The National Agricultural Law Center

The nation's leading source for agricultural & food law research & information

NationalAgLawCenter.org | nataglaw@uark.edu

Blockchain and Bitcoin Basics: Applicability to Agriculture

Carol R. Goforth



This material is based upon work supported by the National Agricultural Library,
Agricultural Research Service, U.S. Department of Agriculture

Blockchain and Bitcoin Basics: Applicability to Agriculture

By

Carol R. Goforth*

Outline

Introduction	1
Background	1
How Blockchain Functions (in a non-technical sense)	4
Understanding Bitcoin: The Basics	5
Other Cryptoassets	7
What about Agriculture?	8
Conclusion	10

Introduction

This is the first in a series of three papers. This paper introduces blockchain and cryptoassets; the second focuses on the potential risks and benefits of creating and/or utilizing cryptoassets in connection with business operations (including those focused on agriculture); and the third focuses on blockchain applications that could be applied to agricultural operations. In order to understand the risks and potential rewards that might be associated with blockchain and cryptoassets, it is necessary to understand what this new technology and new kind of asset is, so that is what the material in this paper attempts to do.

Background

In his 1981 inaugural address, President Ronald Reagan said words to the effect that government was not the solution, it was part of the problem.¹ This statement reflected a growing sentiment that big government could not be trusted. It was made at a time when libertarianism² was becoming an increasingly attractive philosophy for a growing segment of the American population. Many individuals with this mindset were looking for a variety of ways to escape from “Big Brother’s” watchful eye.

* Carol Goforth is a University Professor and the Clayton N. Little Professor of Law at the University of Arkansas (Fayetteville) School of Law. She has decades of experience with corporate, securities and business law issues in the U.S., and has recently published a number of articles and blog posts dealing with the regulation of cryptoassets. She is a frequent expert commentator for CoinTelegraph and serves as an advisor to Honeycomb Digital Investments. She is also the author of *Regulation of Cryptotransactions* (West Academic, 2020).

¹ *Reagan Quotes and Speeches*, ReaganFoundation.org (Jan. 20, 1981) (archived at <https://perma.cc/W7FH-RQTE>).

² *Libertarianism*, Stanford Encyclopedia of Philosophy (first published Sept. 5, 2002) (archived at <https://perma.cc/827Q-CPSK>).



A particular target of the belief that government was over-reaching was the banking industry. The federal Bank Secrecy Act,³ which had been adopted in 1970, required banks to keep tabs on their customers, verifying identities, monitoring accounts and activity, and reporting large or “suspicious” transactions back to the government.⁴ This put both financial institutions and the government in conflict with the long-held American notion that personal finance is a private matter in which the government has no legitimate interest.

There were two other powerful technological advances taking place at about this time. The more visible development involved the creation of the internet and its widespread adoption.⁵ Millions of computers were already using the internet when, in 1989, a software engineer at CERN, the Swiss particle physics laboratory, wrote a paper that laid the groundwork for what would become the world wide web.⁶ This, in turn, facilitated the growth of e-commerce and online shopping.⁷

The other development involved advances in computer cryptography, which is the study of hidden or secret messages or communication.⁸ Encryption transforms data or information into a code that cannot be decrypted without the appropriate parameters or keys. In the modern world, the process generally relies on algorithms to provide keys that are used both to encrypt and decrypt information. In communications between two parties known to one another, each party can be given a private key to encode and decode messages. However, as the volume of commercial internet transactions increased, so did the pressure to develop reliable encryption techniques that would work when the two parties did not have prior contact. Around the late 1990s to early 2000s, the use of public-key algorithms, relying on a public-private key pair, became popular.⁹

³ The Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 is generally referred to as the Bank Secrecy Act (BSA). It is codified at 31 U.S. Code §§ 5311 et seq.

⁴ Requirements for money services businesses can be found at https://www.fincen.gov/sites/default/files/shared/bsa_en_bank_reference.pdf.

⁵ Although it can trace its origins back to an academic research project in 1969, the internet really became a global commercial network during the 1990s. Timothy B. Lee, *The internet, explained*, Vox (May 14, 2015) (<https://www.vox.com/2014/6/16/18076282/the-internet>).

⁶ The paper was called “*Information Management: A Proposal*,” and it was authored by Sir Tim Berners-Lee. *History of the Web*, World Wide Web Foundation, <https://webfoundation.org/about/vision/history-of-the-web/>. A copy of Berners-Lee’s paper is archived at <https://perma.cc/5HBW-8BJY>.

