K2's Emerging Topics In Blockchain And Cryptocurrency

Session Description

Blockchain is one of the most-watched emerging technologies. Yet, few accountants understand how to use this technology to make existing ledger-based systems more efficient, effective, and tamper-resistant. In this session, you will learn the basics of blockchain-based ledgers. You will also learn about the fundamentals of cryptocurrencies such as Bitcoin and Ripple.

Additionally, you will learn about emerging issues in these fields, such as stablecoins, central bank-issued digital currencies, smart contracts, and sovereign identity management. By attending this session, you will see how blockchain-based technologies will change your work with others.

Learning Objectives

- Select the correct definitions for key terms associated with blockchain-based ledgers

- Differentiate the features of a cryptocurrency, a stablecoin, and a central bank-issued digital currency

- Identify key features associated with a smart contract, distributed finance, and sovereign identity

- Select from a list at least three different uses for blockchain-based ledgers covered in the session

This Session

- Blockchain Basics
- Bitcoin, Altcoins, and Stablecoins
- Smart Contracts and Initial Coin Offerings
- Central Bank Digital Currencies
- Non-Fungible Tokens
- Decentralized Finance (DeFi)
- IRS Operation Hidden Treasure\
- Ledgible Tax Pro

BLOCKCHAIN BASICS

What Is A Blockchain?

- A **blockchain** is a theoretically incorruptible ledger of transactions made up of **blocks**, or files, which secure the **transactions** against alteration. Transactions are affected with one-time passwords called "tokens" which are created when a transaction is recorded.

- How is blockchain used in practice?
  - A blockchain-based ledger can be used to create an inalterable transaction record for many things
    - Bitcoin (and other virtual currencies)
    - Private company stock ledger
    - Medical records
    - Insurance policy register
   - Real estate transactions

Blockchain Uses

- While some think of blockchain exclusively as the engine behind cryptocurrencies like Bitcoin and Ethereum, the blockchain protocol has many other uses, and can be configured to offer anonymity and run on a decentralized basis

- Uses for Blockchain include
  - **Cryptocurrencies** (Bitcoin, Ethereum, Ripple, etc.)
  - Recording permanent records like **land transfer records**
  - **Private company stock ledgers**
  - **Smart contracts**, where funds/title/payments can be linked to an objectively verifiable event (like a stock price, stock index, or sports score) and funds automatically transferred when the conditions are met

Blockchain-Secured Stock Ledger

- Is an option now in [Delaware](#), [Italy](#) (LSE), and elsewhere

- The stock ledger is maintained by a service provider like IBM which maintains the ledger on behalf of the private company

- Since the blockchain is maintained by a single entity, it may be possible to recover lost keys to stock certificates
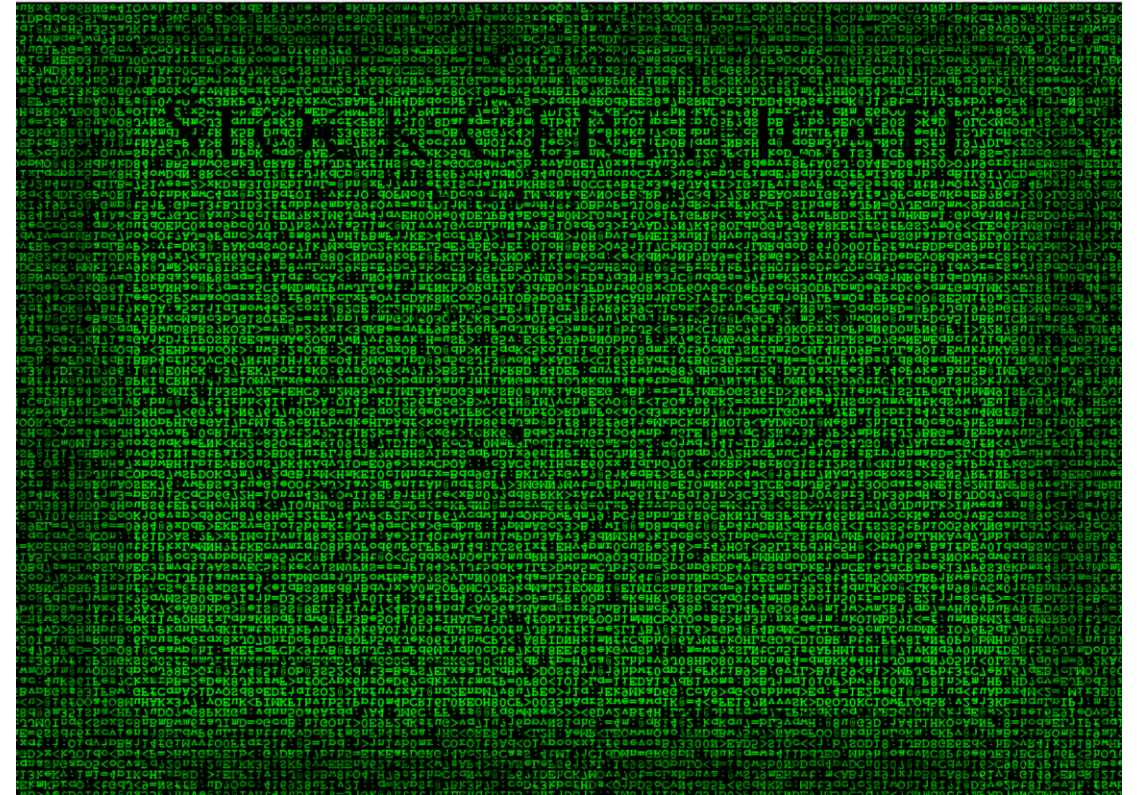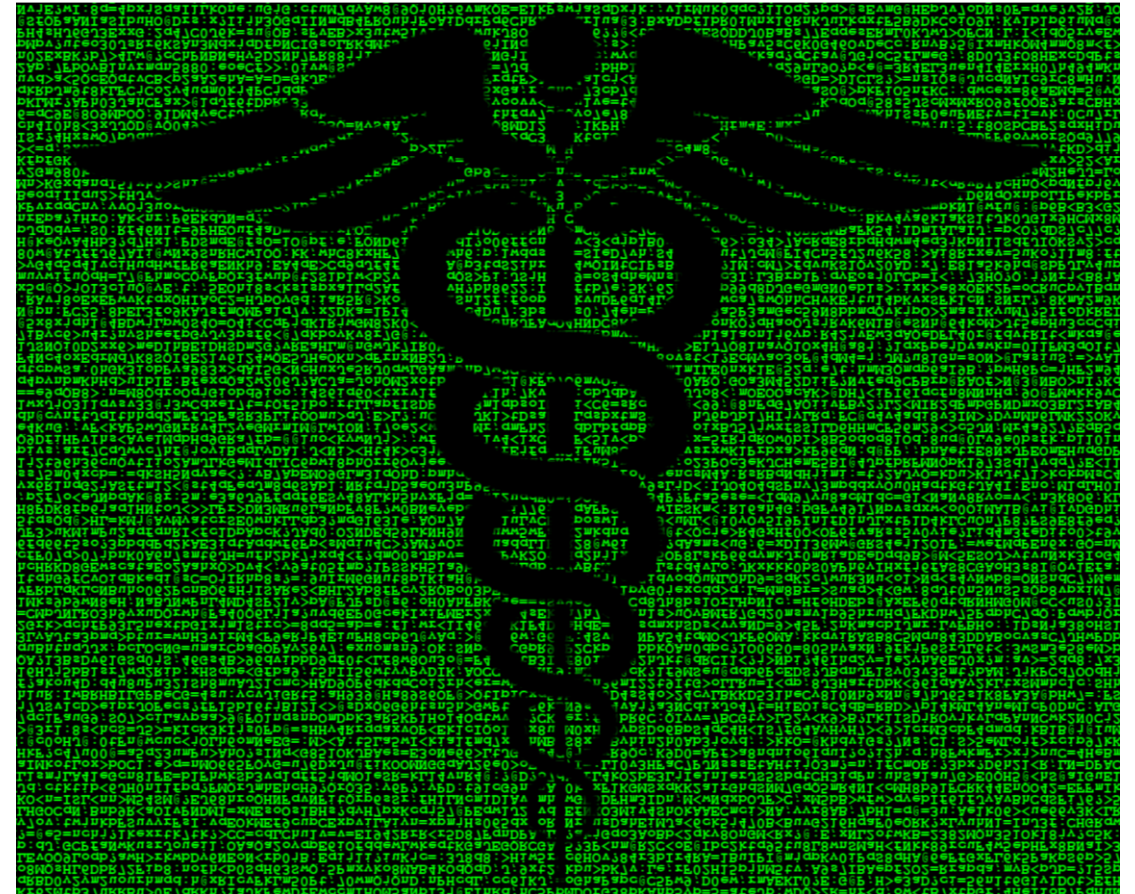
Medical Records

