



IdeaBlock

# What is IdeaBlock?



**IdeaBlock is a suite of blockchain-powered tools that safeguard your IP.**

Our innovative products work to shield users from future legal challenges involving the products and services they work hard to develop and bring to market.



**IdeaBlock is a supercharged cost-saver.**

Last year, the average total cost of obtaining a U.S. patent was over \$60,000 – a sum that forces businesses of all sizes to leave many potentially valuable ideas unprotected.



**IdeaBlock is insurance.**

The traditional government-centered avenues for securing IP protection are rife with uncertainty, shifting legal standards, and contradictory agency guidelines. IdeaBlock provides a strong foundation so that you can build valuable IP portfolios with a sense of confidence and security.

# What is a Blockchain?



A blockchain is a form of distributed database that stores data describing transactions between anonymous users.



Unlike data stored on traditional databases, data blocks are tied together and timestamped using very large cryptographic numbers called “hashes.” This ensures that the blockchain data is unchangeable and can therefore be verified as a true – forever.



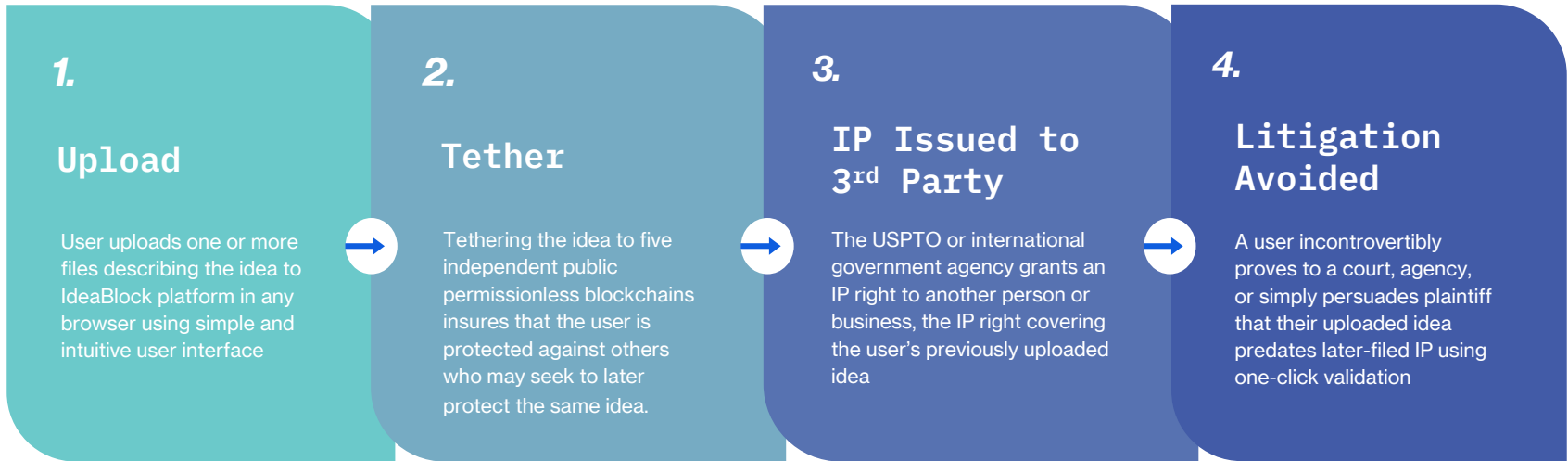
In addition to bare transaction data, many public blockchains allow users to store relatively small amounts of additional data of their choosing inside transactions.



IdeaBlock uses this additional data allotment to anchor idea-specific data to these blockchains, timestamping the idea and proving its existence.

