



## BLOCKCHAIN AND PIRACY IN THE MEDIA INDUSTRY

## EXECUTIVE SUMMARY

It's touted to be as disruptive as the internet was when that came on the scene. Blockchain is the technology that gained notoriety for powering Bitcoin. Bitcoin solved the [double spending problem](#) which ensured that the cryptocurrency could not be spent more than once. Some believe that the distributed ledger and trustless consensus rules are revolutionary. For them, blockchain has the potential to radically change existing business models.

But what does it mean for the media industry and specifically its role related to piracy? Is blockchain an enabler of piracy or is it a defender – helping content owners protect their content and intellectual property rights?

This white paper takes a business-oriented look at the characteristics of blockchain and explores how the technology could be exploited by pirates or leveraged by content owners.

# TABLE OF CONTENTS

<b>Executive Summary</b>	<b>2</b>
<b>Chapter 1: Setting the scene</b>	<b>4</b>
1.1 What is blockchain?	4
1.2 Hype or hope?	6
1.3 How is blockchain being used?	6
<b>Chapter 2: Blockchain as an enabler of piracy</b>	<b>8</b>
<b>Chapter 3: Blockchain as a defender of content rights</b>	<b>11</b>
<b>Chapter 4: Barriers to adoption</b>	<b>12</b>
<b>Conclusion</b>	<b>13</b>

# CHAPTER 1: SETTING THE SCENE

## 1.1 What is blockchain?

It was the Bitcoin white paper published in November 2008 under the pseudonym, "Satoshi Nakamoto," that thrust blockchain into the public eye. Blockchain is the technology that underpins Bitcoin. Yet, this innovative technology was actually invented by [Dr. Kelce Wilson](#) in 2000.

Blockchain provides a tamper-resistant ledger of transactions maintained by a network of computer units (nodes). The distributed ledger is cryptographically protected from modification. Transactions are agreed upon through multi-party consensus agreements.

Let's break that down.

"Blockchain is designed to let you transact digital assets but not copy them."

As blockchain is the technology behind Bitcoin, let's use that as the example. Bitcoin facilitates secure online transactions. It does this by using public key encryption. Keys are used as a form of identification. The public key is your identity, or address in bitcoin, in the blockchain and is referenced in each transaction. The private key on the other hand, is only known by you; it is a master password that gives you access to your digital assets and must be protected.

Blockchain is designed to let you transact digital assets, but not copy them. The transactions, once verified, are included in a block which is appended to the other blocks of information in the chain. This chain of blocks (which is the ledger) is then distributed across a Peer-to-Peer (P2P) network of nodes. In other words, it is shared with everyone in that ledger's network. As the information is distributed, there's no single location (e.g. a central server) where everything is stored.

Each node can keep track of all blocks in the chain. Each block of information must be validated across the network by a miner before it is added to the chain. The successful miner is paid a transaction fee as well as a subsidy, which is how new Bitcoins continue to be created. The network does this by following a pre-agreed set of consensus rules. These rules are a vital part of a blockchain. They ensure that all the nodes are on the same page; adhering to the same procedures and guidelines. The rules for consensus or agreement may be based on:

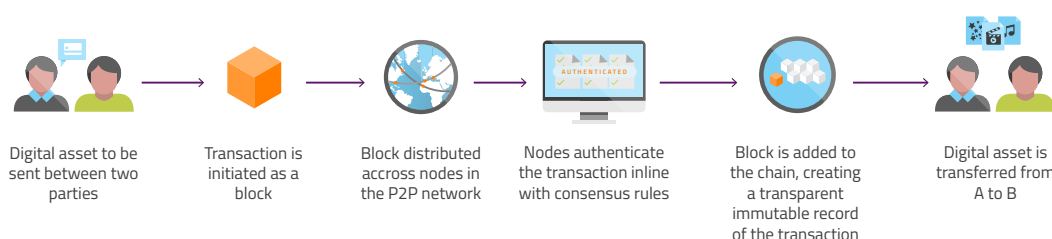
1. **Proof of work.** The node must perform a certain amount of work in order to add a valid block to the chain; this concept is commonly used in cryptocurrencies, including Bitcoin .
2. **Proof of stake.** By this we mean that the node validating the transaction holds a certain percentage of the networks' total value.
3. **Multi-signature.** More than one validator must agree that the transaction is valid.
4. **Practical Byzantine Fault Tolerance.** An algorithm that's designed to settle disputes among the different nodes if one generates a different output to the rest in the network.