⁷ *How eCommerce Industry Got Its Existence?* AgileInfoWays.com (Feb. 23, 2018) (archived at <https://perma.cc/VDB7-N26A>).

⁸ *Cryptography Definition*, KasperSky (archived at <https://perma.cc/LX8D-XB8B>).

⁹ Without getting too technical, a public key algorithm relies on there being both a public and corresponding private key. The public key can be known to the public (hence its name), while the private key is known only to the owner. To create a digital signature the private key creates an encrypted message that is decrypted with the public key. Anyone can thereby authenticate the sender’s claim of authority by using the public key. Alternatively, to send information, the public key is used to encrypt messages, while the private key decrypts them. For a far more detailed explanation, see *Private Key Pair*, Science Direct (archived at <https://perma.cc/SAM5-RAWK>), quoting Jeff Gilchrist, *Encryption*, in Encyclopedia of Information Systems (2003).

If you consider these three developments in tandem, you have an environment where growing numbers of people were suspicious of governmental oversight and interference in private matters; the internet had become omnipresent in the lives of many individuals; and there were new techniques for creating secret messages. The problem was how to leverage those developments to prevent the government from intruding into personal financial matters.

In the conventional world, most monetary transactions require the participation of banks or other money services businesses. When you earn a paycheck, it is rare in the modern world for payment to be in cash. You receive a check, which either needs to be cashed or deposited (either in person or electronically) into a bank account. In either event, a money services business, which may but need not be a bank, is involved. In addition, most of us do not like to carry around large sums of cash. Instead, we leave most of our income on deposit with a bank or other financial institution. We make payments with debit cards or write checks to cover our purchases and pay our debts. In all of these cases, the financial institution, usually our bank, stands in the middle, between us and the ultimate recipient of our hard-earned money. Increasingly, we use cash only for smaller transactions or not at all.¹⁰

Although we don't think of it in this way, when we "deposit" money in a bank, we are not really expecting the bank to keep those dollars right there for our convenience. In essence we are making a loan to the bank, and the bank keeps track of how much we have lent it. When we make a payment or withdrawal from our account, the bank keeps track of that as well. The bank is acting as a trusted intermediary or middleman, maintaining a record, or ledger, of all our transactions. Thus, if we try to spend more than we have on deposit, we get a notice of overdraft, and the payment is declined.

Maybe an example will make this clearer. Suppose I get a paycheck for \$1,000. It is electronically deposited into my bank account, which had a previous \$0 balance since I live paycheck-to-paycheck. The bank adds that \$1,000 to the ledger of transactions for my account. I then have a positive balance of \$1,000. Suppose at that point I write a check for \$1,000 to cover my mortgage payment. When the check is presented for payment, my bank will deduct that amount from my account. If I then try to write a check for or use my debit card to make my \$250 car payment, the bank will decline payment because its ledger shows that I have nothing left to cover that amount. The bank prevents me from showing all my creditors a mock-up of a balance sheet that I have created falsely claiming that I still have that \$1,000. My creditors don't trust me to have an accurate record of my finances; they trust my bank. My bank prevents me from double-spending my money.

The problem, for those who distrust government oversight and bank involvement, is how to use the rise of the internet and new developments in cryptography to create an alternative payment structure that does not involve banks or facilitate government oversight. Certainly, individuals are not always trustworthy, so what would enable a currency substitute that is not backed by a government and that

¹⁰ J. Andjelic, *Paper or Plastic? The Definitive List of Cash Versus Credit Card Spending Statistics*, Fortunly (Feb. 17, 2021) (<https://perma.cc/3H2W-KMAT>).



does not rely on banks as trusted intermediaries to function reliably? That is where the idea of blockchain and cryptoassets (originally conceived as and referred to as cryptocurrencies)¹¹ comes in.

How Blockchain Functions (in a non-technical sense)

The technological foundation for blockchain and cryptoassets was first publicized in 2008, in the form of a paper entitled “Bitcoin—A Peer to Peer Electronic Cash System,” which originally appeared in an online discussion of cryptography.¹² It was posted by a person or persons using the pseudonym “Satoshi Nakamoto,” although the real identity of the author remains a mystery.

This whitepaper describes a system that replaces the middleman (the bank), with a network of computers. In this structure there is no trusted intermediary at all. Instead, the computer software (which was intentionally made open source and therefore available to everyone) is downloaded to every computer whose owner wants to participate. All of the computers that join the network are referred to as nodes.

