Blockchain and Information Technology

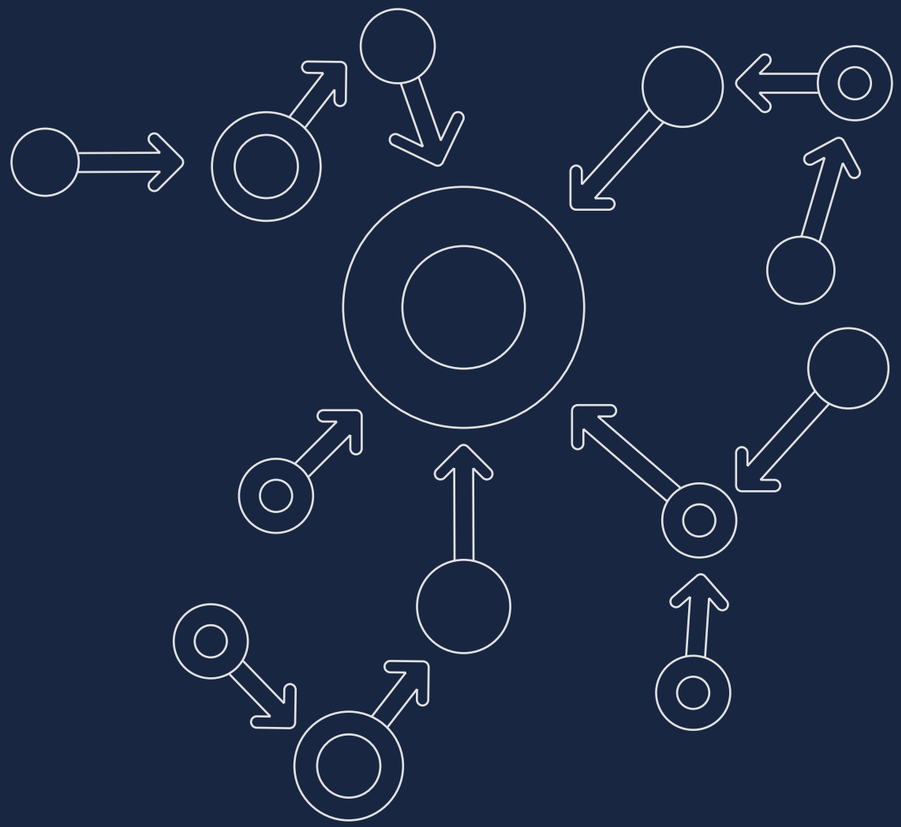
An Industry Analysis

COINACCORD

Blockchain Development Studio

a: 270 Sherman Ave. N., Mill 228
Hamilton, ON. L8L 6N4
e: contact@coinaccord.io
w: https://coinaccord.io

HARNESSING TRANSFORMATIVE POWER THROUGH PERMISSIONLESS INNOVATION.



Addressing Issues in Information Technology

Although it may seem that the technology industry would be the most likely to adapt, adopt, and overcome hurdles faced by technological advances, the truth is that reluctance to change is felt equally in this sector. In many cases, organizations have become accostomed to their business models and are unwilling to change. At times, the risks involved with being a first mover deters companies from engaging with new technology, and unfortunately the prolems we will outline below have existed for

1 CENTRALIZATION

One of the main pillars of blockchain technology is decentralization and the ability to remove dependencies on intermediaries. When it comes to many business models, their inherent centralization of information and services can be dangerous. When a single entity controls a massive amount of data, or services a majority of a population, their customers become easy targets for data breaches. In the last two years alone; Facebook's third party connection to Cambridge Analytica revealed the interests and information of an estimated 97 million users [4], the 2017 Equifax hack resulted in the theft of over 145 million American's social security, tax identification, and driver's license numbers [5], and possibly most concerning, the Aadhar attack on the government ID database exposed the names, identity numbers, and even bank accounts of over 1 billion Indian residents [4]. In most cases, these breaches are the result of simple to exploit vulnerabilities. For example, the Indian ID database was caused by an unsecured API, Equifax used a single, web-based server, and other companies have used publicly accessible servers or failed to implement multifactor authentication. Unfortunately, due to the secrecy and breadth of control that come with centralized services, many of the largest data breaches discovered in recent years have actually been hidden from the public for years.