It's the consensus rules, together with broad distribution and validation of transactions in the ledger which ensure that there's no need for intermediaries (middle men) or trusted third parties to approve the transaction. Once committed to the chain, all the transactions are public and easily verifiable. This transparency means that blockchains are auditable.

What information is contained in the block? Based on the defined consensus mechanism each block contains, at a minimum, its own data and a hash of the previous block as well as a history of all the transactions. Hash is the term for a unique string of characters or digits assigned to each transaction. If there's any change in the data, then a new hash is generated. The original block can't be changed or modified – it's immutable. And it's this which makes it impossible to tamper with – any changes or modifications are evident as the hash will no longer be the same.

So, in a nutshell...

Blockchain can be a public or private ledger where transactions are recorded and authenticated anonymously (well, pseudonymously); which is shared between multiple parties. Once information is entered into the blockchain it can't be altered.



*Figure 1: High level diagram of how a blockchain works*

It's worth highlighting that although you can manage the rights or record of ownership to an asset in blockchain; you can't, however, manage the transfer of, or access to the asset itself. This is especially true if the asset exists outside blockchain in the real world; such as content or other physical goods.

Where blockchain and the real world intersect, real world challenges will remain. For instance, unless video content is part of the blockchain and is restricted for use in that crypto-sphere, it's difficult to prevent people from copying it. Why blockchain works with money is that all participants are incented to prevent others from copying money and the use of that money is restricted to the cryptocurrency.


## 1.2 Hype or hope?

Let's be honest, distributing content across a P2P network is not new. BitTorrent is probably one of the most well-known P2P networks. Why then is blockchain garnering so much interest?

It comes down to its potential.

The combination of blockchain's transparent distributed ledger, trustless consensus and immutability - which doesn't rely on intermediaries and that can be applied to a wide range of industries - is why it's deemed innovative and disruptive. It offers the promise of being able to lower costs, establish a new way of communicating and change the traditional transactional infrastructure.

Particularly in the financial sector, blockchain has directly challenged the role of key players as a trusted third party. Institutions that have been seen as the central authority for a long time – where all transactions were approved, recorded and stored – are now threatened with obsolescence. And it's not just the financial industry. Due to the potentially wide applicability, any cornerstone institution which is a gate keeper of transactions are now facing a challenge to their way of working: lawyers, courts, governments, etc.



“It comes down to its potential.”

Maybe this is another reason for the hype? Blockchain has single handedly been the catalyst for many established, often viewed to be bureaucratic, institutions to cast off their airs of indispensability and start to innovate to stay relevant.

For some, blockchain is a framework that could reduce fraud, corruption, human error or the cost of paper-intensive processes. For others, it offers the potential to expand their reach by offering secure transactions in countries where central authorities are seen to be questionable or are not fully established: some CIS countries or even parts of Africa, for example.

## 1.3 How is blockchain being used?

Before we delve into the media industry, let's look at a few examples of applications using blockchain in other industries and services.

The most well-known application of blockchain is, of course, Bitcoin. In April 2017, [ABI Research](#) reported that the capitalization of Bitcoin was USD \$16.9 billion; using a conversion price of 1 Bitcoin = USD \$1,040.77 with a circulating supply of 16 million Bitcoins. By September 2017, [Money](#) reported that the price of Bitcoin had skyrocketed to nearly USD \$5,000 which makes the market cap much higher.

Bitcoin isn't the only cryptocurrency. In fact, [ABI](#) state that there's now over 750 digital currencies with a total market capitalization of USD \$25.2 billion.

