"SOLUTIONS ARE OUR BUSINSESS"

APRIL 2016

AaSys will be closed on May 30, 2016 in observance of Memorial Day.

Bitcoins/Blockchain and the Future of Banking

Bitcoins was created in 2009 as a way to have another currency other than actual money to make transactions on the Internet. The theory behind bitcoins, also known as cryptocurrency, was to cut out the middle man - the banks. One of the main selling points was to ensure no single institution would control it and people would have the ability to make purchases online anonymously. Each bitcoin transaction is recorded in a public log using the user's wallet ID; names of the buyers and sellers are never revealed. While this helps keep the transactions private, it also served as a way to not easily track who exactly made the purchase.

Bitcoins are stored in a virtual wallet on the cloud or on the user's personal computer. Over the years many merchants have seen the popularity of bitcoins rise hence getting in on the trend and accepting bitcoins as a valid form of payment. Like most products, bitcoin has found a way to enhance the currency and has led to the development of blockchain technology. Blockchain is a public ledger of all bitcoin transactions that have ever taken place and produces a verifiable method of tracking usage. Once it's recorded, it can never be deleted. The blockchain is essentially like a bank statement for bitcoins that are stored in chronological order and has complete information about the addresses and the user's balances from the beginning of the block. The information is stored on a global network ensuring that it's safe and free from hackers. Banks are not too keen about bitcoins, however the blockchain technology has peeked their interest.

Big banks are taking a close look at the blockchain technology and how it can potentially simplify banking. Here are a few of the benefits the banks are looking into:

♦ Security is the name of the game–The blockchain ledger is distributed across thousands of computers which means it is merely impossible for hacker to penetrate, which helps improve security for banks.

♦ The reliability factor –Currently, if a bank's system goes down, users are unable to perform transactions. However with blockchain technology, the bank's system would continue as normal. No single authority has control, which means that if there's an issue, the rest of the network will continue to function as normal.

♦ It's cost effective- Banks believe it will help bring down cost on international transactions and most importantly save on transaction time.

The technology is still up for debate, especially in terms of regulation and access. However, many banks such as Citi Group, Bank of New York Mellon and Wells Fargo are testing the waters. They see enormous potential and don't want to miss out on the next wave of technology that has the ability to help customers and their bottom line. Right now, blockchain apps are being built to handle the next generation of services. While this may be a long way from becoming implemented, banks are more than willing to keep an open mind on technology that may have the potential to produce 100% accuracy while also providing speed and security.

Securing Your Printers

Security is at the top of the list for many companies. It has been reported that the annual cost for a company to resolve cyber-crime is $7.7 million on average. Desktops, smart phones and tablets are not the only devices that can be infiltrated by cybercriminals. Printers are also prone to malicious attacks and are often over looked.

As printers and imaging devices become more sophisticated they also become more vulnerable to attacks that can compromise the networks. We think of printers as just a device that prints our work on paper, however, just like many smart devices, printers also store information such as previous print jobs. If a hacker is able to infiltrate the printer those previous print jobs which could contain sensitive information can be exposed.

Many of today's printers, both wireless and non-wireless, can connect directly to the Internet. They also offer administration and remote control via a websites, but if not properly secured, an unauthorized person could seize control of the printer from a remote location. Here are some tips that can help keep your printer safe:

• Keep your printers' software up to date.

• If the printer can be accessed wirelessly, ensure that the Wi-Fi network is protected.

• Set permissions on your network printers to control who can and can't send and manage print jobs.

• If you do choose to store print jobs on the drive, ensure that it is encrypted with strong encryption methods.

AaSys
Solutions are our Business

Save The Date!

Our Next ISO Peer Group Meeting will be in Florida, West Virginia and Tennessee!

Come join us at our next Information Security Officer Peer Group Meeting in Florida, West Virginia and Tennessee!

Tampa, Florida

Date: Friday June 10, 2016
Time: 9:30 AM – 3:00 PM
More Details to Come on this Event!

West Virginia

Date: July 2016
More Details to Come on this Event!

Tennessee

Date: July 2016
More Details to Come on this Event!

WHAT'S NEW!

AaSys is excited to announce the launch of our new redesigned website coming this summer! The new website has been designed to provide the ultimate user-friendly experience with improved navigation and functionality allowing our customers to access information easily. Stay tuned for the official launch date!