Bits & Bytes

Arkansas' Premier Computer Club

December 2022

Bella Vista Computer Club - John Ruehle Center

Highlands Crossing Center, 1801 Forest Hills Blvd Suite 208 (lower level), Bella Vista, AR 72715

Website: http://BVComputerClub.org **Email: editor@bvcomputerclub.org**

MEETINGS

Board Meeting: December 12, 6pm, in John Ruehle Training Center, Highlands Crossing Center.

General Meeting: December 12, 7pm, "Google Search Techniques", with Joel Ewing. The most common usage of search engines is to search for keywords, but there are also more advanced techniques to use when keywords alone aren't sufficient.

We will meet in-person in Room 1001 on the lower level of The Highlands Crossing Center, 1801 Forest Hills Blvd, Bella Vista, or you may attend the meeting on-line via Zoom. Zoom access information is published on our website.

Visitors or Guests are welcome.

Because of the continuing presence of COVID-19, we recommend observing any current guidelines that may be in effect at the time of the meeting. Consider attending by Zoom if you or others in your family are in a high risk category.

HELP CLINICS

December 3, 9am - noon at John Ruehle center
December 21, 9am - noon at John Ruehle center
Members may request Remote Help on our website at https://bvcomputerclub.org at menu path Member Benefits ►Remote Help .

MEMBERSHIP

Single membership is $25; $10 for each additional family member in the same household.

Join on our website at https://bvcomputerclub.org at menu path Get Involved ►Join/Renew, by mailing an application (from the web site) with check, or complete an application and pay in person at any meeting.

CLASSES

(At BVCC Training Center)

Wednesday, December 7, 9am-11am, "Data: Where Is It And What To Do With It", with Pete Opland.

Tuesday, December 20, 2pm-4pm, "Basic Computer Security, Part 1", with Justin Sell.

Wednesday, December 21, 1pm-3pm, "Installing WiFi Printers", with Pete Opland.

Advance sign up required for each listed class: For reservations: email to edu@bvcomputerclub.org, or sign up at the General Meeting. Classes are **free to Computer Club members.**

Check the monthly calendar and announcements for any last minute schedule changes at https://bvcomputerclub.org .

NEW OR RETURNING BVCC MEMBERS

We are pleased to welcome the following new members or members returning to BVCC after an absence since last month's newsletter:

Gloria Fry	Mary Doyle	Pete Doyle

AMAZON SMILE, A PAINLESS WAY TO DONATE TO BVCC (A REPEAT)

By Joel Ewing

With the coming holiday season, odds are many will be making online purchases and probably some of those will be at Amazon. If you have an account at Amazon, the Amazon Smile program allows you to designate one specific charity to receive a donation from Amazon of 0.5% of the price of each purchase you make at Amazon. The only requirement is that you set BVCC as your designated charity, and then use "smile.amazon.com" as your URL at some point before you authorize the purchase.

The easiest way to set, BVCC as your designated Amazon charity, is to go to the Donate page at https:bvcomputerclub.org (menu path "Get Involved ►Donations" or the "Donate" button on the home page), and then click on the large "Support The Bella Vista Computer Club Inc ... amazonsmile" button on the right side of the Donate page. That will take you to the Amazon site and set your default charity (it may ask you to logon to your Amazon account).   If you have already done this for some other charity, you will first be asked to verify that you want to change your charity designation.

You can alternatively go to https://smile.amazon.com/change" or tap "AmazonSmile" within the Settings menu in your Amazon Shopping app on your smart phone and select "change your charity", searching for the charity name "The Bella Vista Computer Club" (The "The" is part of our official IRS name).

If you make purchases using the Amazon Shopping app on your smart phone, you can set that app to default to use smile.amazon.com for all purchases.

If you make your purchases at the Amazon web site via a browser after searching for the item with one of the usual search engines, the links from the search will take you to www.amazon.com.   In order for your purchase to result in an Amazon smile donation, you must over type the "www" in the URL with "smile" at some point before you actually authorize the purchase.

ARE YOU STILL RUNNING WINDOWS 8.1?

Microsoft update support for Windows 8.1 ends January 10, 2023 along with Windows 8.1 support for Microsoft 365 apps. This potentially affects anyone who is still depending on a PC using Windows 8.1.