With the evolution of blockchains that can include business logic, Ethereum introduced smart contracts. This enabled contract agreements to be automatically executed. They also established the de-centralized autonomous organization (DAO) that could be used for more complex governance structures. These developments opened the door for other applications of blockchain technology to be created. To highlight just a few:

- [OpenBazaar](#) is a blockchain-created P2P, eBay type, e-commerce site using P2P rules to participate.
- [Goldman Sachs](#) predict it will save USD \$6billion a year through optimized clearing and settlement banking procedures; providing lower headcounts and back-office IT costs.
- [Storj](#) is a blockchain-based, cloud-storage company; using encryption keys to access stored data.
- The US Securities and Exchange Commission approved the use of blockchain as a share ownership register for online retailer – [Overstock.com](#).
- The [Estonian government](#) is embracing blockchain for a plethora of their registries such as tax, notarizing marriages, birth certificates and business contracts as well as eHealth to secure the medical records of over a million citizens.



“Blockchain is a nascent technology.”

Besides these, applications are envisaged for the issuing of passports, tracking supply chain deliveries, voting systems as well as providing transparency for how aid money is spent.

Despite the hype and it's potential, it's important to note that blockchain is a nascent technology. Beyond the well-used Bitcoin, a lot of the other applications are largely untested on a wider scale.

## CHAPTER 2: BLOCKCHAIN AS AN ENABLER OF PIRACY

Moving more into the media industry now, let's examine how the pirates can exploit blockchain to accelerate either content redistribution or exploit the software for other criminal activities.

Beyond the obvious fact that cryptocurrencies allow the pirates to get paid and remain anonymous, leveraging blockchain's distributed network as a content repository is definitely prevalent; either as a torrent site or Dropbox.

Play, on [ZeroNet](#), probably one of the best-known examples of a distributed torrent site utilizing blockchain.

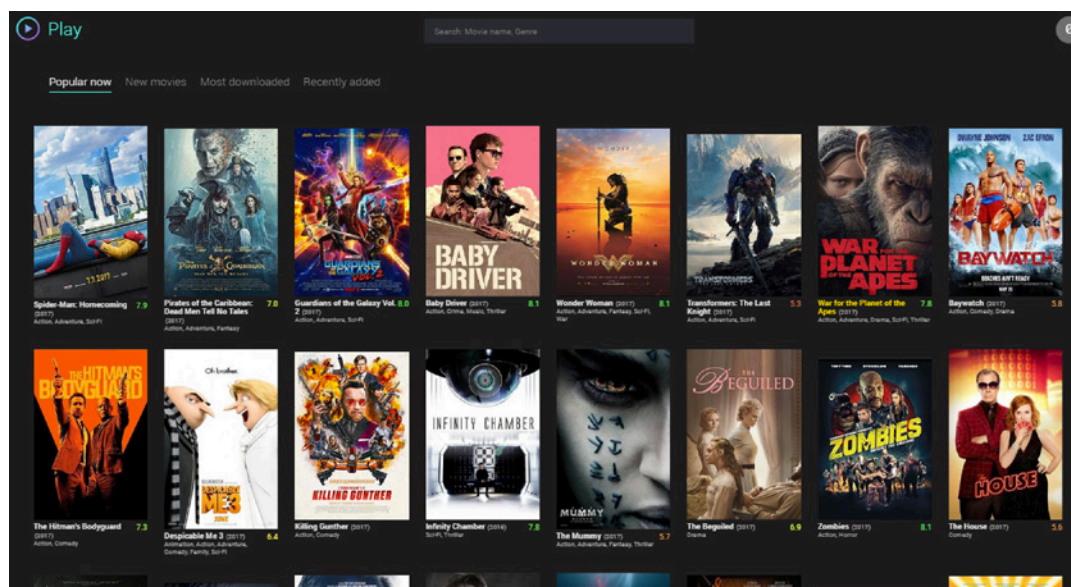


Figure 2: Play on ZeroNet

Play is only accessible for those people who have installed the ZeroNet software. The creators claim is, that with blockchain, unlike its counterparts such as The Pirate Bay, Play is impossible to shut down.



Then there's decentralized streaming options. An early example of this was [PureVidz](#).

