Bits & Bytes

Arkansas' Premier Computer Club

June 2018

Bella Vista Computer Club - John Ruehle Center

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

Website: http://www.BVCompClub.org Email: editor@bvcompclub.org

HOW TO FIND US

All meetings are on the lower level of the Highlands Crossing Center in Bella Vista. You may use entrance A on the West side or entrance C on the South side and take the elevator or stairs to the lower level. Turn left (West) to reach the General Meeting room, right for the John Ruehle Training Center. Additional information is on our web site.

MEETINGS

Board Meeting: June 11h, 6:00 pm, John Ruehle Training Center

General Meeting: June 11th (2nd Monday), 7:00 pm, Community Room A (Rm 1001). **Program:** "Emergency Preparedness & Trusts", presented by Carolyn Grieve and Maryann Sweeney from Arvest Bank.

Bring a guest! New Members and Guests are always welcome at the General Meeting

Genealogy SIG: June 16th (3rd Saturday), 10 am – noon, John Ruehle Training Center

HELP CLINICS

Saturday, June 2, 9am – noon
Wednesday, June 20, 9am – noon
Saturday, July 7, 9am – noon

Help clinics are a free service held in the Training Center for BVCC club members

Bring your tower, laptop, tablet or smartphone for problem solving.

CLASSES

"Introduction to MS Excel" - Joel Ewing, 4 hours in two parts:
Tuesday, June 12, 1pm – 3pm &
Thursday, June 14, 1pm – 3pm

"Basic Computer Knowledge" – Joel Ewing, 2 hrs
Friday, June 29, 1pm – 3pm

Pre-register for classes by calling/texting Joel at (479)831-5748, email to edu@bvcompclub.org or by signing up at the General Meeting on June 11. Classes are **free to Computer Club members** and are at our John Ruehle Training Center. **Check the monthly calendar and announcements for any last minute schedule changes at http://bvcompclub.org .**

MEMBERSHIP

Single membership is $20; $10 for each additional family member. Join by mailing an application (from the web site) with check, or complete an application and pay at a meeting. **With free access to Help Clinics and classes, BVCC membership is a real bargain.**

Check your Membership Card to see if it is renewal time. We value each one of you.

RECYCLE CENTER HELP WANTED

The BVCC needs your help. If you have an hour or more of time you can give to the Bella Vista Recycling Center, they need greeters to assist people dropping off their recyclables. Our income is derived from dues and from grants from the Recycling Center based on hours donated and credited to BVCC.

MARIE HERR

One of our longer-serving Board members, Marie Herr, has been unable to serve on the BVCC Board for a number of months because of health issues with her husband. When possible, she wishes to resume being active in BVCC, but at this point it is indefinite when that might be. After consulting with Marie and in keeping with our ByLaws, the Board on May 14 selected Bob Shewmake to fill out the remainder of Marie's Board term that runs through August 2018.

Marie has been an essential contributor to the leadership of The Bella Vista Computer Club for over a decade and has served BVCC in a number of positions. She served as BVCC Secretary from February 2004 until August 2007 and as a Board member from September 2007 until May 2018. She has also served as Education Committtee Chair for many years.

Marie still holds the title of Education Committee Chair; altlhough at this time any email sent to edu@bvcompclub.org will be handled by someone else on the committtee until either Marie returns or it becomes clear the position should be reassigned.

PROBLEMS WITH CRYPTOCURRENCIES

By Joel Ewing, President Bella Vista Computer Club

Permission to reprint this article is granted to other member groups of APCUG.

There has been much hype about cryptocurrencies in general and Bitcoin in particular. Enough so, that BVCC had a recent presentation on the topic, with one of the conclusions being that as an investment Bitcoin is highly speculative and should be limited to what one can afford to lose. The price of 1 Bitcoin by design tends to increase, but there have been events that have also caused prices to drop rapidly. The block chain technology on which Bitcoin is built is finding many useful applications, but the long term prospects for Bitcoin and other cryptocurrencies is less certain.

An article in the June 2018 edition of *Communications of the ACM*, a professional computer science publication of the Association of Computing Machinery, on "Risks of Cryptocurrencies" by Peter G. Neumann[1], gives a much

1 Communications of the ACM, June 2018, Vol 61 No. 6, Association for Computing Machinery, New York, NY, pp. 20-24.

more negative view of the future of cryptocurrencies. It points out a number of technical reasons why it is unlikely that cryptocurrencies will ever become a wide-spread payment system. This publication is probably not one widely available to those who are not ACM members: A research library at a major university should have access to it in either hard copy or digital form, but it is not a publication one would expect to find at a public library.

I will attempt to summarize the major points of that article.

The argument presented is that cryptocurrencies are simply not satisfactory as a substitute for conventional currencies: they are by design grossly inefficient and involve risks and costs that cannot be resolved. Most of these problems only impact users of Bitcoins, but some impact society as a whole.