- Creates secure, distributed, tamper-proof medical record database on private servers

- Proposed by [MIT Media Lab in the MIT Technology Review](#)

- A company called [MedicalChain](#) is creating an electronic health record based on blockchain

- Healthcare providers can have an offline copy of the records

Virtual Currency

- Blockchain is the core of all major cryptocurrencies, including Bitcoin, Ethereum, Litecoin, Monero, Ripple and Zcash (shown to right)

- The blockchain protocol is how users can stop someone from "double spending" virtual currency

- Canadian central bank ran a test with a virtual currency backed by real $CAD
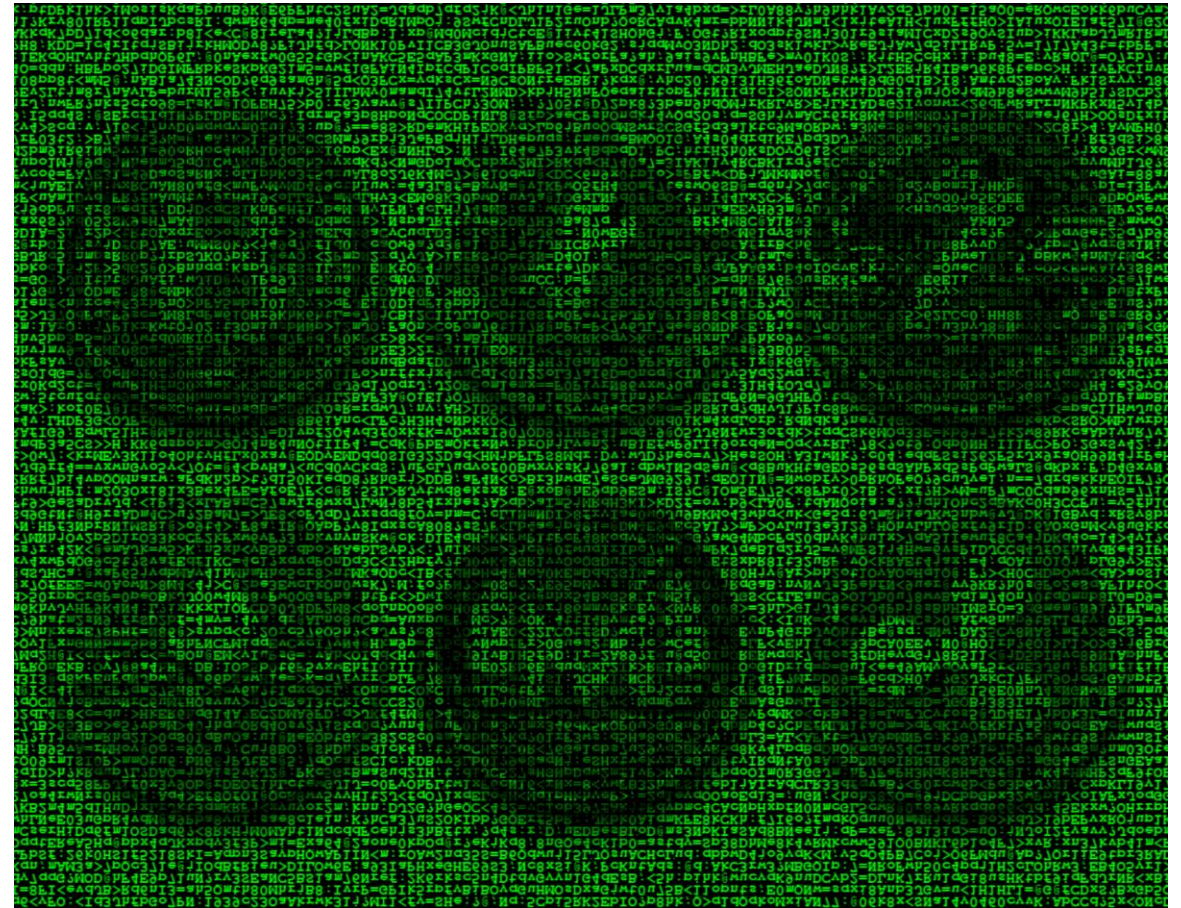
Fundamentals Of Blockchain

- There are at least five fundamental concepts you must understand which are used together to create a blockchain

- Those major concepts are:
  - **Transactions**
  - **Blocks**
  - **Wallets/Keys**
  - **Nodes/Miners**
  - **Hashes**

- While there are many other advanced concepts (proof of work, proof of stake, difficulty level, public vs. private, and many others), we will start here

Poe's "The Cask of Amontillado"

Fundamentals Of Blockchain: TRANSACTIONS

- Records which are to be included in the ledger and transfer the rights associated with something to someone else – like any other ledger, a blockchain-based ledger is designed to track transaction activity

- A transaction represents anything you could record in a ledger – it could be a journal entry, a payment, a transfer of shares of stock, a medical record, or any other kind of record you might store in a ledger

- Transactions are validated by the "Nodes" or Miners before they are assembled into the blocks (batches) used to record them

Fundamentals Of Blockchain: BLOCKS

- A **BLOCK** is a permanent, incorruptible group of transactions which are bundled together and confirmed as unique, valid, and authorized

- **BLOCKS** are groups of transactions which are combined on an end to end basis to create a permanent, unalterable transaction ledger/database

- The process of assembling transactions into "blocks" is done by **MINERS/NODES** who calculate all of the checksums needed to arrange a group of new transactions into a **BLOCK** of new transactions to be added to the blockchain

Fundamentals Of Blockchain: BLOCKS

- A checksum of all transactions in the new block, the new block number, and the true and correct checksum of all previous blocks in the blockchain is included in each new block in the blockchain

- This appending of blocks to one another is why a group of blocks is called a "blockchain", and cryptography is used to make the blockchain very tamper evident using current computer technology

- The blockchain which underlies the cryptocurrency Bitcoin has controls in place which record roughly 2,016 blocks in every two week period – or a new block approximately every ten minutes
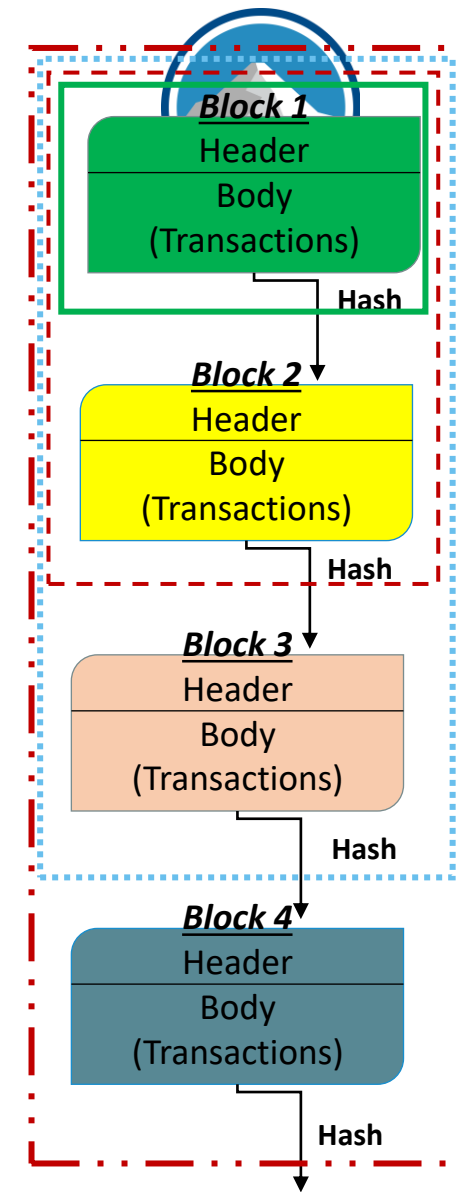
Fundamentals Of Blockchain: WALLETS/KEYS