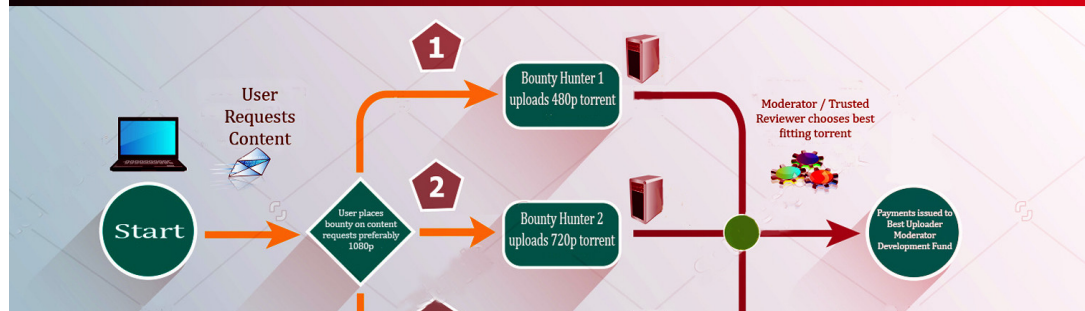


Figure 3: VidZ pirate streaming site utilizing blockchain

We've not seen much activity here since February 2017, but it's worth highlighting in terms of what could be established. They also had a concept of "bounty hunters" who were rewarded in cryptocurrency by the requester for sourcing the desired content. No doubt, this concept will succeed in other scenarios.

There's also the potential that blockchain could be used to circulate links or URLs to pirated content instead of a search option. It could also be envisioned that it would be possible that the block transaction could be to share a pirated movie. The entire movie is contained within a block (or blocks) and those who would like to watch that movie would then buy the key to access it using the preferred cryptocurrency of the pirate. Just like Play, if content is illegally redistributed using blockchain in this manner, then it would be much harder for enforcement activities to be impactful.

Although legal, there are a number of blockchain-based solutions that are appearing which revolve around sharing content. Livepeer, LBRY, DECENT, Alexandria and SingularDTV are all examples. Despite the low uptake at the moment, their attributes of uncensored content, incentive schemes for adding bandwidth and new content as well as using cryptocurrencies are characteristics that would certainly appeal to pirates. Are these sites at risk of being exploited for illegal activities?

[Livepeer](#) is a distributed live video streaming platform offering cheap, uncensored content; where users contribute unused bandwidth in exchange for crypto-tokens.

[LBRY](#) is a marketplace for digital goods e.g., games, movies or college lessons, which offers an incentive to encourage people to contribute and make it the most complete – the go to marketplace. The client application allows users to search, pay and download as well as contribute bandwidth.

[DECENT](#) offers a way of publishing content; users are rewarded for being “a seeder.” The platform is dedicated to the freedom of speech and it states that no third-party can control or influence the content. Authors and artists publish their content and specify its price. The application encrypts the content and finds publishers. The audience can pay to download it.

[Alexandria](#) wants to let content creators determine how their content should generate revenue. The application developed by Blocktech lets users publish, distribute, and sell anything and there’s a built-in payment layer. The site allows for all kinds of free and paid content. Its stance on ending piracy is to make sure that content is widely available as fans do want to pay but just can’t access the content when or where they want it.

[SingularDTV](#) was launched in October 2016 and it’s a blockchain entertainment studio. Its goal is to help artists manage projects - from development to distribution - through tokenization. The founders view it to be an alternative transparent P2P industry and they want to give artists control over their content as well as the revenue it generates.

### Fighting piracy which utilizes blockchain

Although more difficult, it is possible to fight piracy despite adding the pseudonymity that blockchain and also the Darknet injects into the equation. For example, recently two of the largest known Darknet marketplaces AlphaBay and Hansa Market were taken down. [Europol](#) estimated that transactions in Bitcoin and other cryptocurrencies since AlphaBay’s creation in 2014 reached USD \$1 billion.

The key is to work with a security partner who has the specialized expertise in monitoring, detecting and investigating such activity. Many Clearnet tools and techniques are not transferable, as such a different approach is needed in the shadowy depths of the Darknet. Not everyone has these capabilities.