Inefficiencies

New Bitcoins are created by a computational process that requires a significant amount of computational time on a computer, which costs the creator in terms of computer hardware and power costs. The difficulty of the process is designed to keep the supply of Bitcoins less than the demand, so the tendency is for the value of 1 Bitcoin to increase over time. To keep things in balance, as the value of a Bitcoin increases, the difficulty of the generation algorithm also increases. The net effect is is that the Bitcoin network currently is estimated to consume more power than the country of Ireland, and Bitcoin creators (called “miners”) spend about 1/3 of each Bitcoins produced just to pay for their power bills. This does not scale well in a world with serious energy-based environmental problems.

There are limits in the Bitcoin design on the size of transaction blocks and the rate at which transactions blocks can be processed. This imposes limits on the number of transactions per second that can be processed. When the transaction rates approach the global volume limits, only those willing to pay unreasonably high auction-based transaction fees will get their transactions processed. If the transaction processing rate could be increased enough for it to compete with credit card usage, then each node in the Bitcoin network would have to store many gigabytes of additional data per day, all of which would need to be searched to validate each new transactions, resulting in spiraling costs to process future transactions – yet another aspect of Bitcoin that does not scale well. Credit card systems easily support thousands of times the transaction rates of Bitcoin and have done so for years, because it is not necessary to potentially search all past transactions of all customers just to determine if a new transaction is valid.

Risk of Loss

An owner of Bitcoins has two choices, to store his Bitcoins in a “wallet” on his own computer, or to store them on one of a relatively small number of Bitcoin Exchanges. Both choices have been subject to losses, even by computer savvy individuals, either lost through direct theft, lost as a side effect of hardware or software failures, lost because the encryption key that allows access has been lost, or lost by paying for fraudulent services in Bitcoin. If your Bitcoins are lost through an unwise transaction or by someone stealing your key, there is no recourse because unlike credit cards, Bitcoin transactions are irreversible. If lost because you lost your key or because your digital currency tokens were lost, you are also out of luck. Major failures or thefts have occurred on Bitcoin exchanges. Typically those types of events are also associated with loss of confidence and massive drops in the value of Bitcoin.

Problems Using Bitcoin for Payments

Legitimate businesses that offer goods and services for Bitcoin currency don't want to deal with the volatility of Bitcoin value, so they typically use some service to adjust their prices dynamically based on the current value of Bitcoin in some real currency, and as soon as they receive payment, convert the funds to real currency. This means that although the Bitcoin transactions themselves are outside of government control, all government has to do to tax or restrict Bitcoin usage is to focus on the services that convert between official currency and Bitcoin.

The fact that Bitcoin transactions are by design irreversible makes them incompatible with all other forms of electronic payment. This means if you exchange Bitcoins for an electronic currency payment of some kind, even after verifying the electronic payment was credited you have no guarantee that the electronic payment won't be reversed later as fraudulent. If payment is reversed, you have lost the Bitcoins you sold because that transaction can't be reversed. Any service that allows electronic payment in exchange for Bitcoins is similarly at risk: either they must defer delivery of purchased Bitcoins for days, or risk being the victim of a massive fraud attack.

Limitations of a Distributed but Unregulated Cryptocurrency System

In theory, having the Bitcoin ledger maintained on many different servers was supposed to make the system trustworthy by decentralizing the data with each site being validated by the others. In practice, the consolidation of mining into less than 10 entities, self-chosen by their willingness to consume electric power, means that only a majority of that small group effectively controls the Bitcoin system. The value of Bitcoin is simply what people are willing to pay, which makes it vulnerable to sudden collapse if there is a loss of confidence and a drop in demand.

Because there is no regulation, there are a large number of Bitcoin scams, both security schemes and Ponzi schemes, to entrap the unwary.

That fact that exchanges are totally unregulated means that it is not uncommmon for one to collapse from theft, fraud, or incompetence with loss of many Bitcoins from the exchange.

Another obvious downside of cryptocurrency is that its apparent anonymity and irreversibility of transactions attracts those with criminal intent. If you are the victim of a fraud, you can't identify who defrauded you and can't get your Bitcoins back. If cryptocurrency makes it easier for criminals to launder money and harder to bring them to justice, that is bad for society as a whole.

Anonymity is Not Absolute

The perceptions that all Bitcoin transactions shield the identities of all parties to the transaction is not 100% true. While it is true that the actual names of the individuals involved in a single Bitcoin transaction are hidden, the fact that all transaction history is visible and a unique code represents the same individual means that associations can be deduced. The transaction history also includes Internet IP addresses, which may significantly limit the possible real names associated with the transaction , especially since even non-fixed IP addresses from an Internet Service Provider may remain unchanged for months and narrow the search to a single street address. If Bitcoins are used to purchase physical goods from a vendor, the vendor has to know a physical shipping address. Large transfers between Bitcoins and real currency may leave other currency audit trails that can be correlated to Bitcoin transactions. Those techniques may be sufficient to establish the actual names of parties to a Bitcoin transaction.