- A **KEY** is a unique secret password (really an encryption key) associated with the ownership of an asset like a unit of cryptocurrency or shares of stock, or which permits recording data in the blockchain-based ledger

- Private keys are stored in a **WALLET**, an application which allows the user to record permitted transactions in the blockchain-based ledger

Fundamentals Of Blockchain: MINERS/NODES

- **MINERS/NODES** are computers which are part of the network which does the work to validate transactions and combine them together into blocks

- This is called "mining" in the cryptocurrency world, and represents the computing workload required to store, operate, and maintain the blockchain-based ledger in real time

- The mining can be done on a **centralized** basis, it can be done by a **decentralized** private group of computers, or it can be done by decentralized volunteers from the public at large

Fundamentals Of Blockchain: MINERS/NODES

- **MINERS/NODES** are validated by using public/private key-based digital signatures which are created by a user's wallet and then sent to a miner for recording

- Some **MINERS** offer to buy and sell units of a cryptocurrency in exchange for traditional government-backed currencies – these miners are called **EXCHANGES**

- **EXCHANGES** are classified as money services businesses by most governments and must follow the related laws and regulations
  - To register as an exchange with the U.S. Government usually takes about 18 months and costs around $1.5 million
  - Exchanges can (and do) charge fees for their services

Fundamentals Of Blockchain: HASHES

- Hashes are calculations which are a type of checksum or unique signature that positively identifies some data
  - A hash total of invoice numbers in a batch-oriented accounting system is an example of a hash
  - The check digits/check formulas which can be used to determine if an ABA routing number or a credit card are valid are also examples
- ***Hashing is a way of creating a one-way signature associated with an item which uniquely identifies the item while simultaneously obscuring it from use by others***

Fundamentals Of Blockchain: HASHES

- For example, passwords in Linux are typically obscured by being stored in a hashed format in a file called /etc/passwd
  - Linux doesn't actually store the password itself, it stores the hash of the correct password and compares it to the hash of the password which is entered
  - If the hash of the password entered matches the one which is stored, the user is validated
  - It is easy to calculate a hash associated with an input like a password, but virtually impossible to infer, or back into the password from the calculated hash value
- There are many different hash algorithms (calculation methods/formulas)
- Some of the more common ones are SHA1, SHA256, Rijndael, and Blowfish

What's A Hash, Anyway?

- Cryptographic hash functions are formulas which convert data of variable length to a data type of fixed length

- They are designed to optimally calculate a unique result for each possible input string of data, while at the same time making it near impossible to reverse engineer the input string from the resulting hash total

- Check digits are a very simple kind of check function which can be used to validate that something like an account number meets the rules for a particular number type

What's A Hash, Anyway?

- Although it is believed to be mathematically possible for most hash functions to return the same result for two different strings of data, it is exceedingly difficult, and some believe to be impossible under most circumstances
  - This condition is called a **hash collision**
- The number of calculations required to consider all of the possible combinations of characters and then recalculate the related hashes on these combinations to find an equivalent string of data would be near impossible on current computer hardware
- …although in the long term, quantum computing may provide the computing horsepower needed to solve these currently unsolvable problems

K2 Enterprises

What's A Hash, Anyway (Continued)

- For example, your bank's nine-digit routing number has to comply with a check digit formula to prevent accidental miskeying

- The formula is as follows:
  - $3(d_1+d_4+d_7) + 7(d_2+d_5+d_8)+(d_3+d_6+d_9) = x$
  - X must be evenly divisible by 10.

- If a bank's routing number was 064207195, the calculation would be:

  X=3(0+2+1)+7(6+0+9)+(4+7+5)

  X=3(3)+7(15)+16

  X=9+105+16

  X=130, which is divisible by 10, so the check formula works.

Checksum Formulas In ABA Routing Numbers

Formula: $3*(d_1 + d_4 + d_7) + 7*(d_2 + d_5 + d_8) + (d_3 + d_6 + d_9)$

Formula result must be divisible by 10

Routing No	1	2	3	4	5	6	7	8	9	Value	Pass/Fail
064207195	0	6	4	2	0	7	1	9	5	130	PASS
064000017	0	6	4	0	0	0	0	1	7	60	PASS
021001486	0	2	1	0	0	1	4	8	6	90	PASS
021272655	0	2	1	2	7	2	6	5	5	130	PASS
022000868	0	2	2	0	0	0	8	6	8	90	PASS
031100209	0	3	1	1	0	0	2	0	9	40	PASS
091408983	0	9	1	4	0	8	9	8	3	170	PASS

Near Identical Text Has Dissimilar Hashes

We the **People** of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.

Version #1   **Version #2**

We the People of the United State | We the people of the United States,

MD5: 26a981554d7d761230bc7ef3a6645375   **MD5**: fe0dcdc1f3bb6be9e3bdfd708283db51

Hash Value Comparison – One Character Difference Between Two Samples

People	
Adler32	ac6b76e6
CRC32	4632e4a8
Haval	1c5e1a657fc874e460b844a4cd934e18
MD2	71e738565b00c9bb557ed5bb3649d456
MD4	24f41137e6177b312b4b46b6b433d72d
MD5	26a981554d7d761230bc7ef3a6645375
RipeMD128	729c97cc927d20e396265f22bc6443c6

people	
Adler32	d46b7706
CRC32	4e395b69
Haval	f40df0b70f8368edac927b9ffbee2dba
MD2	da338055d688c170d4251e6dd3838705
MD4	aac76560902079aa71f95277542aa216
MD5	fe0dcdc1f3bb6be9e3bdfd708283db51
RipeMD128	d6b8bd2aa7609c7749c9209bc2059cea

Where Is Blockchain Needed?

- Places where items need to be stored in a <u>tamper-evident ledger and marked with a time stamp</u>
  - Insurance policy binder issuance
  - Time-sensitive acceptance of offers (e.g. real estate contract acceptance)
  - Bank account transactions
- Places where the parties who don't know each other need a way to trust each other and have forensically unalterable tamper-evident data storage
  - Supply chain - lets parties like manufacturers, common carriers, and purchasers collaborate with forensically sound protocols to validate that parties have met their obligations under contracts – could replace bankers acceptances, etc.
- Places where the <u>sequence in which records are recorded is important</u>
  - Deeds/title to real estate
  - Liens against assets

BITCOIN, ALTCOINS, AND STABLECOINS

Bitcoin

- The first use of blockchain digital ledger technology and the most common cryptocurrency in the market today

- Applies blockchain technology to the problem of how to create, buy, sell, exchange, and store digital money which is stateless and not asset-backed

- The bitcoin ledger tracks the ownership of all outstanding bitcoins and represents a permanent record of all related transactions

Bitcoin (continued)

- As of 10/10/2021, the market cap of all outstanding Bitcoins was $1.04 trillion (of a total global crypto market cap of $2.32 trillion)
  - Current price is $55,467.45/coin (10/10/2021)
  - Circulating supply is 18,840,075 (10/10/2021)
- Experts estimate that up to 1/3 of all bitcoins are unusable/irretrievable due to the owner's failure to back up the private keys in their digital wallets
- **Website**: Bitcoin.org

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.
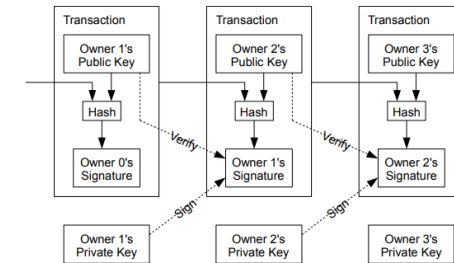
The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

Want to know more? Read the white paper that created the blockchain technology used in Bitcoin

Altcoins

- The name used for any alternative cryptocurrency other than Bitcoin

- Applies blockchain technology to the problem of how to create, buy, sell, exchange, and store digital money