The lack of transparency in centralized systems leads to a multitude of intermediaries that access information, add unnecessary fees, and increase the time it takes to complete regular business processes. Not only does this lead to issues for businesses that need to maintain a constant margin and offer a competitive timeline for their services, but consumers are usually left holding the bag when it comes to covering costs and dealing with wait times. Corruption can also run rampant in companies that don't feel the need to share information with their clients or the public. Currently, there is not much of a standard when it comes to organizational transparency, and because of this, people are trusting government, corporations, and media less than ever before.[6] The data breaches we initially touched upon have been a catalyst for the distrust, and people are beginning to take more precautions with their data than in the past. However, these vulnerabilities are not their only concern, and although recent increases in corporate

social responsibility have led to businesses touting fair trade, eco-friendly, or sustainable products, the authenticity of their certifications have long come under fire.[7] In general, it's become much easier to form companies and provide services, whether it be online or through intermediaries like Uber and Airbnb. Unfortunately, with such technological advances, it's also become harder for consumers to trust and verify the companies they are interacting with on a daily basis.

2 INFRASTRUCTURE COSTS

Building upon our first issue, the centralization of information also leads to a disconnection of data between companies. This silo-ing of information occurs across many industries, and information technology is no exception. Data disconnects cause difficulty in maintaining databases that need to interact with each other, as well as the ability to draw insights and reveal trends. Even IBM realizes the problem and states that to effectively leverage data, companies need to be able to integrate, govern, and trust each other.[2] Currently, real time information sharing may be extremely difficult or even impossible. Employees are left exporting, importing, and manipulating data, leading to redundant information in databases, manual entry errors, and of course - time wasted. These issues will only worsen as artificial intelligence and machine learning allow for more devices to collect more data independently.[3]

> "MORE THAN $26.5 BILLION DOLLARS WORTH OF REVENUE IS LOST TO I.T. DOWNTIME EACH YEAR."
>
> - CA TECHNOLOGIES

We previously mentioned data breaches, and an important aspect of complying to regulations regarding data breaches is revealing them to customers within a timely manner. Depending on the severity of the data breach, it may be a company's legal duty to report the breach to the public. This means verifying where the vulnerability was discovered, who was affected, and how much information was compromised - nevermind trying to figure out where the threat came from. Verifying this, and other forms of information, becomes a logistical issue plagued by fraud, human error, and lengthy and expensive labour costs.

When you consider how these massive stores of data are owned by organizations, you'll find that these large sets of technological infrastructure not only come with expensive start up costs, but the maintenance adds substantial overhead costs to businesses. Ongoing maintenance has to occur in order to avoid service outages, but the associated down time, and the need for backup storage is not a cheap solution. CA Technologies conducted a study in an attempt to calculate the cost of IT downtime, and after surveying over 200 companies they found out that more than $26.5 billion dollars worth of revenue is lost each year.[1]

3 SECURITY AND EFFICIENCY

We've touched upon some of the lapses in judgement that can lead to information breaches; server security, no multifactor authentication, weak access management. Yet there are countless ways that bad actors can infiltrate systems and abuse data. The lowest level of security that a company must implement focuses around user management and access. Confidential and classified files are protected from lower level employee access and should require multiple signatures before access is granted. Unfortunately, people tend to have issues with creating secure passwords, and if they do, there is a chance they may forget them. Thankfully, well outfitted companies will make use of password management systems, but that doesn't help businesses realize what users are doing once they access data. A major issue in the information technology space is "data tampering", where information is altered either purposely or accidentally.[8] Changes to documents that contain private information is surely a cause for concern, but so too are changes that can affect a company's inventory, transaction records, and work logs. These malicious "insider threats" are carried out by employees of an organization, and each example could easily result in loss of revenue from fraud or theft. Being able to track who accesses files is one thing, but being alerted to changes using a time stamped and signed transaction is a promising deterrent.