# How Does IdeaBlock Work?

A USE-CASE-AGNOSTIC GENERAL VIEW OF SYSTEM FUNCTIONALITY



# How IdeaBlock Defends Against Third-Party Patents

**IdeaBlock uses blockchain to create unassailable prior art that can invalidate any patent subsequently granted to others on a user-uploaded idea.**

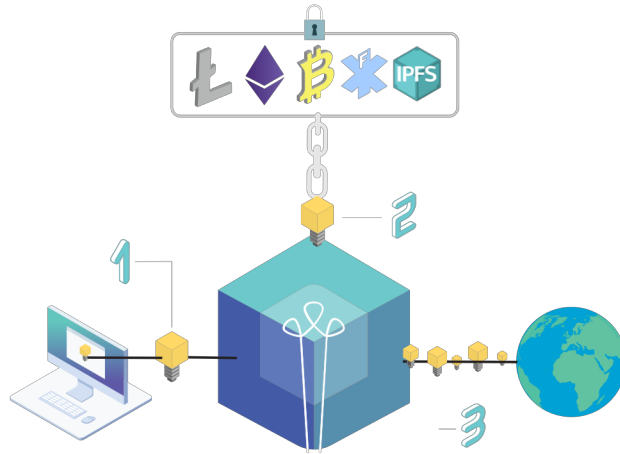
Before blockchain, it was virtually impossible for a defendant to establish the authenticity of internal company materials such as physically date-stamped paper records, emails, and computer server contents – materials which could have otherwise served as anticipatory references to invalidate (i.e., cancel) the patent being asserted against them. To this day, judges simply consider the risk of forgery too high with these items.

**With blockchain, the chances of the five IdeaBlock-connected blockchains failing a test of truth are about the same as the same person winning 23 consecutive nightly drawings of both the Mega Millions and the Powerball lotteries.**

To the best of our knowledge, IdeaBlock is the first company in history to leverage blockchain immutability to prove that both (a) an idea existed at the time of upload and (b) that the idea was made public – which are the two requirements for establishing prior art to invalidate a patent with clear and convincing evidence.

*RELATED FIGURE* 

# IdeaBlock for Patent Defense



## STEP ONE USER UPLOADS IDEA FILES

An IdeaBlock user selects files and enters additional text and metadata to fully describe their idea then uploads the files and description to IdeaBlock via our intuitive user dashboard.

## STEP TWO ANCHOR HASH TO BLOCKCHAINS

IdeaBlock creates and tethers the idea-specific hash to five independent blockchains and creates a validation certificate that can be used to undeniably prove the contents of the Idea and a timestamp indicating the moment it was uploaded.

## STEP THREE SERVE ANCHORED IDEA TO PUBLIC

IdeaBlock uses a proprietary method for proving constant public idea availability, which ensures that any Idea becomes unassailable prior art against later-filed IP from the instant it is uploaded, providing immediate insurance against potential lawsuits and market exclusion in the future.

# How IdeaBlock Protects Holders of Trade Secrets

**Companies that choose to hold certain IP as a trade secret can utilize IdeaBlock to prove prior commercial use of that trade secret to limit potential exposure in a patent suit.**

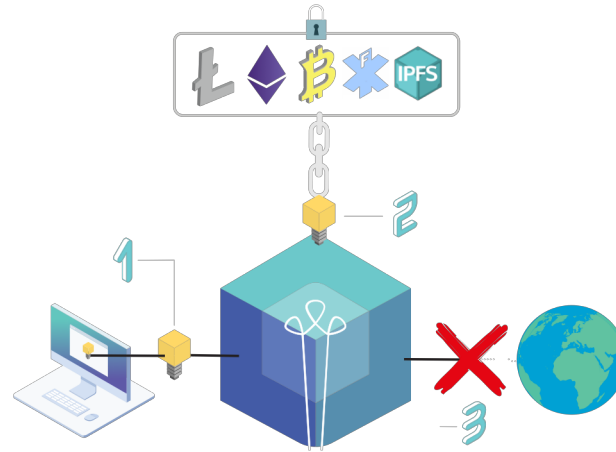
Though the A.I.A. provided an expanded scope for trade secret holders to qualify for a prior use exception when sued for patent infringement, it places quite a burden on these trade secret holders who are sued for patent infringement by a third party who independently invented and patented your trade secret. Namely, these defendants must establish with *clear and convincing evidence* that they used the trade secret in commerce an entire year before the enforced patent was filed.