Transactions are processed as follows. A proposed transaction occurs, where I promise to pay a certain number of Bitcoins to another participant on the network (presumably in exchange for some other goods or service.) The software that has been downloaded onto the computers first verifies that I have the Bitcoins that I am promising to pay. It does this by automatically checking the record of prior transactions to make sure that I am the owner of sufficient Bitcoins, and then adding that transaction to the block of potential transactions being collected. All of these transactions are automatically verified as legitimate by the software, but the block is not yet entered onto the official ledger. At the end of every block, there is a difficult computational problem that is designed to take an average of ten minutes to solve. Nodes that are willing to devote resources to solving that problem are said to be “miners” because the first node that successfully solves the problem, broadcasts the solution to the network and is rewarded with a credit of a number of Bitcoins. The solution is quickly validated by the other nodes, and once accepted the block is added to the string of prior blocks of transactions. This kind of validation is known as “Proof of Work,” or

¹¹ In reality, there are lots of potential labels that have been used to describe what this paper calls cryptoassets. Originally they were cryptocurrencies because that was the original purpose of the new assets, but when additional functionality became possible commentators began talking about cryptocoins, cryptotokens, cryptoassets, digital or virtual assets, or even simply crypto as well as using cryptoassets to cover the range of assets that were being developed. Cryptocurrencies fell out of use because not all of these assets are designed as government (aka “fiat”) currency substitutes. Cryptotokens was confusing because some commentators used that as a label to describe the underlying programming structure, using cryptocoins to describe assets hosted on their own blockchain and cryptotokens to talk about assets that were hosted on a third party’s blockchain (typically the Ethereum network served this function). Digital and virtual assets seemed ambiguous because they do not necessarily reside on a blockchain at all, and because those terms have not gained widespread acceptance particularly in the global marketplace of ideas. Crypto is ambiguous because it is also the abbreviation used to refer simply to cryptography. The remaining option is the cumbersome but inclusive label: “cryptoasset.”

¹² Satoshi Kamamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, available online at <https://bitcoin.org/bitcoin.pdf>.



PoW consensus.¹³ It guarantees that the same block, with potential transactions occurring in the same order, is added to the record of transactions or ledger maintained by every computer in the network.

The name “blockchain” comes from the string of blocks of transactions that this process creates. The blockchain acts to replace the ledger that the bank keeps. It is decentralized because every node or computer in the network has access to the entire string of transactions (including those by every other party)¹⁴ rather than relying on a single, trusted intermediary like a bank. This is why blockchain technology is often referred to as a distributed ledger technology.

There is a lot of new jargon to get used to when learning about blockchain and cryptoassets. For example, the first transaction in a new block is the genesis transaction, and it contains the reward to the prior block’s successful miner. In some blockchains, not every node will have the full power to validate transactions. In those systems, there may be “master nodes” that have rights that other nodes do not. There are other consensus protocols besides PoW for blockchains other than the one on which Bitcoin resides. There are numerous other terms and concepts that would be necessary for a full understanding of blockchain, but this should at least give a preliminary basis for understanding how the technology itself works. The issue of how individual owners of cryptoassets prove ownership and arrange for transfers adds a different layer of issues.

Understanding Bitcoin: The Basics

Cryptoassets are a purely digital asset which means they are nothing more than a string of numbers. If you have paid attention to the news about Bitcoin, it may seem incomprehensible that a string of numbers, backed by no government, no bank, and no company, has been trading at prices up to \$64,000.¹⁵

On the other hand, why do we value a dollar bill? You cannot eat it, wear it, shape it into anything useful, or use it for anything other than a store of value, unit of account, or medium of exchange.¹⁶ It is not backed by any particular store of gold or other assets. We merely “trust” that the government will not print so much new money that our dollar bills become essentially worthless through hyperinflation. Because we have this trust, and because our government mandates that official currency be accepted as legal tender, we accept dollar bills (and other legal currency) in exchange for goods and services. The value that we give to it, however, reflects what we (collectively) think that dollars are worth.

¹³ For a more detailed explanation of the PoW consensus protocol, see Andrew Tar, *Proof-of-Work*, CoinTelegraph (Jan. 17, 2018) (archived at <https://perma.cc/NQ8Q-AQBT>).