- Many altcoins modify how the blockchain protocol is implemented to maintain the records of their transactions
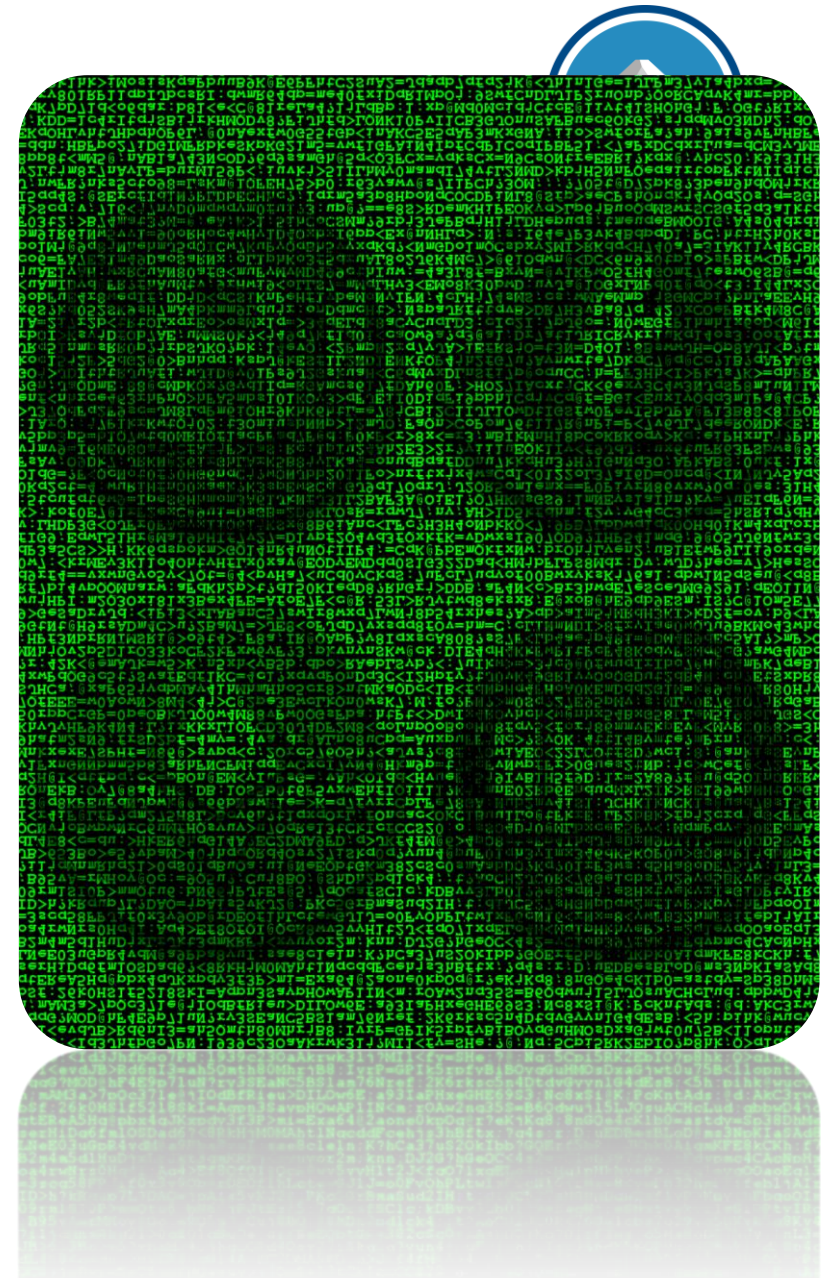
Altcoins (continued)

Some of the common attributes of Bitcoin modified by altcoins include:

- **Asset backed** – Some altcoins are backed by a pool of financial assets held in trust, while others are not backed by anything

- **Stablecoins -** Certain altcoins are designed to have less volatile price swings and have a targeted asset value which closely follows the value of a traditional currency (e.g. USD, EUR, etc.) or a market index

- **Supply of Coins** - While Bitcoin has a fixed formula that steadily increases the number of coins over time, some coins are open-ended and can have an infinite number of units

- **How Coins are Mined** - Bitcoin's open "proof of work" mining algorithm allows anyone to mine bitcoins and validate transactions in the ledger, but there are other mining methods such as "proof of stake", pre-mined altcoins, and privately maintained ledgers

Altcoins (continued)

Some of the common attributes of Bitcoin modified by altcoins include:

- **Centralized vs. Decentralized** - Ledgers can be centrally controlled by an organization or a centralized server, or they can be decentralized, "headless" ledgers which operate according to a set of rules programmed into a mining software application

- **Open vs. Closed Records** – While anyone can review every balance, block, and transaction in a public blockchain, there are also privately maintained blockchains which are used to record data which are not visible or accessible by the public (e.g. investment ownership, private company stock ledgers, etc.)

- **Central Bank Digital Currency (CBDC)**– An altcoin which is issued by the central monetary authority of a nation

Stablecoins

- **Stablecoins** are cryptocurrencies that attempt to tether their value to the value of a reserve asset (USD, gold)
- Think of a stablecoin as being somewhat analogous to a money market fund
- Most stablecoins are backed by either assets held in collateral or through algorithmic buying and selling of the reference asset or related derivatives
- Some common stablecoins are USDCoin, Tether, TrueUSD
- Any discussion of regulation of cryptocurrencies inevitably mentions stablecoins, as they could easily be used to launder money from illicit activities, and it would be very difficult to trace the source

SMART CONTRACTS & INITIAL COIN OFFERINGS

Smart Contracts

✓ A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce a negotiation of a contract

✓ They allow the performance of credible transactions without third-parties

✓ All transactions are trackable, enforceable and irreversible

✓ Many, but not all, use the Ethereum blockchain for recordkeeping and processing
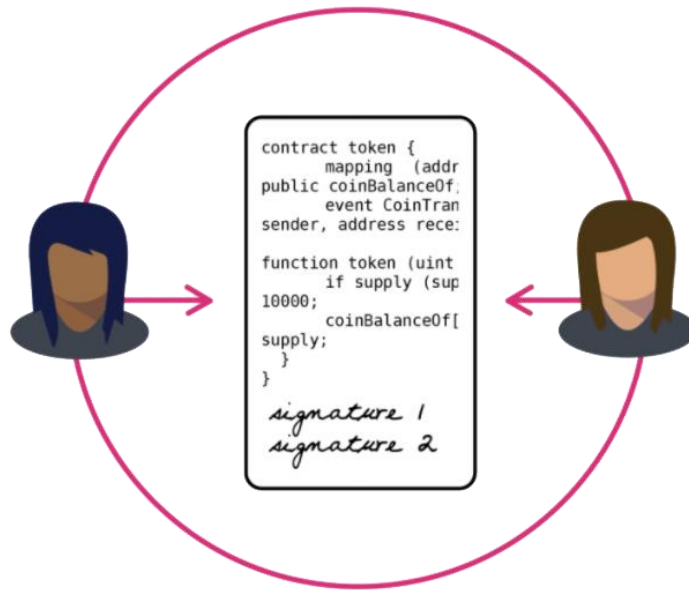
Smart Contracts
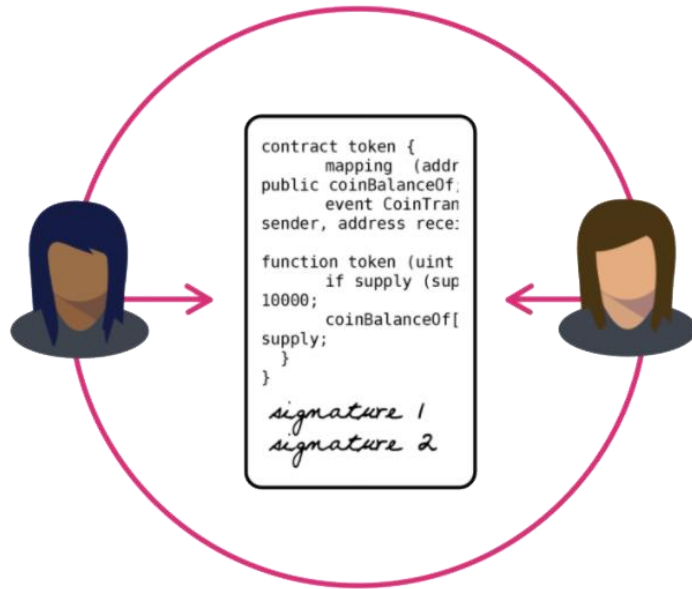
✓ Smart contracts can:

 ✓ Function as 'multi-signature' accounts, so that funds are spent only when a required percentage of people agree

 ✓ Manage agreements between users, say, if one buys insurance from the other

 ✓ Provide utility to other contracts (similar to how a software library works)

 ✓ Store information about an application, such as domain registration information or membership records

✓ Are often used for Decentralized Finance (DeFi) offerings (more on this later)

Initial Coin Offering

- A "liquidity event" to raise money for a venture to be created; some examples might include:
  - A car wash wants to raise money by pre-selling tokens which impart the right to car washes for a period of time
  - A group of programmers want to build an online casino and the virtual coin can be used as the chips in that online casino
- SEC says that if an ICO imparts equity in a venture/organization or if the founders get units in an ICO, that it must comply with SEC rules/regulations
- Good NY Times article on ICOs
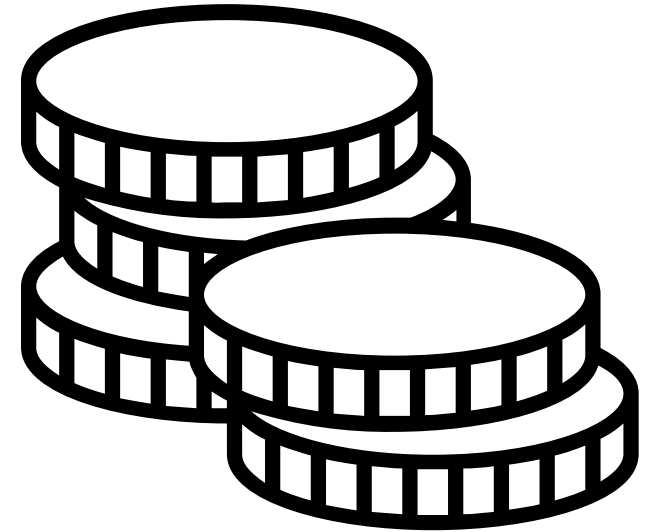
Initial Coin Offerings

Some successful past ICOs include:

- **NEO**, open source Chinese blockchain project (often called "the Ethereum of China") (ICO at $0.03, now trading at $40, all time high of $180)

- **Ethereum**, second largest digital currency by market cap and the platform which runs many smart contracts and altcoins. Ethereum ICO'ed at $0.31, and as of 10/25/2021, those same coins sold at $4,020/unit

- **Alias**, a privacy-focused cryptocurrency. Initial tokens sold at $0.001/token in 2016 and would be worth around $0.15 each now

- **Stratis**, UK-based cryptocurrency, initially raised 1,000 BTC and provided tokens that were initially $0.01/each – and traded at $1.89 earlier this year

Search SEC.gov 🔍

COMPANY FILINGS | MORE SEARCH OPTIONS

ABOUT | DIVISIONS & OFFICES | ENFORCEMENT | REGULATION | EDUCATION | FILINGS | NEWS

Newsroom

Press Releases

Speeches and Statements

Spotlight Topics

Media Kit

Press Contacts

Events

Press Release

🖨 f 🐦 ✉ +

SEC Charges Ripple and Two Executives with Conducting $1.3 Billion Unregistered Securities Offering

Related Materials

- SEC Complaint

FOR IMMEDIATE RELEASE
2020-338

Washington D.C., Dec. 22, 2020 — The Securities and Exchange Commission announced today that it has filed an action against Ripple Labs Inc. and two of its executives, who are also significant security holders, alleging that they raised over $1.3 billion through an unregistered, ongoing digital asset securities offering.

SEC And Crypto

- Many compliance areas are, at best, murky and will take years to work out so you have some kind of safe harbor

- Remember that you have a huge number of vested interests in government, financial services, and other industries who are very threatened by cryptocurrencies – so EXPECT regulation at some point

- AICPA has had four blockchain symposia (I've attended all of them) and they're working with the Wall Street Blockchain Alliance on many of these issues

- Be very careful signing your name or your firm's name – because the liability when you're an "expert" before the SEC is usually severe

CENTRAL BANK DIGITAL CURRENCIES

Central Bank Digital Currencies (CBDC)

- Implement digital currency for a traditional fiat currency issued by a central banking authority

- Unlike other cryptocurrencies, they could be configured to be centralized and require compliance with know your customer regs

- Although stablecoins might track or simulate a particular currency, many are not backed by consumer protections or the full faith and credit of a sovereign nation

- There are many privacy concerns with such currencies, including having the government see every transaction you do with others

Central Bank Digital Currencies (CBDC)

- Some countries have tried variations, many are evaluating:
  - Venezuela's Petro, allegedly backed by oil in the ground (but given that nation's history of asset expropriation, good luck collecting)
  - Equador, while not creating a CDBC, has declared both USD and Bitcoin legal tender in its legal system
  - Canada had a "digital loony" as an experiment, but ended the test without launching it publicly
  - The chair of the EU central bank has said that the EU will have a CBDC at some point in the future
  - Fed Chairman Powell addresses this topic in a video on the Fed's website

NON-FUNGIBLE TOKENS (NFTS)

Non-Fungible Tokens (NFTs)

- Non-fungible tokens or NFTs are cryptographic assets on blockchain with unique identification codes and metadata that distinguish them from each other

- Each NFT is an asset or right tracked in a blockchain-based ledger which allows for it to be bought, sold, and exchanged with others

- Many artists are adopting NFTs to sell their work to speculators

- Some organizations are selling NFTs of digital images, songs, or other intellectual property

- You may be charged a transaction fee (aka a "gas" fee) for NFT trades

Some NFT Transactions

- Jack Dorsey (@jack) first tweet NFT: $2.5 million

- A video of Lebron James dunking a basketball: $200,000 on NBA Top Shot, a website for buying/selling NBA video clips

- Nyan Cat, a GIF, sold for $600,000

- Cryptokitties, a trading fad for unique computer-created art of cats –many examples, some selling for as much as $300,000 each

Cryptokitties – www.cryptokitties.co

Start Your Digital Cat Collection

In CryptoKitties you can breed and adopt Kitties of all colours and shapes. Create Collections of your favourite cats and share them with our breeding community.

Eiffel 65 - Blue
11 kitties ♡ 42

Curated by
Pranksy

99 palindromes ...
99 kitties ♡ 16

Curated by
natealex | discord ...

❤ **otaku gen1 a...**
44 kitties ♡ 10

Curated by
nostrolovesyou

All World Cup Ki...
8 kitties ♡ 11

Curated by
SoaS

Popular NFT Marketplaces

- [NBA Top Shot](#)

- [OpenSea](#)

- [Mintable](#)

- [Nifty Gateway](#)

- [Rarible](#)