“A different approach is needed in the shadowy depths of the Darknet.”

## CHAPTER 3: BLOCKCHAIN AS A DEFENDER OF CONTENT RIGHTS

When exploring the opportunities of blockchain for content owners and rights holders, the cryptocurrency, immutability and smart contracts are characteristics that naturally hold promise. After all, blockchain serves as a registry to track and manage assets. It provides evidence of ownership, usage rights, records status plus records transfers.

From a monetary standpoint, cryptocurrencies could provide another payment mechanism to purchase content. Certainly, Bitcoin is being used and accepted by a growing number of companies. In fact the Hollywood studio, Lionsgate, is one such company.

As highlighted in section 1.3, there are 750 digital currencies in use. One potential for content owners to consider might be to create their own – MovieCoin, for instance. By establishing the cryptocurrency also allows the content owner community to define the consensus rules. For example, it would allow them to articulate what happens if someone re-sells or shares their purchased content to another party. Maybe the forwarding sales price has a small percentage or fee which reverts to the content owner?

“A digital passport could be assigned - a blockchain equivalent of DRM.”

Tracking of ownership (or provenance) remains at the heart of the content lifecycle. Forensic watermarking is a proven way to achieve this. If we look at how blockchain could complement existing technology maybe parallels can be drawn from [Everledger](#).

Everledger, founded by Leanne Kemp, uses blockchain and smart contracts to track and record the provenance of diamonds. Diamonds are high value content and they are susceptible to being the target of criminal activity. Sound familiar? Using Everledger, there's a digital passport for each diamond. With blockchain, its immutability transparently records the origin and subsequent trail of ownership. This would seem to suit the media industry as well. Premium content could be assigned a digital passport, a blockchain equivalent of DRM and the tracking of ownership could be seen as blockchain supporting watermarking.

In section 1.3 , some of the examples highlighted blockchain's potential to optimize processes, make them more efficient and cost-effective by removing the intermediary steps. Maybe this could also be beneficial for content owners? For example, a consumer requests, on blockchain, their chosen content through smart contracts, the transfer of the digital asset is recorded and delivered over the distributed network, and immediate payment is received in cryptocurrency. All of this is done at once and directly between the content owner and consumer.

In Chapter 2, there was the example of Vidz offering a bounty for those who could obtain their requested pirated content. Why not turn this around and use the incentivization to identify illegal content? That is certainly the premise of [Custos](#). Individuals (or bounty hunters) are rewarded when they find new infringements. Custos does this by embedding cryptocurrency directly into the copies of the media which are distributed. When the bounty hunter claims their reward, Custos is able to inform the content owner of who was the original recipient of that content.

## CHAPTER 4: BARRIERS TO ADOPTION

As we've seen, the potential usages of blockchain are many and varied; applicable to all industries and services. Although saying that, it's understandable that some institutions who believe their role will be minimized with the potential use of blockchain may want to delay adoption. For general adoption of blockchain, the challenges are twofold. It's about finding practical uses for the disruptive technology that solve real problems other than a distributed ledger contract or escrow (which you can argue is a special version of a contract). And there's the technology itself.

The advocated premise is that blockchain, due to its distributed nature, is harder to attack – less vulnerable. Hackers don't have a single server or central database to attack. Bad actors have to put in considerable effort to reap rewards.

But, it is possible. Despite the hype and the potential surrounding it, blockchain is a nascent technology. It's still not known how secure the system is or where unforeseen vulnerabilities may emerge. Only when the technology is used more widely will the extent of potential vulnerabilities be uncovered.

Some of these vulnerabilities have come to light. In fact, one caused the June 2016 split to Ether and Ethereum Classic. A hacker took advantage of a DAO vulnerability which resulted in a USD \$50 million heist of Ether. Another example is the hacking of [Coinbase](#) - the world's largest exchange for trading cryptocurrency.

Blockchain is also not immune to collusion attacks. Because the chain operates on a consensus model, it only requires exceeding 50% mining power to cheat the network into accepting unlawful transactions. While this is extremely difficult to imagine in the main Bitcoin blockchain, in smaller chains or forks with lower participation, it is much easier to imagine this type of coordinated fraud.