¹⁴ The transactions are identified only by an “address,” a unique identifier that serves as a virtual location to which a cryptoasset may be sent. Bitcoin addresses are generally used only in a single transaction.

¹⁵ Bitcoin prices can be easily tracked through a number of websites. I tend to use CoinMarketCap.com, which as of May 1, 2021 lists \$64,863.10 as the all-time high for a single Bitcoin. That price was reached on April 14, 2021. (To access historical information about Bitcoin pricing, click on that particular cryptoasset and then look at information on the right-hand side of the page, clicking “show more” to see the all-time high.)

¹⁶ These are the traditional attributes of “money.” See *Money*, Merriam Webster (online) at <https://www.merriam-webster.com/dictionary/money>.

Similarly, cryptoassets also reflect what we think they are worth. The first reported real-world transaction involving Bitcoins occurred in 2010, when 10,000 Bitcoins were used to pay for two pizzas.¹⁷ Assuming the pizzas had a value in dollars of \$30 (\$15 each), this would have put the value of a single Bitcoin at approximately 1/3 of a penny.

Since that time, there have been enough people who have believed in the potential of Bitcoin to increase the value of the asset dramatically. The current market value simply reflects what people are willing to pay for Bitcoin (or other cryptoassets) today. As provided in the original software, there is a cap on the total number of Bitcoins set at 21 million. New Bitcoins are created every 10 minutes, but the reward is halved approximately every four years,¹⁸ and eventually all available Bitcoins will be issued.¹⁹ In other words, the supply of Bitcoin is finite, helping to create upward pricing pressure.

Many Bitcoin purchasers are clearly buying on speculation, in the hope that there will be additional increases in the price over time. In fact, Bitcoin has become so popular that its total market capitalization (the value of all issued Bitcoins at current valuation) exceeds a trillion dollars.²⁰ Even traditionally conservative banking institutions like Deutsche Bank have concluded that Bitcoin is too big to ignore.²¹ There are now a number of businesses that will accept payment in Bitcoin.²² So how does a Bitcoin payment take place? Understanding the answer to that question requires understanding how Bitcoin ownership works.

Cryptoassets essentially function using three fundamental pieces of information. The first is an address,²³ which is associated with a balance. That address is used for both sending and receiving funds. The address is, in turn, associated with public and private keys that are part of the encryption process. The public key can be known to the public (hence its name), while the private key is known only to the owner. To create a digital signature the private key creates an encrypted message that is decrypted with the public key.

¹⁷ Aaron Hankin, *Bitcoin Pizza Day: Celebrating the \$80 Million Pizza Order*, Investopedia (updated Jun 25, 2019) (archived at <https://perma.cc/ZRH6-DMYT>).

¹⁸ The original reward for mining was 50 Bitcoins, but that amount was halved to 25, then to 12, and then to 6.25 Bitcoins on May 11, 2020. *Bitcoin-halving 2020: What you need to know*, CMCMarkets (archived at <https://perma.cc/PEY2-JEUJ>).

¹⁹ The last Bitcoin is likely to be mined in 2140. Daniel Phillips & Scott Chipolina, *What Will Happen to Bitcoin After All 21 Million are Mined?* DeCrypt (Ap. 20, 2021) (archived at <https://perma.cc/PR48-C9ZE>).

²⁰ See Bitcoin Chart, <https://coinmarketcap.com/currencies/bitcoin/>.

²¹ Helen Partz, *Bitcoin is now ‘too important to ignore’, Deutsche Bank says*, CoinTelegraph (Mar. 19, 2021) (archived at <https://perma.cc/88PF-8Q7F>).

²² For a list of U.S. companies accepting Bitcoin payments as of early 2021, see Ofir Beigel, *Who Accepts Bitcoin as Payment*, 99Bitcoins (updated Jan. 17, 2021) (archived at <https://perma.cc/FBU4-7MXW>).

²³ To obtain the unique alphanumeric sequence that serves as a location to which proof of ownership of a cryptoasset can be sent, you will need a crypto wallet. This is software that allows the owner to send, receive and prove ownership of a cryptoasset. Wallets create new addresses every time the owner generates an invoice or receives a payment request.

Anyone can thereby authenticate the sender's claim of authority by using the public key. Alternatively, to send information, the public key is used to encrypt messages, while the private key decrypts them.