Search OpenSea
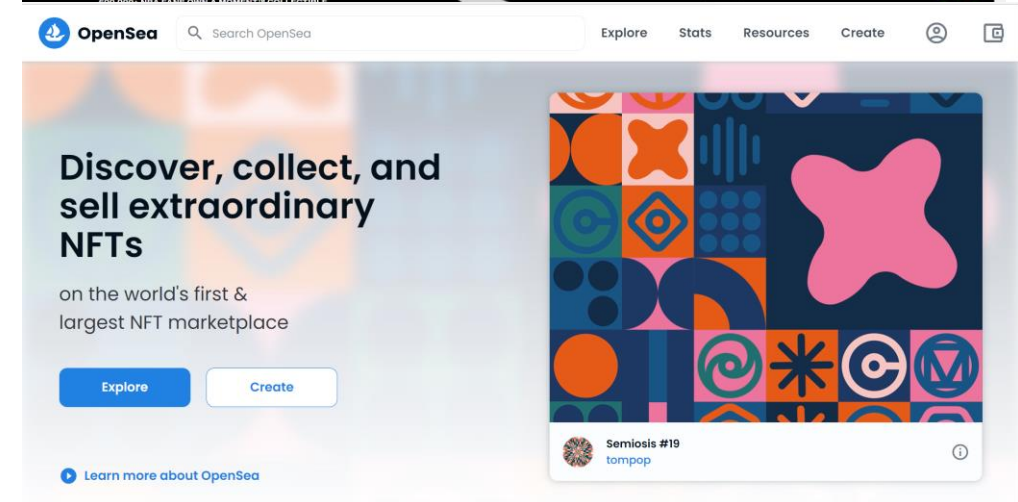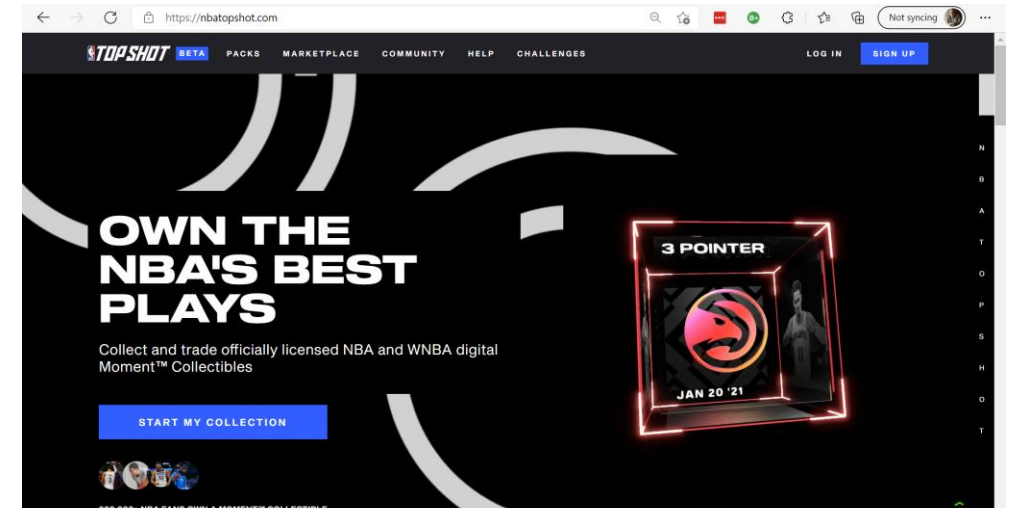
Top collections over last 7 days ⌄

1	CryptoPunks	+44.26%
	9,633.41	

6	HeadDAO	+699.81%
	2,916.01	

11	CreatureToadz	-
	2,292.52	

2	Bored Ape Yacht Club	+78.24%
	6,968.47	

7	Boonji Project	-
	2,847.88	

12	CyberKongz	+38.31%
	2,115.96	

3	Doodles	−3.29%
	6,198.57	

8	Party Ape	Billionair...	+116.34%
	2,634.67	

13	Cool Cats NFT	+20.62%
	1,964.84	

4	JUNGLE FREAKS BY TR...	−51.97%
	3,999.78	

9	CrypToadz by GREMP...	−17.05%
	2,391.16	

14	Mutant Ape Yacht Cl...	−7.69%
	1,921.36	

5	Kaiju Kingz	−51.77%
	3,793.2	

10	Party Degenerates	-
	2,388.55	

15	MekaVerse	−88.73%
	1,866.51	

DECENTRALIZED FINANCE (DEFI)

Decentralized Finance (DeFi)

- Concept is that where bitcoin is digital money, DeFi is blockchain-based peer to peer financial products and services
- Can theoretically be used for things like
  - Insurance
  - Lending
  - Borrowing
  - Derivatives trades
  - Asset trades
- Generally executed on a "peer to peer" basis and may fall afoul of many different financial services/insurance regulations
- Many DeFi products are executed with smart contracts on the Ethereum blockchain/platform

DeFi – What's Good About It?

- No account approval – just create a wallet and start trading

- Pseudonymous - No "know your customer" regulations here (which also can be bad, as you may not know who you're interacting with)

- Flexible – Move assets without waiting for transfers and paying expensive fees

- Fast – interest rates often update as often as every 15 seconds and can be higher than Wall Street

- Transparent – Everyone can see the transactions in a decentralized app ("dapp")

DeFi – What's Bad About It

- No customer service or central authority to call with questions
- Transaction rates on the Ethereum platform fluctuate and may make transactions expensive
- Higher volatility than you would have from a bank/broker with traditional financial assets
- You have to maintain your own records for tax purposes
- You (or your counterparty) could easily fall afoul of many different regulations – banking, money laundering, investment/securities, insurance, etc.
- There are many scamsters trying to cheat people out of capital in the current environment – which has been described by some as "The Wolf of Wall Street" on steroids

IRS OPERATION HIDDEN TREASURE

IRS And Operation Hidden Treasure

- Announced in March 2021 by IRS at a tax law conference
- Established in 2021, continues and expands previous IRS cryptocurrency initiatives
  - By the end of 2015, Coinbase had 5.9MM customers, had traded $6B in cryptoassets, and yet IRS reports only 800-900/yr reported gains during same time frame
  - 2019 IRS letters to those who have bought or sold $10K+ in crypto
- Partnership between IRS Criminal Investigation Division and the new IRS Office of Fraud Enforcement
- Focuses on addressing untaxed capital gains associated with cryptocurrency transactions
- IRS has picked TaxBit to do data analysis and tax calculations for audits of taxpayers with cryptocurrencies

Operation Hidden Treasure

- As early as the first AICPA Blockchain Symposium (2018), many participants reported that IRS, SEC, and other regulators were struggling to address cryptocurrency enforcement
  - There is no master directory which links crypto owners to their wallets
  - BUT transactions are recorded indelibly forever in the blockchain
  - AND exchanges which buy and sell cryptoassets with USD must register as Money Services Businesses with Treasury/FinCEN
  - AND must comply with Know Your Customer (KYC) rules and other Anti-Money Laundering (AML) regulations under the Bank Secrecy Act (BSA) and the USA Patriot Act

Operation Hidden Treasure

With all of that having been said, here's what we read in articles on the subject (there's not much forthcoming from IRS)

- Although audits where there's substantial understatement of taxes can go back farther, I'd expect IRS to go for the three open tax years first, then look for prior transactions that might warrant examination

- Some "whales" with large untaxed gains from prior to 2015 may be targeted IF IRS knows who they are and the amount at stake is significant or IF the examination of a crypto wallet shows that there were significant transactions in earlier periods

- Remember that you will need to value transactions at the fair value at the date of the transaction – so you will need someone to help you calculate that fair value

- Some people are going to go to prison for not paying taxes on their crypto, and some will blame their tax preparer for not including (even if they didn't tell you about it) – so you may want to reconfirm that there were no transactions in prior years in your next meetings with your clients

Operation Hidden Treasure

- Many cryptoasset holders have no records/reports associated with their trading activity, and therefore may not be able to prove any basis associated with their crypto holdings

- New question on 2020 1040 re: cryptocurrencies

- Accounting Today reports the following:
  - IRS will use third-party tools to analyze 2016 and forward
  - AT reports that the vendor providing cryptoasset data for IRS expects the information flow to IRS starting in early 2022

- Don't forget that non-attorney accounting professionals can be compelled by IRS to testify against their clients, so your client may need a tax attorney if they believe they may have a problem

Catching Crypto Cheaters

- While Bitcoin and other cryptocurrencies are "anonymous" in that amounts in the bitcoin blockchain have not historically been subject to "Know Your Customer" regulations, that is changing

- Most exchanges where you can buy/sell crypto have to register as "money service businesses" (1.5 years/$1.5 million dollars to get this license from U.S. Treasury)
  - You can't do large numbers of transactions in USD without complying with KYC and a host of other anti-money laundering regulations

- Since the entire blockchain is public (although not identified with anyone specifically), all IRS has to do is connect the dots for an account with another account which they can identify – then they have someone to subpoena for your client's data

- There are AML compliance platforms that look for large crypto transactions across the entire blockchain and then try to back into who the parties to the transaction are

- Remember that the rest of the world (including Canada) has VAT, so foreign government agencies/regulators could tip off IRS if their enforcement efforts identify a U.S. crime

LEDGIBLE TAX PRO

Ledgible Interfaces

- Ledgible has automated interfaces which support the major blockchains, exchanges, wallets & accounting platforms
- More interfaces are being added every month