Earlier, when we spoke of centralization, we discussed how one company storing a multitude of data increases the likelihood of an attack. These large data stores fall victim to ransomware attacks, similar to the own Ashley Madison sustained, where hackers demanded a payment in Bitcoin before they would hand control back to the company.[9] Imagine how difficult it would be for bad actors to tie someone's email to their name, address, or ID if that information was split apart and stored separately across various machines. In fact, utilizing blockchain technology allows for added security just by having more computers in your network. Instead of having to overtake a single computer, making changes to the system without being caught requires control of over half of a network. If an organization has thousands of computers in their network, the potential reward versus the time and expense it would take to hack a system may not seem advantageous.

Lastly, between the numerous regulations that companies must follow in order to remain compliant, maintaining proper business processes and documentation can easily become cumbersome. Dealing with consumers worldwide opens up businesses to an abundance of data regulations. Canada has the Digital Privacy and Personal Information Protection and Electronic Documents Acts, there's the United State's Cybersecurity Information Act and Federal Exchange Data Breach Notification Act, and most recently the European General Data Protection Regulation. Blockchain provides the potential to automate, without human error or tampering, the processes, documentation, and verification of compliance. Correctly coding such business processes could save organizations hundreds of thousands of dollars in time, efficiency, man power, and legal fees.

Situation Analysis

"THE ONLY CONSTANT IN THE TECHNOLOGY INDUSTRY IS CHANGE"

- MARK BENIOFF

Political & Regulatory Drivers

Data security has been a consistent headline grabber the last few years. As major organizations fall victim to security breaches, more regulations are being passed that protect consumers and their data privacy. Most notably, 2018 saw the implementation of Europe's GDPR, several aspects of this regulatory advancement exist to simplify technology and data storage laws for consumers. Some of the topics under fire include long winded and confusing terms of service, clear and recorded consent, quicker breach notification, and the right to be forgotten.10 Though it is important to note that even though these regulations improve upon the current landscape, they still don't take into consideration blockchain and cryptocurrency advancements. In fact, laws regarding cryptocurrency, and digital money in general, barely exist. The government's speed when it comes to adapting and updating regulations is almost glacial. Thus the technology is being used today with very little guidance and extremely differing outcomes for those who are prosecuted.11

Social Drivers

As more of the world becomes plugged in, people may not even realize how dependent they have become on centralized businesses. A study done last year revealed that two thirds of Americans get their news from social media - an industry plagued with bots, spam, and fake accounts.12 Fortunately, as harrowing as those numbers may seem, people have begun to realize that they have become the product in a data driven world - and they want to make sure they are protected. Younger generations are also looking for peer-to-peer solutions as opposed to falling back on massive corporations. AirBnb and Uber may be newer examples of the sharing economy, but marketplaces like Kijiji and Etsy have long connected local and global buyers and sellers.

Technological Drivers

Blockchain technology has been both positively and negatively compared to the internet and dot com bubble of the early 90's. However, analyzing the dot com bubble may actually provide a source of hope for blockchain believers. Companies like Amazon, IBM, and Adobe were all born in the boom and have not only survived, but thrived afterwards.14 Decentralization, disintermediation, transparency, and security will be the new measures of success for blockchain startups and their success. Blockchain represents more than cypherpunk hype, with the Web 3.0 comes another change to the way humans can interact online. Web 1.0 provided only a means to read data, 2.0 saw the rise of blogs, sharing, and writable data, and now the web 3.0 revolutionizes interaction, machine learning, and automation.15

Economic Drivers

A solid case for a business' economic incentive to utilize blockchain technology and cryptocurrencies would be the ability to tokenize processes within their organizations. Granted, forms of tokenization already exist today in models like loyalty programs. However, the difference is glaring when it comes to valuation and ownership. Tokens would be owned and maintained by the user in their wallet, ownership can be fractional, and users may even chose to exchange their tokens for cash. Recently Security Token Offerings have made the regulated sale and distribution of natural resources possible through tokens. Businesses could tokenize payments, services, utilities, any process where it makes sense. Ultimately, blockchain and cryptocurrencies are leading to a shift in business models where customers maintain ownership of their data and become a more active participant in organizational economies.