Because Bitcoin and other cryptoassets have no physical form, they cannot actually be stored anywhere. Nonetheless, to claim ownership of these assets you need a crypto wallet. Instead of storing the cryptoassets, these wallets store information and in particular the private key needed to access Bitcoin addresses. Loss of the private key will essentially render the corresponding assets inaccessible, which has resulted in some very high-profile stories about individuals and businesses "losing" Bitcoin and other cryptoassets.²⁴

Instead of keeping track of their own private keys, some Bitcoin owners choose to have a wallet service or crypto exchange maintain custody of their assets (or technically, control over their assets, by having the private keys that access the relevant addresses).²⁵ Exchanges are major targets for hackers,²⁶ so if you are leaving your assets in the control of these services you need to be certain that they are large, reputable, and ideally protected in some manner such as through insurance.²⁷

Other Cryptoassets

The preceding information has focused on Bitcoin, which was the original cryptoasset. There is, however, nothing that limits the use of cryptoassets formed with blockchain technology to serve as a substitute for currencies. In fact, while the first several cryptoassets following Bitcoin were generally designed as alternatives to Bitcoin (and therefore earned the label of "altcoins," shorthand for alternative coins), cryptoassets have now been designed with a large range of potential uses in mind. For example, there are cryptoassets that represent ownership of a portion of a commodity, assets that serve as collectibles,

²⁴ For example, in 2019 the death of the only holder of private key for a Canadian crypto-exchange resulted in the reported loss of access to \$145 million (USD) worth of crypto. Jeffrey Gogo, *Canadian Exchange Insolvent After CEO Allegedly Dies With Keys*, Bitcoin.com (Feb. 2, 2019) (archived at <https://perma.cc/7RZ4-B9VL>). Another widely circulated report indicated that a lost password has compromised the ability of a private owner to recover approximately \$220 million in Bitcoin. Frances Mulraney, *Computer programmer has just two guesses left for his password to access \$220m in Bitcoin before digital wallet locks FOREVER*, Daily Mail.com (Jan. 12, 2021) (archived at <https://perma.cc/868L-YLB6>).

²⁵ For example, you can have exchange services such as Coinbase, Binance, or Gemini store your cryptoassets. In fact, this is a necessity if you are activity trading. See David Kemmerer, *The Best Places to Store Your Cryptocurrency*, Cryptotrader (Ap. 3, 2021) (archived at <https://perma.cc/GAY7-NPKX>).

²⁶ For a depressingly long list of exchange hacks from 2011 to 2020, see *A Comprehensive List of Cryptocurrency Exchange Hacks*, SelfKey Blog (Feb. 13, 2020) (archived at <https://perma.cc/W3QR-Q68R>).

²⁷ One recent example of the risks of dealing with a less reputable exchange involves the Turkish exchange Thodex, which suddenly went offline in late April 2021 with the CEO allegedly disappearing with hundreds of millions of dollars in cryptoassets. Sandali Handagma & Jamie Crawley, *Turkish Crypto Exchange Goes Offline, CEO Missing*, CoinDesk (Ap. 22, 2020) (archived at <https://perma.cc/2ME7-7CJ7>). Compare this with Coinbase, which insures its online bitcoins. "At Coinbase, we're committed to security by using industry best practices and storing up to 97% of bitcoins in encrypted, geographically separated, offline storage. To further protect our customers, all of the bitcoins stored in online computers are insured." *Is Bitcoin secure? Has this network ever been hacked?*, Coinbase Help (archived at <https://perma.cc/WE2X-Z7KY>).

assets that document membership or provide identity verification, in addition to other possibilities. Blockchain technology can also enable businesses to create systems that act as a marketplace to facilitate transactions, improve operational efficiencies, trace ownership or otherwise.

As an example of a cryptoasset that represents ownership in an underlying commodity, the Digix Gold Token (DGX) is a digitally tradeable form of gold.²⁸ One DGX represents a single gram of gold, in a digital asset that is readily divisible, easily transferable, and extremely secure. Other examples include efforts to tokenize crude oil²⁹ and bananas.³⁰

Cryptoassets that serve as collectibles are not like cryptocurrencies or other cryptoassets where each such asset is identical and interchangeable. Known as Non-Fungible Tokens (NFTs), crypto collectibles contain unique identifiers and rights. Thus an NFT generally represents “ownership” of a particular digital asset, with no other cryptoasset containing exactly the same content. Although Cryptokitties were the first NFTs to gain widespread popularity,³¹ probably the most notorious example is “Everydays: The first 5000 days,” a work created by digital artist Beeple which sold in March 2021 for \$69.3 million.³²

As for an example of a cryptoasset that is used to document membership, consider chiliZ, a cryptoasset hosted on the Ethereum blockchain used to fund activity on the Socios.com platform.³³ Fans of participating teams use their chiliZ to buy fan tokens associated with participating sports teams. Owners of the applicable “fan tokens” can then vote and engage in club decisions as posted by Socios.com, with their ownership demonstrating membership in the applicable club’s fan base.