To help meet this high standard, IdeaBlock offers trade secret protection that utilizes blockchain technology to unassailably prove via one or more unique file hashes tethered to five different robust digital ledgers that you did indeed possess and use the idea in commerce before the required date to qualify for the prior use exception.

The figure on the next slide shows a bit more about what the IdeaBlock trade secret protection service looks like at a high level.

# IdeaBlock for Trade Secret Defense

IDEABLOCK FUNCTIONALITY FOR PROTECTING PRIOR USE RIGHTS OF TRADE SECRET HOLDERS



## STEP ONE USER UPLOADS TRADE SECRET FILES

An IdeaBlock user seeking to establish prior use rights for IP that is being kept as a trade secret first selects files and enters additional text and metadata to fully describe their trade secret. To complete the upload process, the user is sure to confirm three (or more) times that this is to be kept as a trade secret object, and uploads the files and description to IdeaBlock via our intuitive user dashboard.

## STEP TWO ANCHOR HASH TO BLOCKCHAINS

IdeaBlock creates and tethers the relevant file hash to five independent blockchains and creates a validation certificate that can be used to undeniably prove that the user was in possession of (and/or commercial use of) and a timestamp indicating the moment it was uploaded.

## STEP THREE BLOCK ACCESS TO TRADE SECRET FILES

Because it is being kept as a trade secret, naturally we do not expose the uploaded idea files to the public, once the trade secret files have been hashed and placed in the blockchains, the source files are either (a) completely deleted from all filesystems and returned to the user via secure encrypted email, or (b) only kept in an encrypted vault storage system that is separate and isolated from any normal day-to-day IPFS and web traffic



## Isn't IdeaBlock Obsolete in our First-to-File System?

**No.**

The first-to-file paradigm introduced in the U.S. in 2012-2013 by the America Invents Act (A.I.A.) is relevant only for purposes of obtaining a U.S. patent. Though IdeaBlock can, and in our opinion should, be used in tandem with a patent filing to significantly strengthen overall protection for the subject IP, IdeaBlock's service offerings are not directly relevant to any analysis under the A.I.A. first-to-file provisions.

Can't I do the same thing IdeaBlock does by sending an email with my idea attached or a letter to myself with the idea in the sealed envelope?

**No.**

In a first-to-invent system, proof of the date on which an inventor conceived of an idea was very relevant in cases where two or more individuals may have conceived of the idea independently around the same time. After passage of the A.I.A. and implementation of a first-to-file system, a proof of conception date gets an inventor effectively nowhere, as the filing date of a patent application or verifiable public disclosure of the idea become much more relevant. IdeaBlock could be said to provide a similar service to the pre-A.I.A. “mailing” strategy in the post-A.I.A. system. Specifically, rather than simply prove conception and possession of an idea, IdeaBlock creates trusted, verifiable proof of public disclosure of the idea, which prevents anyone else from obtaining a valid and enforceable patent on the user's uploaded idea.

# How can we be sure that a judge will uphold the validity of a blockchain-backed validation protocol for IP?

**Unfortunately, we can't without a DeLorean or crystal ball. However . . .**

Consider this: though estimates vary relatively widely, the probability of making a DNA evidence “cold hit” on an innocent person is anywhere from one in tens of millions to one in a billion. In other words  $1:10,000,000 - 1:1,000,000,000 = 1.0e^{-7}$  to  $1.0e^{-9}$