Market Dynamics & Competition

Peer-to-peer marketplaces are not a new solution, however, to have enterprises looking at decentralized technology that increases transparency definitely is. Although solutions being implemented at the enterprise level today are not fully decentralized or transparent, major corporations like IBM, Microsoft, Google, and Amazon have all acknowledged and embraced blockchain technology. Currently, the user experience is not streamlined enough to attract everyday citizens, and active users of blockchain technology are by no means the majority, yet the early adopters and developers in the space are working hard to continue creating a new technological ecosystem. Notably, there has been general consensus regarding the growth of blockchain technology and the likelihood that it will not be disappearing anytime soon.13

Benefits of Blockchain Technology

CUSTOMIZABLE

- Organizations can choose to put large aspects of their business onto the blockchain or smaller, individual steps in a process. It's important to realize that many aspects of a business do make for good blockchain applications. However, for those that do, a company may choose to build their own solution or utilize existing architectures.
    - To interact and use trusted validators, companies can use **Stellar's** specialized consensus mechanism.
    - For those looking to maintain a higher level of privacy and remain permissioned, **Hyperledger** is a popular solution for enterprises.
    - Organizations looking to maintain an open source, public model can utilize **Ethereum** technology and their associated applications.
    - If you're looking to speed up business processes you can take advantage of computer power in a decentralized network without having to put any of your data onto the blockchain. Projects like **Golem** allow you to access additional computing power, speeding up processing time.
- Many solutions have already been tried and tested and reside in public databases as customizable, open-source code. Due to the collaborative environment in the blockchain space, you would not have to worry about building a product from scratch, but instead can utilize existing code and build on top of it.
- Smart contracts can automate processes that deal with data entry and reference other databases without needing to export manipulate data. They can be used as escrow accounts, for file protection, to remove redundant processes, as validators, and much more.

TRUSTLESS

- With smart contract interactions on a peer-to-peer network, as long as you can verify the contract, you don't need to place any trust in other parties. Ethereum, the leading platform for smart contract creation, is currently working on an update to their coding language that would make it much easier to read and write code, making the system more usable for all those involved.
- Transactions can be tracked and reported on a public blockchain, meaning that consumers, regulators, or even business partners don't need to trust that certain processes are occuring. Sensors can be set up to record and report transaction to a blockchain, allowing for real time reporting of data validated through consensus.
- Anchoring data to a blockchain allows for validation without revealing information. Information in external databases can be hashed onto a blockchain where the hash represents an unaltered version of a dataset.
- The removal of intermediaries and ability to interact directly provides businesses with a competitive advantage when it comes to fee structures and deadlines.
- When using smart devices to create mesh networks, a single node's failure does not affect the resilience of the network. In contrast to the hub and spoke models of the past, blockchain networks expand points of access to the hub creating a robust network of connected devices, mitigating service outages.

SECURE

- Sharding data increases security as a single file can be broken up into several indiscernible files distributed across a network of computers. Even if one computer is hacked, the information collected would not be a complete, readable file.
- It's difficult to tamper with records that have been verified and published to blockchains since each individual block is linked to the block both before and after it. Through cryptography, hashing creates an input that can only be created by inputting particular values which will always produce the same result. As soon as one of these inputs is altered, the hash will provide a different value, alerting users to a change of record. Going into older files to tamper with data becomes essentially impossible as a bad actor would need to falsify every block since the file they want to corrupt and receive consensus.
- Multisignature access is a form of key management that can be used to protect information, funds, or verify transactions. A particular action (accessing a file, withdrawing funds, receiving a wire transfer) won't be allowed to occur through smart contract technology and the signature of multiple parties.
- The larger the amount of computers in your network the harder it becomes for a bad actor to take control. In order to falsify transactions using a Proof-of-Work consensus model, hackers would need to control over 51% of the computers in a network. Simply put, a higher number of validating nodes in your network, or utilizing an existing network with many validating nodes, can increase your security.