If your hardware is recent enough and sufficiently capable, you might have an option of migrating to Windows 10. Just be aware that hardware that originally came with an Operating System of Windows Vista or earlier probably lacks the power to run Windows 10 acceptably.   A computer that originally came with Windows 7 may be able to run Windows 10, but could be a slow performer with Windows 10.   A successful migration to Windows 10 would at least solve the immediate problem, until Windows 10 end-of-support occurs in late 2025.

Should you elect to upgrade to a newer PC, be sure to look for one that either comes with Windows 11 or is capable of running Windows 11 if you plan to keep your PC longer than three years.   After October 14, 2025 Windows 10 will no longer be supported, requiring hardware capable of running Windows 11.

WHAT IS BLOCKCHAIN TECHNOLOGY?

By Joel Ewing, President BVCC
Bits & Bytes, Dec 2022
president (at) bvcomputerclub.org

One of the new buzzwords one frequently sees today, primarily in reference to cryptocurrencies, is "Blockchain". Sometimes it is used as a synonym for cryptocurrency, which is inaccurate. Blockchain technology is used as part of the underlying architecture for implementing cryptocurrencies, but it has many other potential uses as well. Some of those other uses include monitoring of supply chains, copyright and royalties protection, and managing medical clinical trials data.

There are now literally thousands of cryptocurrencies in existence. The implementation details are of course different for each, but all are implemented on Blockchain technology and no doubt use many of the same concepts as Bitcoin.

There is a public perception that Blockchain technology was created with the creation of Bitcoin by the mysterious Satoshi Nakamoto around 2008, and you will even find claims to that effect on the Internet. In reality, many of the concepts on which Blockchain is based have much earlier origins dating as far back as 1972. Blockchain technology was first outlined in a 1991 article by Stuart Haber and W. Scott Stornetta[1]. Bitcoin was just the first major usage of Blockchain technology that was large enough to attract the attention of the general public.

The main feature of Blockchain technology is a distributed (decentralized) shared digital database, designed to allow new information to be added by multiple parties while preventing previous information from being changed. In other words, transactions are designed to be "immutable" once written. The intent of the design is to allow multiple independent copies of the database to exist with update rules that allow new transactions to be validated and propagated to all copies of the database in ways that keep the copies in sync and allow all copies to be trusted, even if the individual parties maintaining the database copies don't completely trust each other. Each party that adds a block to the Blockchain communicates an added block to all the other maintainers, and if two parties attempt to add blocks that compete as the next block, a majority vote resolves the conflict.

Security of The Blockchain Itself

Sometimes the use of Blockchain technology is used to bolster a claim that a cryptocurrency is secure. That is an over-simplification, as the devil in in the implementation details and update protocols, and specific implementations can include design flaws. It is not impossible to hack Blockchain cryptocurrency ledgers, but it is sufficiently difficult that criminals currently use much easier approaches.

Public Blockchains, where the maintainers of the Blockchain are open to anonymous participants, can be compromised if 51% of the distributed ledgers can be controlled by a single party. The integrity of the shared distributed Blockchain ledger is enforced by majority vote of all the ledger copies. If one party can nearly simultaneously update a majority of the ledgers, then the ledger can be altered in unintended ways. With Bitcoin, proof-of-[computational]-work is required ("mining") to update a ledger. The increasing cost of mining Bitcoin

[1] "How to Time-Stamp a Digital Document",*Journal of Cryptology. **3** (2): 99–111.*

is an incentive to consolidation and cooperation among the mining community. This could at some point in the future threaten the immutability of the Bitcoin Blockchain. With Ethereum cryptocurrency, proof-of-stake (a requirement to put 32 ETH, close to$40K, into escrow) is used to become a maintainer. It would be costly to gain 51% control, but not impossible.

The easiest direct theft of cryptocurrency typically involves hackers draining funds from accounts whose credentials they have compromised by some means -- with at least five major heists in the first half of 2022. This usually involves attacks against cryptocurrency exchanges or against Blockchain bridges, which allow fund transfers between many different cryptocurrencies. Both of these types of on-line sites hold digital cryptocurrency assets of many users, making them attractive targets for cyber-criminals or for profitable mismanagement.

