On the Origins and Variations of Blockchain Technologies:

In their article “On the Origins and Variations of Blockchain Technologies,” Alan Sherman, Farid Javani, Haibin Zhang, and Enis Golaszewski break down blockchain technology for the reader – how it works and what it is used for.

According to the authors, blockchains are essentially virtual ledgers comprised of nodes that are indefinitely linked together, creating an unchangeable directory of all transactions. Access, control, and consensus policies determine the overall information handling of the blockchain process. Access policies determine who has access to any given information, control policies determine how blocks are added to the blockchain, and consensus policies determine what the final and irrefutable ledger contains after additions to the blockchain.

The idea of the blockchain can actually be derived from a concept contrived back in the 1970s, called a distributed database. More specifically, it is based on an tree structure called the Merkle Hash Tree, which is a linear tree with time-stamped nodes so that past additions can be found, and nothing can be meddled with except what is on the end of the tree using public-key cryptography (recommended by Merkle, but first implemented by Bitcoin). Essentially, blockchain comes down to being a publicly maintained ledger by mutually suspicious groups, which was an idea known as the vault system crafted by David Chaum in 1979. The vault system is dependent on public ceremonies that occur as new nodes are added to the public ledger, which is the ability for the public to inspect, test, and view new nodes added to the ledger to ascertain what is accurate. In a successful vault system, Chaum describes four different roles: watchers, doers, executives, and czars. While watchers passively watch the state of the ledger, doers carry out actions within the system. Executives confirm the legitimacy of new nodes added by doers, and czars manage who the executives are and what policies they follow. Interestingly, Chaum leaves it open to the reader to determine whether those four roles should be carried out by computer programs or humans.

While the permanent and unchangeable aspects of blockchain prove useful in the financial world, the authors bring up other challenges that come with the use of blockchain, including the need for privacy versus indelibility, anonymity versus accountability, and current engineering decisions versus long-term use and security.

As for what I think of blockchain technology, it is certainly here to stay, but I often wonder in what capacity. Currently, it is used to manage new global fiat currencies, but given how new the subject is and governments’ ability to delay decisions, I wonder how that will change with government regulation. Will independent nations have their own blockchain currency systems, as they do current currency, or will it continue to act almost like gold in that the value is globally recognized and readily utilized? I am sure I will find out in the next 10 years.

Cloud Computing and the Common Man:

John Viega in 2009 wrote the article, “Cloud Computing and the Common Man” as the usage and popularity of cloud computing began rising in the early 2000s to help his readers understand the technology and how it is actively utilized. Viega writes that cloud computing is the process of having an “unseen cluster of resources on the Internet” perform operations as opposed to the client-side device. There are three types of cloud systems as of 2009: software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS).

SaaS requires any given user to purchase a subscription to an application or software product where some or all of the data and/or code exists elsewhere but the user’s device. A great example is Google Docs – it stores documents on Google’s server instead of on the user’s device as Microsoft Office would do with a Word document. While users can edit Google Docs on their machines, the data is only temporarily there before being saved back onto Google’s server where it will remain. PaaS is very similar to SaaS for the user, but instead of designing the program to run and/or store data on the creator company’s Web infrastructure, it is built to run elsewhere. IaaS, similar to PaaS, allows the developing company to choose the software’s runtime environment. This is an especially useful option for providers that want to control how many virtual machines are actively in use in order to be more cost-effective.

One of the dangers of cloud computing is that sometimes personal or private information is the content being shipped from the user’s machine to servers elsewhere, which opens opportunities for hackers to steal data in the transfer process. Cloud system providers help deal with this issue by keeping all the code a hacker might want to toy with to achieve their goals on the server-side of the cloud computing process, where changes in the system due to a hacker’s actions can be easily monitored by IT staff. However, cloud system providers must be careful when requesting data from users that they verify the queries so that hackers cannot ship a code-modifying query to the back-end where it could have disastrous effects. Essentially, cloud system providers want to ensure that hackers cannot easily acquire application-essential code, which requires the provider to assume that the entire client-side is unsafe territory. SaaS and PaaS both rely heavily on the cloud system provider’s security, whereas using IaaS, developers have much more control over security since they can determine the application to run on separate virtual machines running on the same physical machine. Viega recommends that any organization using cloud-based solutions for storing data should also maintain local data backups in case of lost or hacked data in the cloud.