Blockchain Use Cases

The use cases discussed below range from least disruptive to most disruptive in nature. Keeping in mind the available customization of blockchain technology, the earlier examples may be viable as changes to a single process without tokenization, all the way up to trust an aspect of your business to your customers

User Authentication

One of the simplest use cases for blockchain technology may not always be the simplest to implement. However, with strong user authentication and transaction recording, the monitoring and validity of business records can be improved. This comes in a several forms:

- **Multisignature Authentication:** This kind of protection can be applied to various business processes requires multiple parties to approve a transaction before it occurs. Some examples may be needing a supervisor and manager to sign off on a bill payment that's over a pre-approved amount. Another example could be limiting access to confidential documents unless there is a signing authority.

- **Signed Transactions:** A digital wallet in a business could represent automatic parking validation through sensors in your company parking garage, access to confidential files, even tokens for food in the lunchroom - and it also creates an immutable, time stamped record of these transactions. Essentially, if transactions are done through employee digital wallets, they can be tracked, recorded and validated. This is accomplished without revealing employee identities because the system is pseudo-anonymous. Unless employees choose to share their public key with others, only the company that assigns the keys would know who the address belongs to. This particular example could be achieved on a private blockchain that operates inside a business and does not share any data on a public interface. Additional authentication and transaction signatures can also help to reduce fraud, data breaches, and tampering with customer or company records.

Assigning a key pair to employees (this doesn't necessarily mean you need to use tokens) allows for critical steps in their tasks to be monitored and verified, as well as their devices. Think of a wallet with an associated key pair the same way you would think of your personal wallet; yes, you could have a bank card/cash in it (digital and physical money) but you may also have a driver's license (identification and government validated proof that you can drive), a health card (government validated access to your province's health care system), loyalty cards (membership tokens for rewards at approved stores). Each of these can cards could be recreated and represented on the blockchain through your digital wallet and protected by your key pair.

Data Management

Data anchoring and sharding are both implementations of blockchain technology that can secure information while also increasing transparency. In some cases, a business may even defer data to avoid custodial risk and concerns outside of their skillset.

- **Data Anchoring:** Anchoring data allows businesses to maintain off-chain database that can be referenced and verified on the blockchain, without revealing any data regarding what is inside said database. You may use this form of data management when creating copyrighted documents. A business could keep the actual information regarding a copyright out of the public eye in a private database, but create a hash of that information and write it to the blockchain. You now have a timestamped record of the document being created and if anyone tampers with the document, the hash will be altered - alerting you to the change. You're not revealing any private information but still have an immutable record that it exists as a reference to its creation. It can even be used for user management when they want something to be deleted. If the hash of their original file does not return a value in a block explorer (an interface that can search blockchain transactions), the file would no longer exist, proving it was deleted from the anchored database.

- **Data Sharding:** Sharding data refers to taking a single piece of data and breaking it into many pieces that are then stored across a decentralized network of computers. This solution makes it incredibly difficult to hack a company's data since recovering one piece does not allow the hacker access to a readable file. In order to put the file together, it requires the signature of the owner, even those on the network who are storing the data pieces can not gain access to the files. This removes the threat of a centralized data breach since a company would not be storing all of their documents in a single place.

- **User Controlled Data:** Companies may decide that they want certain pieces of data to reside under the control of user maintained key pairs. This could remove their responsibility regarding sensitive information and provide the advantage of customer control. Organizations wouldn't have to take on additional risk and can focus on the aspects of their business that they do they best - which may not be security, encryption, or data management.