The goal for blockchain-based businesses designed as a marketplace is generally to create more efficient coordination between potential suppliers and customers. Storj³⁴ is a startup that falls into this category. It is designed to facilitate transactions between those with excess digital cloud storage and others who desire additional capacity to securely store digital information. Storj also coordinates payment between the parties.

²⁸ *The future of owning gold is digital*, DiGix (archived at <https://perma.cc/7LBN-4QA4>).

²⁹ The Venezuelan Petro was to be backed by the country’s oil reserves. Leon Markovitz, *Venezuela’s Petro Cryptocurrency Is a Gift to Future Generations*, CoinDesk (Sept. 2, 2018) (archived at <https://perma.cc/286V-QBJM>).

³⁰ The amusingly named bananacoin was offered for sale in 2017, ostensibly to expand an environmentally friendly banana plantation in Laos. Bananacoin. "White Paper Bananacoin," (archived at <https://perma.cc/7V6Z-RMCD>) at pp. 3-11. On the other hand, there have no significant recent updates to the project website, and the cryptoasset does not appear to trade on any major crypto exchange. *Bananacoin*, Investopedia (Ap. 13, 2021) (archived at <https://perma.cc/HEM3-WQNA>).

³¹ Samuel Haig, *Surprise CryptoKitties Drop Overwhelms Winklevoss-Backed Exchange*, CoinTelegraph (May 15, 2020) (archived at <https://perma.cc/N5GP-XHT6>).

³² Sam Bourgi, *Beeples NFT auction closes at record-setting \$69.3M*, CoinTelegraph (Mar. 11, 2021) (archived at <https://perma.cc/49HV-FFU5>).

³³ *Chiliz Exchange Review*, Cointelligence (archived at <https://perma.cc/ZY5F-7JF3>).

³⁴ *Decentralization Delivers Better Security & Privacy*, Storj <https://www.storj.io/how-it-works>.

Many of the cryptoassets designed to improve operational efficiency do so in the world of currency exchange. Ripple's XRP token, for example, is designed to reduce transaction costs and delays particularly in transnational financial exchanges.³⁵ Similarly, OmiseGo's OMG token allows merchants to accept payments through China's ALIPAY supporting a large number of international currencies.³⁶

One of the most compelling use cases for blockchain has been in source tracing in supply chain applications. As explained by some of its proponents, "Blockchain can greatly improve supply chains by enabling faster and more cost-efficient delivery of products, enhancing products' traceability, improving coordination between partners, and aiding access to financing."³⁷ In 2020, diamond, gold, tea, coffee, beverage, food, and automotive industries have all at least started testing blockchain-based supply chain applications.³⁸ These projects are designed to improve efficiency, accuracy, reliability, transparency and security of the supply chains in these areas.

What does all of this have to do with Agriculture?

Very little of this (aside from the very last point just made) relates directly to agriculture, but that does not mean that blockchain and cryptoassets are irrelevant to farmers, ranchers, agribusinesses, and others involved in agricultural enterprises. The potential benefits of blockchain applications in the agricultural sphere are varied and potentially profound. A distributed, decentralized ledger on the blockchain offers potential benefits of improved transparency and trustworthiness, immutability which decreases the risk of fraud and counterfeit claims regarding origin or pricing, improved ability to detect delays and malfunctions, enhancement of food quality and safety, and increased efficiencies both through the avoidance of costs and delays associated with intermediaries but also through faster communication that can help limit food waste.³⁹

One report has suggested that the positive potential of blockchain in agriculture includes the promise of:
...a reliable source of truth about the state of farms, inventories and contracts in agriculture, where the collection of such information is often incredibly costly. The blockchain technology can track the provenance of food and thus helps create trustworthy food supply chains and build trust between

³⁵ Ripple, *XRP: The Best Digital Asset for Global Payments* (archived at <https://perma.cc/A63X-V2NZ>).

³⁶ OmiseGo, *OMG Network* (archived at <https://perma.cc/XAF4-GS38>).