Since 2009, cloud computing has obviously come a long way. Back in 2009, I imagine cloud computing was mainly utilized by corporations, but since then it has become necessary for everyday personal users. Google even extended the use of cloud computing to the gaming industry with the creation of Stadia, which allows players to run computation-heavy video games on any screen that has a connection to the internet (and therefore access to Google’s servers). It is amazing to see how while Viega and others might have been wary of cloud systems back in 2009, it is extremely commonplace 12 years later.

Data Security in the World of Cloud Computing:

In their 2009 article “Data Security in the World of Cloud Computing,” John Harauz, Lori Kaufman, and Bruce Potter dive into the background, purposes, and security of cloud computing. One of the first ideas that the authors point out is that cloud computing requires a heavy amount of trust on behalf the user to the cloud computing provider to provide security for their information as it is passed to/from and stored on provider’s servers.

But before delving into the security concerns, the authors describe the background of the cloud. The idea originated back in the 1960s from J.C.R. Licklider with the advent of the Internet, which is a global interconnection of computer applications and information. Cloud computing is a “service-oriented architecture (SOA),” which is to provide a “scalable services delivery platform,” allowing users to access cloud provider computation power from their devices connected to the Internet. There are several different types of clouds used for various purposes, including infrastructure clouds (for hardware management), software clouds (for software management), and application clouds (for application or social networks) among others. Salesforce.com and Amazon Web Services were pioneers in the cloud computing industry, providing various cloud-based services to users. Other big tech companies such as AT&T, Google, and Microsoft all entered the cloud computing industry as its usefulness and necessity for future computer usage became apparent. However, cloud computing requires a critical level of trust for the cloud provider to keep the user’s data safe and also perform the proper operations.

While cloud computing effectively moves the computation load from the user’s machine to the cloud provider’s servers and reduces the user’s machine’s need for computing power (making heavy computations more affordable), it comes at a risk. In order to maintain security, cloud providers use encryption schema to safeguard data stored on their servers, have access barriers to prevent unauthorized access to data, and have routine data backups to prevent the loss of data. Some interesting questions that the authors raise about the security of information are: “Who has jurisdiction over data as it flows across borders? Can governments access that information as it changes jurisdiction? Is there more risk in storing personal information in data centers that belong to a single entity rather than in multiple data centers?”

In 2009, the answers to these questions were unknown and left as “yet-to-be-written law,” but 12 years later I do not think I know the answers to any of these questions. It seems that today, there are more concerns with user privacy (data collection, targeted advertising, etc) than there are with cloud computing security.

Never Mind Pearl Harbor – What about a Cyber Love Canal?:

Written by Sean Smith of Dartmouth College and John Erickson of Rensselaer Polytechnic Institute in 2015, “Never Mind Pear Harbor – What about a Cyber Love Canal?” tackles security and privacy issues of our current information infrastructure. After all these years of exponential development and use, the current information infrastructure has serious vulnerabilities that make it as vulnerable and defenseless as Pearl Harbor was during WWII.

As the Internet of Things – computers controlling more everyday aspects of life, such as thermostats, household appliances, and automobiles – becomes increasingly more real, the possibility and threat of malicious usage simultaneously becomes increasingly more real and dangerous. Smith and Erickson draw upon the events of Love Canal for an analogy to a possible outcome of the implementation of the Internet of Things. In Love Canal, chemical waste was buried under land that became used for homes and schools, leading to health problems within the community and later, complete abandonment of the area. If pieces of the current information infrastructure were to be “infected” as Love Canal was by loss of control, this could lead down a path to “cyber brownfields,” which would be the internet equivalent of an abandoned community.

Smith and Erickson then dive into pointing out the weaknesses of the current information infrastructure. Input flaws (such as buffer overflow) continue to pervade cyberinfrastructure, re-using standard components (as is common in the world of engineering to reduce waste) can lead to security issues in the form of leftover malware, and current password authentication is an exceptionally weak form of security since people share, reuse, and choose weak passwords. The authors predict as the IoT continues to be implemented, if current upkeep methods persist such as not updating or confirming the security of old devices, serious future issues could arise as those security issues could lead to greater effects in our daily lives. If compromised machines in the IoT do not shut down, it could lead to arbitrary actions that create worse situations than if it had just turned off, such as if an autonomous vehicle turned left on a read light into oncoming traffic rather than remaining stopped. People already struggle to keep their devices updated and protected, so imagine the failure of upkeep when there are many more devices for each person to oversee and use – it could prove disastrous.