Subscription as a Service

The subscription as a service (SaaS) model is a proven system that has been adopted by many organizations globally, however, until recently a SaaS solution on the blockchain did not exist. This definitely created some hesitation for business owners looking to implement blockchain technology who didn't want to experience potential changes to their business processes. Thankfully the 1337 Alliance has proposed EIP 1337, an addition to the Ethereum blockchain's code that would allow for SaaS capabilities combined with intuitive user interfaces[17]

- **User Benefits:** This system may be even easier to use than token systems - there's no need to understand tokenomics or the utility presented in a project's whitepaper. An interoperable system makes wallets aware when users are paying recurring subscriptions fees and prompts a subscription management user interface. Cancel any time from the same application that you use to pay your bills.

- **Organizational Benefits:** Companies will benefit from the consistent cash flow that comes from knowing your subscriber, churn, and conversation rates. Even more valuable is the ability to simplify receiving payments on a global scale from customers using different carriers and currencies. Of course, putting this information on the blockchain would also increase security and transparency when done correctly.

Mesh Networks

Mesh networks are a decentralized infrastructure for routing data, the antithesis of the centralized and more commonly used hub and spoke model. In a mesh network each device has the potential to act as a node routing data back to the hub; mitigating network failure and lowering the costs of infrastructure setup. In the past, they were impractical for various reasons such as network integrity and a lack of incentive to develop the technology. With blockchain,incentives for participation and usage of the network can be tokenized allowing monetization of the technology. Creating a more robust infrastructure for internet service receivers and an overall better internet experience with less downtime and better connectivity

- **Robust Infrastructure:** With smart devices connected as nodes on a mesh network, the number of potential nodes is greatly increased allowing horizontal scaling with more devices routing data back to the hub.

- **Accessibility:** By creating a robust network of nodes, the network can cover a larger area allowing a greater number of users to connect to the network.

- **Tokenized Incentives:** Tokens can be programmed to reward those users who maintain good node uptime, creating a positive feedback loop between node hosts and network users

Tokenization

While early digital currencies focused on the function of simple money transfer, the potential of programmable money in the internet-of-things cannot be overstated. Organizations can look into monetizing several aspects of their offerings through tokenization structures.

- **Bandwidth:** A company could tokenize their bandwidth by issuing digital tokens that represent the right to use the network. This can be combined with a pay-per-use model where the user experience is much more fair than current options and has the potential to reduce wasteful bandwidth usage. Since bandwidth is a finite commodity, users and companies could trade and sell their bandwidth tokens as technological advancements increase demand.

- **Hosting:** as opposed to tokenizing your service, companies could also create a token that incentivises users to grow their network. In this example, if your organization provides hosting services, you can increase the space you have to offer by providing a token to people who share their digital storage space within your network. Companies benefit from a more robust, potentially global network, while creating a peer-to-peer system that includes and rewards participants.

Decentralized Autonomous Organizations

When running a company traditionally a board representing the interests of shareholders would make decisions on the directions of a company or organization this bureaucracy can be a hindrance, decentralizing this power back to the users/members of a community is a powerful idea. Experiments with DAOs have been ongoing since the early days of cryptocurrency, and in 2019 the fruition of these developments are finally beginning to show their value.

- **Improvement Proposals:** Any stakeholder in the organization may submit improvement proposals to the DAO, these proposals may cover any number of decisions.

- **Coded Structure:** Rules and business decisions are pre-programmed and viewable by all in the organization lowering the bloat caused by quarrels and disagreements on direction

- **Transparency:** Every decision and transaction with the DAO can be recorded in a blockchain, greatly lowering the risk of corruption or bad actors colluding in a way not beneficial to the organization, additionally funds may be tracked on the ledger ensuring they are being spent appropriately.

- **Weighted Interest:** As voting in a DAO usually costs a user a certain amount of money there is pressure to be more thoughtful with improvement proposals selected and overall governance of the organization.