One of the original design goals and appeal of cryptocurrency was its independence from traditional financial institutions, but the reluctance of many to directly transfer and manage cryptocurrency led to the creation of cryptocurrency "exchanges". These exchanges act very much like banks in that they assume the task of holding the digital wallets of many customers, holding customer digital currency credentials and access to cryptocurrency assets and handling transfers. One major problem is that these digital exchanges are not classified as banks and are not regulated like banks. There have been multiple instances of such exchanges using the cryptocurrency entrusted to their care for risky digital loans and investments to the extent that the exchange eventually fails with considerable loss to its users and possible loss of confidences and loss of value for all digital currencies.

Although such direct theft can be significant, it is still overshadowed by simple fraud losses, where the user is taken in by some clever con artist or investment fraud and willingly transfers his cryptocurrency for a "great" deal, only to realize too late he has been taken and there is no way to cancel an immutable cryptocurrency transaction to an anonymous party.

Security is much simpler to maintain with private Blockchains, where maintenance authority and access to the ledger is restricted by a controlling authority and there is positive identification of all participants. The Blockchain technology prevents unintentional corruption of the ledger, and the controlling authority can institute any network security, backup, and audit procedures deemed appropriate.

Bitcoin Wallets

Bitcoin wallets are created using a secret mnemonic "seed" phrase of 12 to 24 words. That seed is then used to generate and store into the wallet an asymmetric private/public encryption key pair and possibly additional derivative private/public encryption key pairs. The nature of these key pairs is that data encrypted with the public key can only be decrypted using the private key, data encrypted with the private key can only be decrypted using the public key, and knowing the public key does not allow you to find the private key. The public key(s) are used inside the Blockchain to identify the wallet holder as the owner of Bitcoin assets. The private keys are available only to the wallet owner, and are used to prove ownership of Bitcoin assets and authorize transfer of those assets. The public keys of other wallet owners are used to identify the receiver of a Bitcoin transfer.

Should you lose your Bitcoin wallet, you will be unable to access any of your Bitcoin assets; but it is possible to re-construct a Bitcoin wallet if you at least remember the secret phrase used to generate it. If you lose both your wallet and the secret seed phrase used to generate it, then all the Bitcoin assets associated with the keys in that wallet are permanently lost to everyone. One source estimates that as much as 25% of all bitcoins that have ever been created have been lost in this manner.

If you allow your Bitcoin wallet to be copied by someone else, or if your wallet "seed" phrase is stolen by someone else, then that party can access and transfer all the assets associated with that wallet.

One individual can have multiple wallets, each of which may have multiple key-pairs; but each public key belongs to a single wallet and hence to a single owner.

Owners and receivers of Bitcoin assets are only known by their public keys, but this does not guarantee complete anonymity and secrecy: the pattern of transactions associated with the same public key, especially when it is associated with purchase of goods and services that require name or address to deliver, or conversion to or from physical currencies to accounts that have a name and address association, may be sufficient to deduce the actual owner associated with a public key. Patterns of transfers between various public keys may also be sufficient to imply relationships among their owners or that the keys are associated with the same owner.

Bitcoin Blockchain Structure

Blockchain gets its name from its structure: A sequential progression or stack of blocks, with each block chained to its immediate earlier predecessor, or parent. The details of the structure of the blocks and their size varies depending on the application using the Blockchain technology, but in all cases each block contains a header part and a transaction part. The header contains a block creation timestamp, the hash value[2] of the header of the previous or parent block, a hash value derived from the transactions in the current block, and some other fields. Every block has an associated "block height" ordinal that is one greater than that of its parent block. The Blockchain is initially set up with a single genesis, block-height-0 block that is built into all application code that works with that specific Blockchain implementation.

The header hash value of a specific block is unique[3], and if you validate that the block header has the correct hash value, then the header fields have not been altered and you have also validated the transaction (Merkle root) hash value in the header, which can be computed from the individual transaction hash values to prove all the transactions are unaltered as well. It is possible that the timing of adding new blocks from two different nodes may conflict and temporarily produce two new blocks with the same parent block and block height, but majority vote will eventually eliminate the one that is not the true next block.

[2] The hashing function used is a double SHA256 (SHA256 applied twice) yielding a 32-byte value.