Although I am excited for the day where only autonomous vehicles travel on public roads, Smith and Erickson bring up great points about upkeep and security of such systems. For the IoT to be successful, it will require extremely active upkeep, and in emergencies quick and accurate solutions, which might prove difficult with the comparative speeds of the ability to get help versus the ability for something disastrous to occur.

The Great Wall Syndrome:

In 2005, Michael Thelander wrote his article, “The Great Wall Syndrome,” to discuss the nature of threats to privacy and security online, specifically how the unknown threats on the inside pose extreme danger.

According to a 2004 survey, 70 percent of reported security breaches came from people working within the company. Some other staggering statistics include that 70 percent of staff have stolen key information from their company, and 72 percent of the offenders had no ethical or moral dilemmas regarding their actions if it meant helping themselves. (Thelander, 2005)

With the decreasing size of physical storage hardware and increasing size of storage space (USB pen drives, Apple’s iPod, handheld digital recorders, etc), moving data from place to place has become easier than ever. The data can take the form of malicious code ready to infiltrate organizations’ information architecture, or it can lead to quick and easy information theft. As technology devices, such as the iPod, become more common to carry into and out of the workplace, such devices can pose serious risks to companies with private data.

In addition, companies have to take into to consideration that if they place bans on such devices, not only is it unlikely to actually prevent the usage of easily carried storage devices, but underground movements could also rise in resistance and create worse problems. Instead, Thelander recommends that organizations will need to draw up (or update/modify) acceptable use policies for employees to adhere to regarding technology in the workplace, and also implement network-based management tools to maintain surveillance over the workplace online environment. For example, Thelander recommends the following:

* “prohibit the use of portable data storage media and devices,”
* “prohibit the use of a computer’s USB ports without permission,”
* “prohibit the connection of MP3 and video recorders and players to PCS,”

among other rules. (Thelander, 2005)

As someone now living in 2021 where USB drives are practically irrelevant and smartphones, tablets, and laptops have taken over the workplace, this article almost seems ridiculous. Back in 2005, I am sure the threat felt very real (and am also sure there were serious incidents that lead to large damages to organizations), but Thelander might have had a heart attack if he knew what was coming. Yes, insider information stealing is probably a problem even today, including instances where those insiders brought to light disturbing but necessary information, like Snowden back in the early 2010s. However, to prevent the use of USB ports without special permission would be the equivalent of requiring permission to access the company wi-fi with a smartphone, which is practically unheard of. This article truly surprised me with such a different perspective on technology in the workplace from current standards.

Information Hiding as a Challenge for Malware Detection:

In their 2015 article, “Information Hiding as a Challenge for Malware Detection,” Wojciech Mazurczyk and Luca Caviglione analyze the current state of malware detection. Because of the insanely massive influx of new forms of malware (approximately 130 million new forms in 2014 alone), the cybersecurity industry is having an extremely difficult time protecting against new threats. With the modern sophistication of malware, hackers are able to effectively hide their malware from even the most highly regarded malware detection programs using various information hiding techniques to pass the malicious code into other systems for infiltration and abuse.

The idea of information hiding is extremely old and commonly known, such as steganography, which cloaks secrets in various carrier forms, including but not limited to tattoos and invisible ink to hide information from outsiders. An interesting method for hiding software information is embedding it on a very popular carrier such as using least significant bits of an image’s pixels. Similarly, hidden information can be shared over networks by “manipulating the content of unused flags within headers or by modulating the inter-packet time of network flow datagrams.” (Mazurczyk & Caviglione, 2015)

Because of the comparatively larger number of sensors that smartphones have over personal computers, such as cameras, GPS, WLAN, and Bluetooth, smartphones are extremely susceptible to having hidden information passed in and out. This partially explains the gargantuan 1800 percent increase in mobile malware in 2013 and 2014. Interest in the area of mobile malware and Android’s open source nature has allowed researches to craft malicious applications for the sake of identifying weaknesses in mobile security, such as Soundcomber, which can track button presses during phone calls. Tracking button presses can lead to acquiring extremely private information such as PIN numbers for bank services. Other such malicious applications like Luke Deshotels and AirHopper can communicate via sound and light waves to nearby devices to receive the hidden information without the mobile user ever knowing.