Blockchains

Algorand (ALGO)	Bitcoin (BTC)	Bitcoin Cash (BCH)	Bitcoin Gold (BTG)	Bitcoin SV
Dash (DASH)	EOS (EOS)	ERC20 Tokens	Ethereum (ETH)	Ethereum Classic (ETC)
Litecoin (LTC)	Monero (XMR)	Stellar (XLM)	ZCash (ZEC)	

Exchanges

Bibox	Binance	Bitfinex	Bitstamp	Bittrex
Blockchain	Coinbase	Coinbase Pro	Gemini	HitBTC
Huobi	Kraken	LBank	OKEX	Poloniex
ZB				

Accounting Platforms

quickbooks   xero   NETSUITE
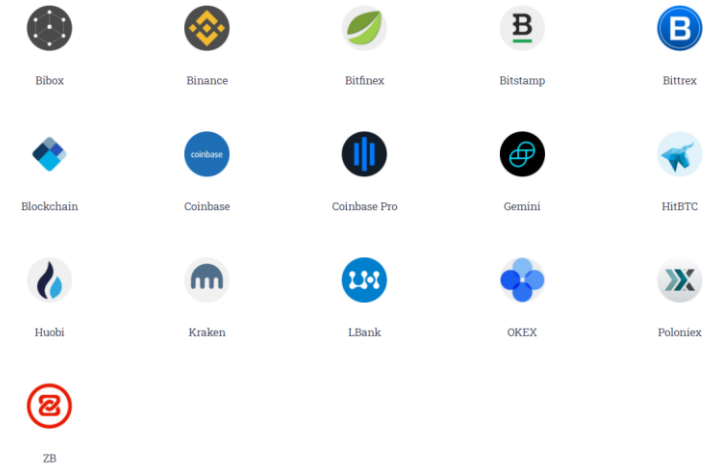
Ledgible Tax Pro by Verady

- Gathers transaction data from most major cryptocurrencies and exchanges
- Has the data needed to calculate basis and fair value of transactions in many cryptocurrencies
- Generates reports for supported currencies which can be used for gain/loss reporting and an inventory of open positions

Get a free cryptocurrency checklist (shown above) by filling out the online form at https://www.cpate.ch/verady

bftcpa
Tax Year 2020

Support

Tax Overview   Exchanges   Wallets   Transactions   Reports   Planning   Settings

Wallets   LEARN MORE

+ ADD WALLET DATA

View
All Wallet Types

View
All Blockchains

BTC
Feb 7, 2021 12:56 PM

BFT

50 Addresses

Add Wallet Data   ✕

Wallet Name
Brian Demo Wallet

Select Blockchain

BCH

BTC

DASH

LTC

? Help

K2 Enterprises

Support

Tax Overview | Exchanges | Wallets | Transactions | Reports | Planning | Settings

Wallet - *Brian Demo Wallet*

◄ WALLETS   ⟳ REFRESH

| SUMMARY | ADDRESSES | SETTINGS |

Blockchain	Wallet Value	Derived Addresses	Last Update
₿ BTC	$164.78	50	Feb 7, 2021 01:05 PM

Wallet Assets

Asset	Quantity	Fiat Value (USD) ↓	BTC Value
₿ BTC	0.0044	164.7814	0.0044

Recent Wallet Transactions ⓘ

Date ↓	Quantity	Fiat Value (USD)	Asset	Transaction Hash
December 12, 2020 12:38 PM	0.00435539	$80.13	BTC	7a471759f58c...
December 12, 2020 12:38 PM	0.01171063	$215.44	BTC	7a471759f58c...
December 12, 2020 11:31 AM	0.01204562	$221.93	BTC	dda05305bb9...
December 12, 2020 11:31 AM	0.01171063	$215.76	BTC	dda05305bb9...
June 17, 2019 7:41 PM	0.01440276	$134.67	BTC	ab0acf0b08fe...
June 17, 2019 7:41 PM	0.01204562	$112.63	BTC	ab0acf0b08fe...
July 18, 2018 4:38 PM	0.01495169	$109.24	BTC	da7dbeaaca2...

⓪ Help

Tax Overview | Exchanges | Wallets | Transactions | Reports | Planning | Settings

Wallet - *Brian Demo Wallet*

◄ WALLETS   ⟳ REFRESH

| SUMMARY | ADDRESSES | SETTINGS |

Derived Addresses - *Brian Demo Wallet*

Search wallet addresses   🔍   ?

1	17xrEG959wqkfRHLqJcdFncJ3kLJw48jgX
2	1DrWiJaWLg1o9mVn9JVP1KV6b7tWWDo7TR
3	1Bq8Di7CANMoJLS8JzGvCr8Kn77Dmsp38b
4	13qNWhMcQ9FWmZe5XrqMaNYtvQdfHjtrTN
5	1Ee5h9wpF9kv47vfPGHFTiJS7w4tHoR8BZ
6	1DiTxWFt1buifK3HenVQxTb739fmKp5wSd
7	1CdjvFYseophPzXosiwW19eQkUrb2tMK8W
8	184Udtt4EfdnqfvhVPnjxyJwQEVHngVryj
9	14S33AbCGcbu8FeNCWZAUaDa2foVHXHDmu

Help

K2 Enterprises

Tax Overview | Exchanges | Wallets | Transactions | Reports | Planning | Settings

Transactions 📖 LEARN MORE

⟳ RUN TAX UPDATE + CREATE ENTRY

Filters: *Applied* Clear All Show Default

📅 Transaction Date | 🗂 Wallets | 🔄 Exchanges | 🪙 Currencies | 🏷 Types | 🚩 Tax Disposals | 🏷 Fees

6 Transactions Found

☐ Show Multi-Select

	Date ↑	Wallet/Exchange	Type	Proceeds ⓘ	Cost Basis ⓘ	Quantity	Currency		Gain/Loss ⓘ	Actions
➕	7/18/2018 12:00 PM	BFT	↗ Outgoing Transfer 99cbf6c3d61d180... 📋	$5.50	$5.50	- 0.000742	₿ BTC	🚩	$0.00	⋮
➕	7/18/2018 12:39 PM	BFT	↗ Outgoing Transfer b25602a186774c... 📋	$7.54	$7.52	- 0.001014	₿ BTC	🚩	+ $0.02	⋮
➕	7/18/2018 4:38 PM	BFT	↗ Outgoing Transfer d828884caf8db0a... 📋	$3.65	$3.71	- 0.0005	₿ BTC	🚩	- $0.06	⋮
➕	6/17/2019 7:41 PM	BFT	↗ Outgoing Transfer 268528208cfa4b3... 📋	$19.75	$15.67	- 0.002112	₿ BTC	🚩	+ $4.08	⋮
➕	12/12/2020 11:31 AM	BFT	↗ Outgoing Transfer 0a97331b309d1e... 📋	$3.68	$1.48	- 0.0002	₿ BTC	🚩	+ $2.20	⋮
➕	12/12/2020 12:38 PM	BFT	↗ Outgoing Transfer 5696f6af760ab6a... 📋	$132.77	$53.54	- 0.007217	₿ BTC	🚩	+ $79.23	⋮

⏻ Help

Tax Overview   Exchanges   Wallets   Transactions   **Reports**   Planning   Settings

Tax Reports On Demand

Ready to get your reports? Just input your wallet and exchange data to get started. Learn more about tax report outputs or generate a report below.

IRS Form 8949

PDF output of IRS Form 8949 to capture long and short term capital gains/losses

TurboTax Import

Compatible CSV file for import into TurboTax

TaxAct Import

Compatible CSV file for import into TaxAct

Transaction Export

An export CSV of all imported transactions

Income Transaction Export

An export CSV of all transactions with an income categorization

Gift Transaction Export

An export CSV of all with an gift categorization

Help

Tax Reports On Demand

Ready to get your ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~tax report
outputs or generat~~~~~~~~~

IRS Form 8949
PDF output of IRS

TurboTax Import
Compatible CSV fil

TaxAct Import
Compatible CSV fil

Transaction Expor
An export CSV of a

Income Transactio
An export CSV of a

Gift Transaction E
An export CSV of a

Generate 2020 Report

Select the type of report you would like to generate and click Next.

Tax Reports

○ IRS Form 8949

○ TaxAct Import

○ TurboTax Import

Other Reports

○ Gift Transaction Export

○ Income Transaction Export

◉ Transaction Export

ⓘ **Transaction Export**
An export CSV of all imported transactions.