IT Solutions

Problem	Solution	Blockchain Use Case
The level of transparency surrounding business practices, partners, and supply chains is low for companies operating today.	Share aspects of your business with users or the public without jeopardizing security, efficiency, or organization secrets.	On a less intrusive scale, companies can opt to put certain transactions onto a blockchain in order to increase transparency regarding supply chain, partnerships, patent documents, or really any business process that involves a transaction. More drastically, an organization could choose to have aspects, or their entire business governed as a DAO. This would allow people to propose and vote on changes, program practices, and record every part of the business on the blockchain. This would be the ultimate form of decentralization as the original owners would no longer have sole say in what occurs in the business.
Information is currently stored in a siloed manner across various organizations, this makes real time data sharing and decision making difficult.	Increase access to public information by sharing databases of information in an accessible network.	By decentralizing information, gathering insights from real time data becomes simpler. Transaction data could be automatically updated on a blockchain providing references to off-chain databases where info is stored. This would simplify business to business transactions and transparency while removing the need to contact several intermediaries when a user needs their data.
Fee structures put in place by third party partners can reduce the trust between an organization and company and lead to customer dissatisfaction.	Reduce the pain points for customers that result from unnecessary fees and costs placed upon them by companies covering third party charges.	Disintermediate using peer-to-peer systems. Deal directly with consumers using either existing applications or creating your own. This can refer to contracts, money transfer, communication - almost anything that you pay an outside company for.

Problem	Solution	Blockchain Use Case
Large infrastructure that is maintained by a single organization can result in expensive maintenance fees and potential service outages.	Create an infrastructure system that doesn't depend on a single point of failure.	Again, mesh networks can provide advantages by reducing the need for down time during maintenance. Even if machines go out on a mesh network, the other nodes have a complete and up to date copy that continues to run. A virus or issue that infects centralized infrastructure could be expensive to fix and result in service outages during the maintenance period. This also includes regular maintenance schedules that many companies conduct during "off hours".
Poorly monitored or maintained databases can lead to document tampering, whether intentionally or accidentally, and errors in inventory management.	Remove the need for manual analysis while adding a level of security and versioning to data.	Implementing multi-signature access to secure documents is not an entirely new process, however, by linking access to a key pair and putting the transaction on a blockchain, businesses would be aware of when documents were accessed and whether or not they were changed (through hashing). Utilizing smart contracts for referencing databases also removes the manual export and import of data that can result in errors.
Centralized systems with closed networks are more prone to data breaches and hacks.	Increase the robustness of your network and use additional security measures to protect sensitive data.	Again, increase network size though decentralization would decrease the simplicity of hacking into a system. The more nodes present in a system, the more of them you need to take control of in order to own the network. Sharding is an extra layer of security that can break sensitive data into many small pieces, split them up across the network, and remove the ability to gain access to a full piece of data by simply hacking a few nodes. Inter Planetary File System (IPFS)is Ethereum's version of decentralized file storage that uses sharding to keep info safe. Storing data on the blockchain is expensive and counterintuitive, IPFS allows for interactive data storage using smart contracts.
Complying to regulations surrounding user information and privacy can be a cumbersome and time intensive task.	Simplify and automate regulatory processes by removing redundant, manual involvement.	Smart contracts can be used to program and automate business processes. Specifically referring to privacy, these contracts can be used to update users, reference data, or create outputs to ensure compliance measures are taken correctly. An organization could program a smart contract to operate according exactly to regulations.