[3] While the article on hashing functions (Bits&Bytes, Sept 2022) makes it clear it is EXTREMELY improbable two blocks would hash to the same 32-bit value, that is not the same as mathematically proving that it is impossible to have duplicate hash values for two different blocks. Each network node holding the complete Blockchain would be in a position to verify and insure there is no hash conflict with previous blocks. In the absence of a proof that block hash duplicates are impossible, one would hope the Bitcoin implementation does not rely on uniqueness without verification.

Each transaction within a block has its hash function computed and those hash values used to construct a Merkle Tree -- a tree structure where the leaves are the hash value of individual transactions, the next level is a hash value based on two transactions, the next level on four transactions, and so on, until finally you get to the root of the Merkle tree which is a hash value dependent on all transactions in the block (and this is the value placed in the block header). This somewhat complex structure makes it easy to verify that a specific transaction with a known hash value is present in the transaction part of a block containing 1000's of transactions by just looking at the small part of the block that contains the header and the Merkle Tree.

Each network node maintaining a copy of the Bitcoin ledger would be able to locate a particular block using either the Block Height value or the Header hash value for that block. If there were a need to reference a specific transaction, that is usually done by giving the transaction hash value and the block height of the containing block.

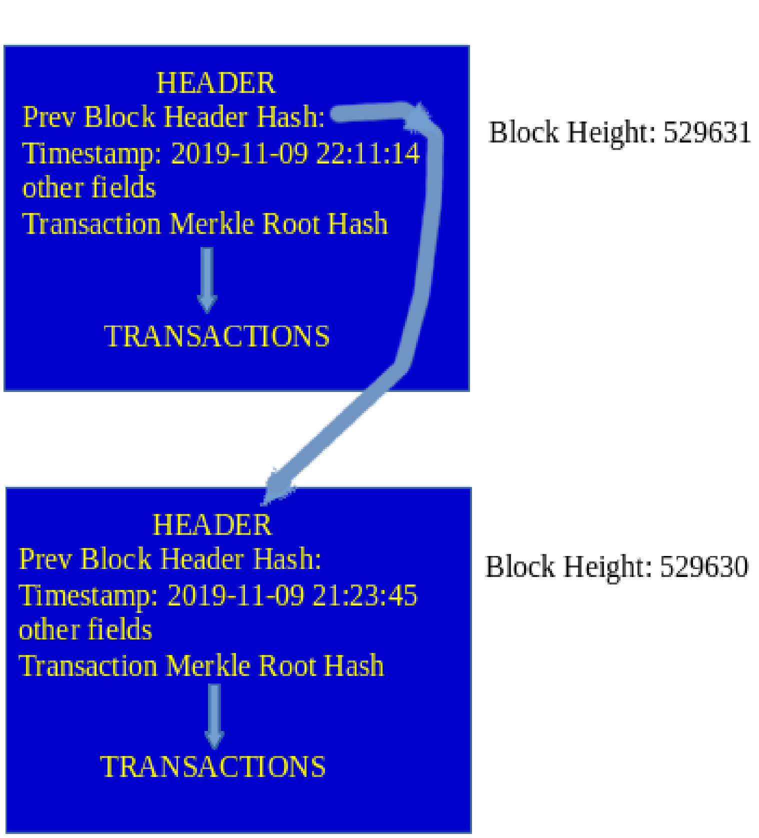

Figure 1: Two Consecutive Blocks

Once a block has been successfully written to the Blockchain, the data in any given block cannot be altered retroactively without altering all subsequent blocks, and 51% of those nodes with a copy of the ledger would have to concur with such an unusual action.

Overview of Bitcoin Transaction Structure

The details of how to build a Bitcoin transaction are more complex than is appropriate for discussion here, but the general concepts can be covered.

Transactions typically have multiple parts, each part representing an "unspent transaction output", or UTXO record. These represent the assets of individual Bitcoin owners, who are identified only by a private cryptographic key associated with the owners Bitcoin wallet.

Each transaction consists of input UTXOs, referenced by Transaction Hash and Block Height of the containing block, representing Bitcoin amounts in *satoshis (1 BTC or Bitcoin =* 10^8 *satoshis)* owned by the transaction originator, and output UTXOs, representing amounts transferred to another public key or retained as "change" by the current owner. Change is typically required because each UTXO asset used as input to a transaction must be completely consumed. You try to select the minimum combination of UTXOs to cover the transaction, but unless they just happen to total to the exact amount required, change is returned in the form of an output UTXO. The typical minimum number of UTXOs for a transaction involving change would be 1 input UTXO and 2 output UTXOs (one of which is the "change" retained by the original asset holder).