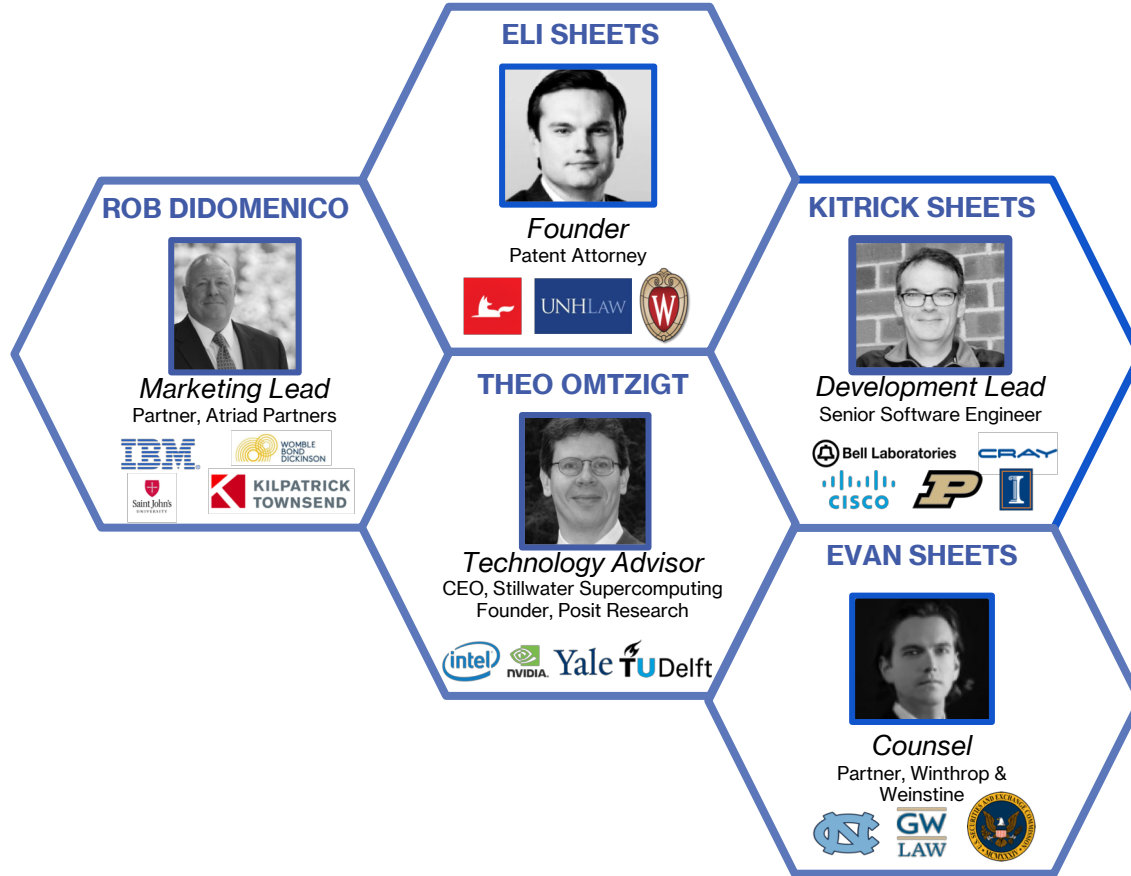
The chances of random collision (hash values from two different inputs resulting in the same hash output) using the SHA-256 hash algorithm that IdeaBlock and its implemented blockchains utilize has been estimated at anywhere from  $1:2^{75}$  to  $1:2^{91}$  which translates to  $2.64e^{-23} - 4.03e^{-28}$

Therefore, the chances of a random person hitting a false DNA positive is anywhere from 16 to 19 orders of magnitude more likely than ever seeing the same SHA-256 hash appearing in any place, ever.

I realize that the math above does not amount to a precedential federal judicial opinion – but with math and number magnitude like that, I will say it would be quite brave to bet against us.



# TEAM




# CONTACT



IdeaBlock

ELI SHEETS

@sheets173 

shooter#1349 

eli.sheets 

eli@ideablock.io

612-710-0208

ideablock.io

PATENT PENDING