³⁷ Vishal Gaur and Abhinav Gaiha, Building a Transparent Supply Chain, Harv. Bus. Rev. (May-June 2020) (archived at <https://perma.cc/FX47-WZMU>).

³⁸ Who's Using Blockchain in 2020, and How? Logistics Bureau (Jul. 28, 2020) (archived at <https://perma.cc/CZT7-J9AD>). This source highlights Walmart's blockchain projects in food supply chain traceability. Other businesses named in this source as being involved in blockchain efforts in regard to food and agricultural products include the IBM Food Trust, the Norwegian Sea Food Association, Anheuser-Busch Inbev, the Coffee Board of India, and Unilever (for its tea plantations).

³⁹ It has been noted that the benefits of blockchain could go "a long way towards reducing the Value in Bulk commodities is lost due to inefficient supply chains and intermediaries, currently estimated to be 30% in Western economies and 50% in the developing world according to the United Nations, Food and Agricultural Organization." Caile Ditterich, *How agriculture can benefit from blockchain*, The Global Treasurer (May 9, 2018) (archived at <https://perma.cc/R7U6-EMS4>).



producers and consumers. As a trusted way of storing data, it facilitates the use of data-driven technologies to make farming smarter. In addition, jointly used with smart contracts, it allows timely payments between stakeholders that can be triggered by data changes appearing in the blockchain.⁴⁰

Individual farmers, ranchers, or those involved in various agribusinesses may, of course, contemplate other actions relating to cryptoassets. They may be considering investment in one or more of the existing forms of crypto.⁴¹ They may want to investigate the feasibility of accepting cryptoassets as payment for their agricultural products.⁴² They may also want to consider whether to create their own cryptoassets, which might serve as ownership in part of what they are currently producing or which might relate to a different aspect of their operations.⁴³

Conclusion

This is the first of three papers in a series, and as such it is only designed to introduce readers to the nature of blockchain and cryptoassets. It may therefore have raised more questions than it has answered.

The second paper in the series will look at practical and legal issues in connection with the potential use of blockchain technologies and cryptoassets, including how they are regulated (with a particular focus on U.S. law). The third paper will examine some of the current blockchain initiatives and operations focused on agriculture, with the goal of introducing readers to the range of current opportunities and options.

⁴⁰ Hang Xiong et al, *Blockchain Technology for Agriculture: Applications and Rationale*, Frontiers in Blockchain (Feb. 21, 2021) (archived at <https://perma.cc/6WFF-RAMU>).

⁴¹ A decision of whether to invest in a cryptoasset implicates a host of other issues. First, the cryptoasset and its creator or issuer need to be researched. Claims need to be verified, and there should be a consideration of whether the issuance has been incompliance with applicable law. The ease of resale should be considered, which means looking at which exchanges might list and allow trades in the asset. Pricing information and whether the value is susceptible of manipulation will also need to be considered. Finally, there will be tax issues because the IRS currently requires taxpayers to pay either ordinary income or capital gains tax on any gains, depending primarily on how long the asset has been held prior to resale or exchange.

⁴² There are a number of issues to consider before doing this. First, cryptoasset prices are volatile so the value of what is received is far from certain even over a few days, and sometimes over a few hours. Second, there are difficult tax and accounting issues to consider, which require input from a tax advisor familiar with the particular circumstances of the person considering accepting cryptoasset payments. In addition, there will be a cost to converting the cryptoasset to fiat currency which is likely to be required in order to enter into most subsequent financial transactions.

⁴³ This would be the most complicated of options, because at the current time cryptoassets are heavily regulated by a variety of federal agencies. The IRS treats cryptoassets as property and considers transactions in such assets to be the equivalent of taxable barter arrangements. The Securities and Exchange Commission tends to regard most cryptoassets as securities, requiring registration or compliance with an exemption under federal law, which generally requires the assistance of sophisticated securities counsel as well as the expense and inconvenience of compliance. A business assisting in the transfer of cryptoassets may be treated as a money services business by the Financial Crimes Enforcement Network, meaning that the business might have to register and comply with various onerous record-keeping and reporting requirements under the federal Bank Secrecy Act. At the very least, competent legal advice is essential before there is any attempt to create and issue a new form of cryptoasset.

The information contained in this document is provided for educational purposes only. It is not legal advice, and is not a substitute for the potential need to consult with a competent attorney licensed to practice law in the appropriate jurisdiction.