References

1. https://www.informationweek.com/it-downtime-costs-$265-billion-in-lost-revenue/d/d-id/1097919
2. https://www.ibmbigdatahub.com/blog/if-big-data-and-analytics-exist-silo-does-outcome-matter
3. https://www.veriday.com/blog/data-silos-killing-business/
4. https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12#9-chegg-40-million-13
5. http://fortune.com/2018/02/11/equifax-hack-exposed-extra-data/
6. https://www.edelman.com/trust-barometer
7. https://www.theguardian.com/sustainable-business/2016/mar/10/fairtrade-labels-certification-rainforest-alliance
8. https://www.forbes.com/sites/rachelwolfson/2018/07/03/how-a-leading-cyber-security-company-uses-blockchain-technology-to-prevent-data-tampering/#2880cc064529
9. https://www.pandasecurity.com/mediacenter/security/lessons-ashley-madison-data-breach/
10. https://blog.marketo.com/2018/02/biggest-changes-coming-gdpr.html
11. https://www2.deloitte.com/insights/us/en/industry/public-sector/future-of-regulation/regulating-emerging-technology.html
12. https://www.reuters.com/article/us-usa-internet-socialmedia/two-thirds-of-american-adults-get-news-from-social-media-survey-idUSKCN1BJ2A8
13. https://hackernoon.com/the-blockchain-isnt-going-anywhere-here-s-how-to-stay-ahead-today-and-ensure-success-tomorrow-2d3146a82c2e
14. https://blockonomi.com/bitcoin-vs-the-dot-com-bubble/
15. https://wittycookie.wordpress.com/2012/06/04/what-are-the-major-differences-among-web-1-0-2-0-and-3-0/
16. https://medium.com/gitcoin/eip-1337-subscriptions-launches-eacbb947e229
17. https://1337alliance.org/

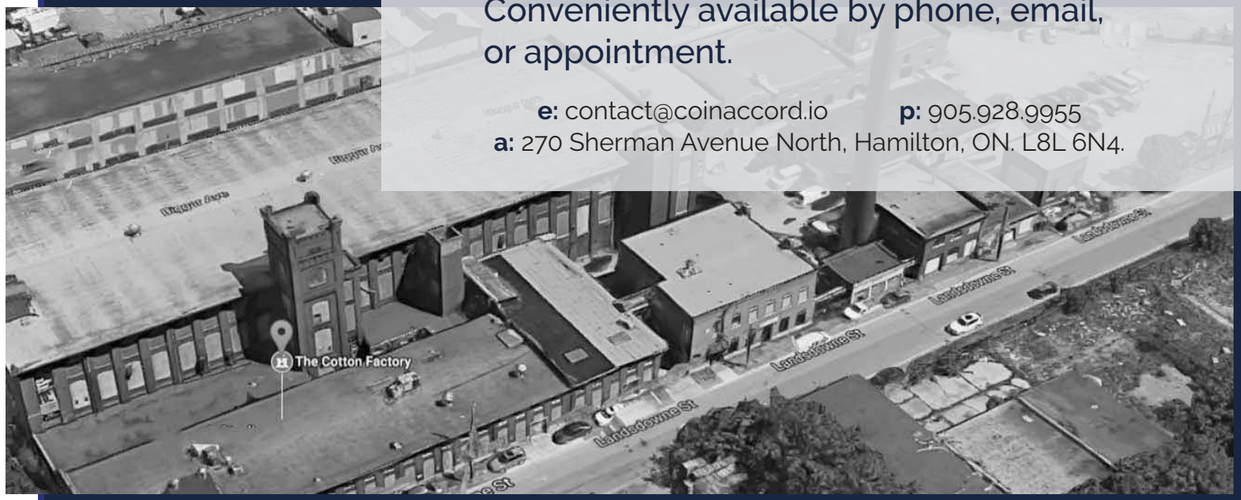
About Us

Ronald Chan
Co-Founder

Ronald Chan is a hands-on entrepreneur and born leader who has spent his entire career immersed in technology and its revolutionary effects. Ron's ambition to adapt and advance as an early adopter of incipient technology has lead him to blockchain technology and its disruptive nature. While applying his more than 25 years of change management, Ron is creating new business models and developing solutions for the web 3.0.

Alex Sheluchin
Co-Founder

Alex Sheluchin is an experienced software developer with an unwavering interest and belief in the efficiencies of emerging blockchain technology. With over 6 years of specialized software development as a Senior Developer at Netquity, a commercial aviation enterprise software firm, Alex has honed his programming skills and gained experience in high pressure, time sensitive projects. He now applies this experience as Coinaccord's head blockchain developer.



Conveniently available by phone, email, or appointment.

e: contact@coinaccord.io **p:** 905.928.9955
a: 270 Sherman Avenue North, Hamilton, ON. L8L 6N4.

COINACCORD