What is truly frightening about this article is that the future trends section at the end left the reader with a less-than-comforting statement that the authors “hope that raising awareness” will result in further research. In 2019, there were over 287 million smartphone users in the United States alone, and just 4 years previous when this article was written, there was little to no research about how to properly defend against information hiding malware tactics. I hope that in the last 2 years and the years to come that mobile security receives more attention from the technology industry as mobile devices become even more commonplace throughout the world.

The New Face of War:

After the revealing of Stuxnet’s successful infiltration of over 30,000 machines, the world was reeling in fear of cyber warfare as a new plane for determining global dominance. Samuel Greengard writes about this new phenomenon in his article “The New Face of War,” discussing the meaning of cyber warfare and its future in society.

Greengard starts by writing about how easy it would be to infiltrate government systems which in 2010, were anywhere between ten and twenty years old – a long lifetime for systems that may hold extremely confidential government data. However, he notes that future cyber attacks targeting civilian structures such as power grids, telecommunication networks, and financial networks are extremely plausible given the damage any such attack could do to a society hinged on electricity and online communication. More interesting are Greengard’s comments about how cyber warfare changes the methods of beating opponents. Where old-fashioned methods included clubbing an opponent to death or bombing the enemy until they turned to dust or gave in out of terror, cyber warfare highlights the value of intelligence and under-the-radar control of enemy information structures.

Perhaps the most spectacular and equally most frightening aspect of cyber warfare is that attacks can originate from anywhere at any time. Greengard references the plausible DDoS attack on Estonia’s government web sites by Russian-hosted servers and how it could never truly be proven whether it was a Russian government-sponsored attack. After the events of 9/11 in 2001, the U.S. people have maintained a healthy fear of terrorist attacks, and terrorist cyber-attacks could prove devastating in the future, and it might never come to light where such attacks would come from. In addition, hacking detection systems such as radar allow for creating holes in enemy defenses for more classic forms of warfare, such as the Isreal sneak attack bombing against a nuclear plant in Syria. For decades now, the United States and the People’s Republic of China have sent cyber attacks across the Pacific in effort to gain any political or economic advantage over the other.

Although there is much to fear about cyber warfare – the possibility of foreign governments obtaining personal information, devastating damages due to blackouts/DDoS attacks, or governments blackmailing each other over gathered confidential information – I find that I am not afraid on a day-to-day basis of such events. Yes, cyber warfare is real and attacks do occur, but either I have enough faith in the United States cyber defense to keep us safe, or I am naively optimistic that nation’s do not actually wish to see the complete downfall and destruction of others, because I truly have no fear of impending cyber warfare. At the very least, it is far superior to getting drafted and sent to the trenches.

Should Sniffing Wi-Fi Be Illegal?:

In his 2014 article, “Should Sniffing Wi-Fi Be Illegal?” Paul Ohm tackles topics revolving around privacy and network communications and surveillance. In the past, United States courts have cracked down hard on individuals and politicians over wiretapping and sharing private conversations publicly, meanwhile in the present day, big technology companies such as Google collect thousands of terabytes of unencrypted, private information. While some believe it is the fault of those who do not encrypt their communications, Google walks a fine line of being able to collect data because of their terms of agreement and the use of the collected data – for their users benefit.

Over the years as technology has quickly integrated itself into modern society, Congress has been forced to make decisions on what is/is not legal as far as collecting others’ private information, and in cases regarding telecommunication have consistently prohibited recording private conversations for blackmail or malicious purposes. Although professional or semi-professional computer users may be able to easily encrypt their communications or find ways to tap into others’ networks to steal information, the average user certainly cannot. When writing laws, the government must consider the needs to protect civilians without advanced computer knowledge, even if some (possibly many) can fend for themselves online.

Ohm also notes that arguing that the benefits of Wi-Fi sniffing by companies such as Google for the consumers outweigh the invasion of privacy is a red herring argument. In addition, he notes that what Google did as they launched a fleet of vehicles that collected data via Wi-Fi sniffing was nearly legal, since wiretap laws solely deal with the collection of communications, rather than service set identifiers or media access control addresses. According to Ohm, Google has never sufficiently explained why exactly they needed to capture packet content in order to provide users with a better experience with Google’s various mapping services.

Having grown up with a technologically oriented father, I have never worried about my privacy online because of various tools he implemented to help keep our identities safe. However, when news of political targeted advertisements based on collected data via Facebook reached me after the 2016 presidential election, I realized just how invasive and abusive big tech companies can be when it comes to privacy and data collection. Just as the founding fathers of the United States saw fit to include a section in the Bill of Rights about maintaining individuals’ privacy, the government today needs to take steps to reign in the intrusive actions of data collecting agencies that disguise themselves as search, email, and social media tools…To answer Ohm’s question – yes, Wi-Fi sniffing should be illegal.