CANCEL   CREATE REPORT

Help

TransactionOrder Details

Timestamp:	Sat Dec 12 2020 17:38:43 GMT+0000 (Coordinated Universal Time)
Hash:	7a471759f58ca22e131e25a4755955ef58ccbe0a72e773eae6beb3242ad6f6e5 📋
Source:	Bft (wallet)
Type:	Transfer	Transaction Side:	Outgoing
Categorization:	No Category (Add)	Quantity:	0.007217 (BTC)
Price:	$18,397.08	Ignored:	No (Ignore)
Proceeds:	$132.77	Cost Basis:	$53.54
Gain/Loss:	$79.23		

🔍 Open In Block Explorer

Memo

Purchase

Characters

Blockchain.com   Wallet   Exchange   **Explorer**

Buy Bitcoin   Trade

Explorer > ₿ Bitcoin Explorer ▾ > Transaction

🔍 Search your transaction, an address or a block

USD ▾

Summary ⓘ

USD | **BTC**

Hash	7a471759f58ca22e131e25a4755955ef58ccbe0a72e773eae6be... 📋		2020-12-12 12:30
	1ADpk9Los2C6YKNLyqcr5q4YFhidT8Yj28	0.01171063 BTC 🌐 ➡	17xrEG959wqkfRHLqJcdFncJ3kLJw48jgX 0.00435539 BTC 🌐
			12GJbYo4a1SxNsT9G3CF4cXbMFqjiwwwcv 0.00721700 BTC 🔴
Fee	0.00013824 BTC (61.168 sat/B - 15.292 sat/WU - 226 bytes)		0.01157239 BTC

Customer ID: brian@tankersley.com
Account Number: 1567150

Dear BRIAN TANKERSLEY,

Thank you for shopping at Newegg.

This is the invoice and receipt for your recent order. Please keep a copy for your records.

Invoice Summary:

Your Sales Order Number: 495228311

Order Date: 12/12/2020

Order Total: $131.05

Billing Information	Shipping Information
To view your Bitcoin payment receipt, click the URL below.	BRIAN TANKERSLEY
	███████████████

Invoice Number:	186339443
Invoice Date:	12/12/2020 10:25:05 AM

ORDER SUMMARY

Order # 495228311

Sold and Shipped by Newegg
Est. Ship Date: **12/14/2020 by End of Day**

Crucial X6 1TB Portable SSD - Up to 540 MB/s - USB 3.2 - USB-C - CT1000X6SSD9

Qty: **1** $119.95

Subtotal:	$119.95
Tax:	$11.10
Shipping:	$0.00
Grand Total:	**$131.05**

...

SHOP NEWEGG   MY ACCOUNT   CUSTOMER SERVICE

	A	B	C	D	E	F		G	H	I	J	K	L	M	
1	Currency	Curr	Date	Ignored	Internal	Price		Quantity	Source	Source	Tax Category	Transaction Id	Tx Side	Tx Type	Tx-Hash
2	Bitcoin	BTC	7/18/2018 15:42	No	No	$	7,418.20	0.01684600	BFT	wallet		646de125639ea667e9d	incoming	transfer	4300235
5	Bitcoin	BTC	7/18/2018 16:00	No	No	$	7,418.20	0.00074200	BFT	wallet		99cbf6c3d61d1802d846	outgoing	transfer	090bc80
8	Bitcoin	BTC	7/18/2018 16:39	No	No	$	7,438.23	0.00101400	BFT	wallet		b25602a186774cd3073!	outgoing	transfer	2348a68
11	Bitcoin	BTC	7/18/2018 20:38	No	No	$	7,306.10	0.00050000	BFT	wallet		d828884caf8db0aa3db6	outgoing	transfer	da7dbea
13	Bitcoin	BTC	6/17/2019 23:41	No	No	$	9,349.95	0.00211200	BFT	wallet		268528208cfa4b3e67bc	outgoing	transfer	ab0acf0b
17	Bitcoin	BTC	12/12/2020 16:31	No	No	$	18,424.13	0.00020000	BFT	wallet		0a97331b309d1e33b75	outgoing	transfer	dda0530
20	Bitcoin	BTC	12/12/2020 17:38	No	No	$	18,397.08	0.00721700	BFT	wallet		5696f6af760ab6ad109a	outgoing	transfer	7a47175!

Form 8949 — Sales and Other Dispositions of Capital Assets

Form 8949
Department of the Treasury
Internal Revenue Service

▶ Go to *www.irs.gov/Form8949* for instructions and the latest information.
▶ File with your Schedule D to list your transactions for lines 1b, 2, 3, 8b, 9, and 10 of Schedule D.

OMB No. 1545-0074
2019
Attachment
Sequence No. **12A**

Name(s) shown on return

Social security number or taxpayer identification number

Before you check Box A, B, or C below, see whether you received any Form(s) 1099-B or substitute statement(s) from your broker. A substitute statement will have the same information as Form 1099-B. Either will show whether your basis (usually your cost) was reported to the IRS by your broker and may even tell you which box to check.

Part I   **Short-Term.** Transactions involving capital assets you held 1 year or less are generally short-term (see instructions). For long-term transactions, see page 2.

Note: You may aggregate all short-term transactions reported on Form(s) 1099-B showing basis was reported to the IRS and for which no adjustments or codes are required. Enter the totals directly on Schedule D, line 1a; you aren't required to report these transactions on Form 8949 (see instructions).

You *must* check Box A, B, or C below. Check only one box. If more than one box applies for your short-term transactions, complete a separate Form 8949, page 1, for each applicable box. If you have more short-term transactions than will fit on this page for one or more of the boxes, complete as many forms with the same box checked as you need.

- ☐ **(A)** Short-term transactions reported on Form(s) 1099-B showing basis was reported to the IRS (see **Note** above)
- ☐ **(B)** Short-term transactions reported on Form(s) 1099-B showing basis **wasn't** reported to the IRS
- ☒ **(C)** Short-term transactions not reported to you on Form 1099-B

Part II   **Long-Term.** Transactions involving capital assets you held more than 1 year are generally long-term (see instructions). For short-term transactions, see page 1.

Note: You may aggregate all long-term transactions reported on Form(s) 1099-B showing basis was reported to the IRS and for which no adjustments or codes are required. Enter the totals directly on Schedule D, line 8a; you aren't required to report these transactions on Form 8949 (see instructions).

You *must* check Box D, E, or F below. Check only one box. If more than one box applies for your long-term transactions, complete a separate Form 8949, page 2, for each applicable box. If you have more long-term transactions than will fit on this page for one or more of the boxes, complete as many forms with the same box checked as you need.

- ☐ **(D)** Long-term transactions reported on Form(s) 1099-B showing basis was reported to the IRS (see **Note** above)
- ☐ **(E)** Long-term transactions reported on Form(s) 1099-B showing basis **wasn't** reported to the IRS
- ☒ **(F)** Long-term transactions not reported to you on Form 1099-B

(a) Description of property (Example: 100 sh. XYZ Co.)	(b) Date acquired (Mo., day, yr.)	(c) Date sold or disposed of (Mo., day, yr.)	(d) Proceeds (sales price) (see instructions)	(e) Cost or other basis. See the Note below and see Column (e) in the separate instructions	(f) Code(s) from instructions	(g) Amount of adjustment	(h) Gain or (loss). Subtract column (e) from column (d) and combine the result with column (g)
0.00020000 BTC	07/18/2018	12/12/2020	3.68	1.48			2.20
0.00721700 BTC	07/18/2018	12/12/2020	132.77	53.54			79.23
2 Totals. Add the amounts in columns (d), (e), (g), and (h) (subtract negative amounts). Enter each total here and include on your Schedule D, line 8b (if Box D above is checked), line 9 (if Box E above is checked), or line 10 (if Box F above is checked) ▶			136.46	55.02			81.44

Note: If you checked Box D above but the basis reported to the IRS was incorrect, enter in column (e) the basis as reported to the IRS, and enter an adjustment in column (g) to correct the basis. See *Column (g)* in the separate instructions for how to figure the amount of the adjustment.

Form **8949** (2019)

K2 Enterprises

The End
QUESTIONS?