Note that there is no counterpart in the Bitcoin Blockchain to the current balance of a checking account. The current Bitcoin balance for a Bitcoin owner is the sum of all the unspent UTXO's for that owner across all transactions in all blocks of the Bitcoin Blockchain. The owner's digital wallet contains all the private/public keys associated with the wallet, from which the total of all the unspent UTXO assets owned by the corresponding public keys in the Bitcoin Blockchain can be computed, but that balance itself is not directly stored anywhere in the Blockchain. For the sake of efficiency as a starting point for computing an owner's bitcoin balance and figuring out how to make payments, it would be useful for a wallet to at least keep a local copy of all the transaction addresses in the Blockchain that contain UTXOs with unspent assets, and maybe even cache a local copy of the UTXO itself; but I have no idea if this is done. Worst case is that to verify bitcoin balance and create a transaction the entire Blockchain would have to be scanned for assets, instead of just the blocks added since the previous scan.

Bitcoin Transaction Processing Fees

The sum of all the input UTXOs for a transaction are normally less than the sum of all the output UTXOs. The unspecified remainder is a fee that is given to the party that records the transaction on the Bitcoin Blockchain. While payment of a fee is not mandatory, those transactions that offer a higher fee per byte of transaction data are processed first. To get acceptable processing time, fees must generally be offered; and during times of peak processing volume, higher fees are required to get acceptable processing times. According to nasdaq.com:

> "As of Aug. 23, 2022, the average Bitcoin transaction fee is 0.000044 BTC, or $0.957. In the past year, it has fluctuated from less than $1 to nearly $5. However, at its peak in April of 2021, the average transaction fee reached over $60."

Note that unlike credit card and many other on-line payment methods, a Bitcoin transaction fee is not based on on the value transferred by the transaction, but on the number of bytes to describe the transaction. The cheapest transaction fee would be one where all the assets to be transferred come from one input UTXO and only one output UTXO was required for payment -- it makes no difference whether the amount transferred is $10 or $10 million dollars. On the other hand, if the transaction payment requires you to combine the assets from many different UTXO transactions, the transaction size in bytes would be much greater and the transaction fee correspondingly higher, even if the total value transferred by the transaction is low.

Note that also unlike credit card transactions, the total volume of transaction traffic that can be handled is much lower, and when the rate of transactions approaches that limit, individual transaction processing fees can surge unpredictably making Bitcoin transactions much more expensive than credit cards for small transactions.

Also keep in mind that a party from whom you are purchasing goods or services with bitcoin may impose their own processing fees, which might be based on a percentage of the transaction value.

Other Blockchain Capabilities

In other applications, transactions in the block chain may represent the transfer of something other than cryptocurrency, and the rules for when the transfer occurs can also be much more complex (even with Bitcoin). This technology has been used for the transfer of digital art or for copyrighted assets, or as a means to record the movement of physical material from one party to another. Transfers can also be conditional on various other events, such as allowing the transfer of assets to occur only after some contract has been digitally signed by all parties, or after multiple parties have agreed to the transfer.

FUNDRAISER RAFFLE IN THE WORKS

The details have not all been decided at this point, but at sometime in the near future we will raffle off an extremely capable desktop computer that has been customized by our own Pete Opland.   Someone will win a good machine for a small donation.

The base machine is Dell Optiplex 5060 Tower Desktop with an 8th generation CPU that benchmarks at 12.89. It has been enhanced to include Windows 11 Pro (on the solid state drive), MS Office 2021 Pro Plus, and two hard drives configured as 1 TB RAID-1 storage to protect user data from a single hard drive failure.   A comparably configured computer could easily retail in excess of $700.

The tentative plan is to offer raffle tickets for a donation of $10 and have members help to distribute the tickets. Participation in the raffle would also be available to non-members of BVCC.   Physical presence at a meeting would not be required to win the raffle, but in that case the winner would need to be able to schedule a time to pick up the prize.   Details and the exact timing of the raffle will be finalized in December.