Legally Speaking - Software Patents Are Falling Down:

In Pamela Samuelson’s article, “Legally Speaking - Software Patents Are Falling Down,” she discusses the Supreme Court’s decision that “a computer-implemented method and system for facilitating settlements of financial transactions was unpatentable subject matter as an abstract idea,” and the effects of that decision in *Alice v. CLS Bank*.

Although computer program patentability had a rocky start in the 1970s with the *Gottschalk v. Benson* case over transforming binary coded decimals to binary (Benson’s work was not patentable), in 1981 the Supreme Court swung the other direction in *Diamond v Diehr*, where software was utilized in a rubber-curing process. Hey professor! I just thought I would toss these quick sentences in here to make sure I am not boring you too much. I hope you are doing well and are ready to enjoy summer break! Throughout the 1980s, 1990s, and late 2000s, the tech industry exploded with patents as anything that produced “useful, concrete, and tangible result” was worthy of a patent. However, in *Alice v. CLS Bank*, the Supreme Court decided that computer processes were not patentable because Alice’s abstract concept was simply that but implemented by a computer process. Her abstract concept was not expanded upon or contain extra pieces to “transform the nature of the claim,” which could have deemed it patent worthy.

Since the *Alice* decision, the patentable subject matter guidelines have been revised to better reflect what the Supreme Court deemed worthy, and about three-quarters of patent litigations regarding patents from the 80s-late 00s have failed to hold up in court under the new guidelines. Huge companies such as Hulu, Costco, and Capital One have all successfully challenged patents regarding various computer processes that, in retrospect, seem fairly commonplace. For example, in Hulu’s case, they challenged a patent with a system for using advertising as income and currency to provide consumers with a product or access to content.

Although I am sure lawyers have field days over such court cases regarding huge tech companies and random individuals or small companies with patents for computer processes, I have no sympathy for the people holding onto purposeless patents. I am a firm believer in open-source material for the purpose of pushing the tech industry ever-forward, but to a certain extend I understand some need for points uniqueness within the industry. The capitalist competition that urges companies to invent will fail when every business has access to the latest and greatest code. “Why should I try to invent something new and exciting when somebody else will probably do it before me, and possibly do a better job?” It certainly sounds like a path to a stagnate market.

The Troll under the Bridge:

Written in 2013 by Will McDermott and LLP Emery, “The Troll under the Bridge” discusses the state of technology patent lawsuits in the United States and the ability for random patent holders to sue big tech companies for patent law infringement. As the title states, these patent holders are the trolls under the bridge, blocking the path of progress for the sake of scraping some money from the companies that dominate the market.

More specifically, leading up to and during 2013 there was a slew of non-practicing entities (NPEs) rising from the land of the dead to make their claim against infringers. Even worse, companies that once applied for and received patents for technologies and processes that they no longer require shrug their patents off to NPEs almost as an investment opportunity. The NPE picks up the patent that the company no longer needs (and no longer wants to pay the government fees to keep), the NPE goes out and finds victims to fall prey to patent infringement based on the recently acquired patent, and the rewards are split between the NPE and the company.

Although most NPE patent lawsuits result in settlements to avoid expensive legal fees that would exceed the humble, modest request from the NPE for the use of their patented idea/product/process, there are a few that take NPEs to court over the supposed patent infringement. However, this is an extremely tricky task since in normal patent cases, a company might make a case against patent infringement by discerning between what they produce and what the patent-holding company produces. In NPE patent cases, these arguments fall flat since NPEs do not produce or sell anything, so the defendant cannot easily make such distinctions. On the bright side, joint defense groups sometimes rally together after an NPE accuses several groups of patent infringement to share information and combat the allegations of infringement.

After reading the previous article, “Legally Speaking – Software Patents Are Falling Down,” I could not be gladder to hear about the Supreme Court decision of the *Alice v. CLS Bank* case. At first, I thought it might prove difficult for small tech businesses to find a foothold in the market without easier access to patents, but such ridiculous legal actions like those of NPEs reduce my sympathy for small tech companies almost completely. I would still promote those that ethically seek out patents with ideas/innovations that are patent worthy, but a broad decision like the *Alice v. CLS Bank* case makes sweeping up NPE garbage much easier.