Privacy is another area of concern. Although encryption keys are used, which hides the true identity of the user, there is certainly more that can be implemented to improve the weak form of pseudonymity that exists at the moment. The encryption key is fully anonymous, the point is that its path through the block chain, as it pertains to the real world, is not. Because the approximate time of the transaction and value are recorded publicly, it is possible to infer information about the user or merchant, such as their turnover or buying profile, based on the transaction even though their account balances are not recorded. Although the public identity is opaque in and of itself, the usage of the identity in the context of the blockchain and real-world transactions weakens the pseudonymity of the keys as applied to the blockchain.

"It's still not known how secure the system is or where unforeseen vulnerabilities may emerge."

Besides the security aspects, there's performance and scaling to consider. The recent August 2017 Bitcoin fork which led to the creation of Bitcoin Cash (BCash) was underpinned by the disagreement about the size limit of the block. The high volume and demand for Bitcoin and its 1MB block size limit meant that transaction times could take from 10 minutes up to over 40 hours during peak periods. Some of the Bitcoin community wanted to increase the size limit to 8MB per block in the hope it will reduce the transaction times.

There's no doubting the potential of blockchain. Given the interest and hype around the technology, it is likely that some of these issues will be solved as blockchain continues to evolve. This should increase the adoption rate.

## CONCLUSION

Since blockchain is in its infancy, it is hard to predict how reliable the technology will be or how widespread it will become. It could prove to have the capacity to introduce a new level of trust in the way business is conducted, or it may not survive [Gartner's Trough of Disillusionment](#).

Before investing heavily in solutions using blockchain, there are a number of factors that should be considered.

Firstly, there are the unsolved issues of privacy, security, performance and scalability. Then, there's the distributed ledger. Some financial organizations which have started to explore how blockchain could benefit them by implementing a private network instead of a public one, have concluded that they could achieve similar results without blockchain. Other distributed networks could work just as well, so maybe blockchain isn't the panacea.

Vulnerabilities in software are unfortunately part of the digital world. The need for a comprehensive anti-piracy and cybercrime prevention strategy is critical whether you use blockchain or not. However, at its current stage of maturity the risk with blockchain is higher. It's a new technology. The full extent of its weaknesses is not fully understood. Using the technology at this stage of its development could leave you open to attack in the future.

As to whether blockchain is an enabler of piracy or defender of content rights? This is yet to be seen. Ironically, the improvements necessary to protect consumer privacy may ultimately make the blockchain an ideal place for pirates as well.

What is clear, is that when it comes to protecting your content, revenue and brand, it's important to work with a partner that understands the changing pirate landscape and has experience in anti-piracy activities as well as has experts in cybercrime security.

## About Irdeto

Irdeto 360 Security is an end-to-end, pre-integrated solution that meets even the most stringent security requirements, enabling operators and content owners to offer premium media services, such as 4K UHD VOD, live sports and early release window movies. It provides unparalleled breadth and depth to meet changing security needs, from content protection, to piracy control and cybercrime prevention, to key management by a trusted authority. Its proven success comes from the combined power of innovative technology, a diverse team of experts and a global network to deliver best security practices.

With Irdeto, content owners, sports rights holders and distributors (operators) have the confidence that they have a true and accurate picture of piracy and that they are using the best-in-class products & services to combat threats now and in the future. Only Irdeto offers an end2end piracy control solution integrating watermarking, online piracy detection, enforcement activities and cybercrime capabilities with a proven track record of success on a global scale.

Irdeto has a global team of multi-discipline specialists and has a successful track record in rapidly identifying, disrupting piracy and leveraging its established networks to track down pirates and their supply chains. This combined with Irdeto's world renowned content protection solutions mean that Irdeto is well placed to be the trusted security partner of choice.

For more information about how the Irdeto Piracy Control & Cybercrime Prevention solutions can help you in the fight against online piracy, visit the website: [www.irdeto.com](http://www.irdeto.com).