

An Introduction to Blockchain & NFTs

Jimmy Nguyen
Founding President, Bitcoin Association for BSV

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto satoshin@gmx.com www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.



Digital Timestamping: Stuart Haber & W. Scott Stornetta

J. Cryptology (1991) 3: 99-111

Journal of Cryptology

© 1991 International Association for Cryptologic Research

How To Time-Stamp a Digital Document1

Stuart Haber and W. Scott Stornetta
Belloore, 445 South Street,
Morristown, NJ 07960-1910, U.S.A.
stuart@belloore.com
stornetta@belloore.com

Abstract. The prospect of a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media raises the issue of how to certify when a document was created or last changed. The problem is to time-stamp the data, not the medium. We propose computationally practical precedures for digital time-stamping of such documents so that it is infeasible for a uner either to back-date or to forward-date his document, even with the collusion of a time-stamping service. Our procedures maintain complete privacy of the documents themselves, and require no record-keeping by the time-stamping service.

Key words. Time-stamp, Hash.

Time's glory is to calm contending kings, To unmask falsehood, and being truth to light, To stamp the seal of time in aged things. To wake the morn, and sentiael the night, To wrong the wronger till he render right.

The Rape of Lucrece, I. 941

1. Introduction

In many situations there is a need to certify the date a document was created or last modified. For example, in intellectual property matters, it is sometimes crucial to verify the date an inventor first put in writing a patentable idea, in order to establish its precedence over competing claims.

One accepted procedure for time-stamping a scientific idea involves daily notations of one's work in a lab notebook. The dated entries are entered one after another in the notebook, with no pages left blank. The sequentially numbered, sewn-in pages of the notebook make it difficult to tamper with the record without leaving telltale signs. If the notebook is then stamped on a regular basis by a notary public or reviewed and signed by a company manager, the validity of the claim is further enhanced. If the precedence of the inventor's ideas is later challenged, both

¹ Date received: August 19, 1990. Date revised: October 26, 1990.

Improving the Efficiency and Reliability of Digital Time-Stamping

Dave Bayer*

Barnard College

Columbia University

New York, N.Y. 10027 U.S.A.

dab@math.columbia.edu

Stuart Haber
Bellcore
445 South Street
Morristown, N.J. 07960 U.S.A.
stuart@bellcore.com

W. Scott Stornetta
Bellcore
445 South Street
Morristown, N.J. 07960 U.S.A.
stornetta@bellcore.com

March 1992

Abstract

To establish that a document was created after a given moment in time, it is necessary to report events that could not have been predicted before they happened. To establish that a document was created before a given moment in time, it is necessary to cause an event based on the document, which can be observed by others. Cryptographic hash functions can be used both to report events succinctly, and to cause events based on documents without revealing their contents. Haber and Stornetta have proposed two schemes for digital time-etamping which rely on these principles [HaSt 91].

We reexamine one of those protocols, addressing the resource constraint required for storage and verification of time-stamp certificates. By using trees, we show how to achieve an exponential increase in the publicity obtained for each time-stamping event, while reducing the storage and the computation required in order to validate a given certificate.

We show how time-stamping can be used in certain circumstances to extend the useful lifetime of different kinds of cryptographic certifications of authenticity, in the event that the certifying protocol is compromised. This can be applied to digital signatures, or to time-stamping itself, making the digital time-stamping process renewable. Secure Names for Bit-Strings

Stuart Haber* stuart@surety.com W. Scott Stornetta* scotts@surety.com

Abstrac

The increasing use of digital documents, and the need to refer to them conveniently and manningsoundy, take an important question: can one "name" a digital document in a way that conveniently enables users to find it, and at the same time enables a user in possession of a document to be some that it is adouted the one that is refused to by the name? One crucial piece of a complete solution to this problem would be a method that provides a cryptographically surifiable label for any bit-string (for example, the content, in a particular format, of the document). This problem has become even more assis with the ensempace of the Wuld-Wild Wild, where a document (whose only existence may be en-line) is now tryically named by giving its URL, which is merely a pointer to its virtual location at a particular moment in time.

Using a une-way hash function to call files by their hash values is expringraphically verifiable, but the esselling names are unwidely, because of their length and randomners, and are not permanent, mice as time goer on the hash function may become witnessle to attack. We introduce procedures not create names that are short and menningful, while at the same time they can persist indefinitely, independent of the long-with of any given hash function. This is done by naming a bit-string according to its position in a growing, directed acyclic graph of one-way hash values. We prove the security of our naming procedures under a reconstable completing theoretic cryptographic assumption, and then describe practical uses for these names. An implementation of our naming scheme has been in use since January 1903.

1 Introduction

Uses of documents need to refer to those documents in order to keep records and in order to communicate with other users of the documents. In practice, users name their documents in various ways. A same must be unambiguous, at least in the context of its use; this requires some connection between the name and the intention of the document it

Permission to ensite digitalitant capies of all or part of this material for personal or clusters are in granted without the provided that the copies were not reade or distributed for partition or commercial analysis, the capparright notice, the tile of the publication and its data appear, and unlike in given that capping it is by particulation of the ACM, for, to copy otherwise, he required to the providence of the ACM or copy otherwise, he required to the first or continuous control or the ACM or copy otherwise.

CCS 97, Zarick, Switzerland Converted 1997 ACM Deptity (412-2000)4 ... 53.50 names.

In the traditional world of paper documents, there are evasly reasonable parameters of this connection. In the conof printed books and magazines, large print runs that are the result of single typesetting efforts make it easier to be confident that all copies of a printed document are the same, with a definite name printed in a conventional place in the document. Making a change to a paper document of any sort, even a small change, typically leaves foressic evidence.

A characteristic feature of digital documents, by contract, is that they are easy to copy and to alter. The naming problem is especially travelsling if the document crists only on-line and never in conventional paper-based form. For unline documents, a useful naming scheme weall allow users to employ the name to find documents, as well as to check the integrity of the documents that they find. A number of proposals have been made for such naming systems (see e.g., [SM 34, KW 35, BD* 35]]. These proposals address in different ways the problem of how to "nesolve" the name into a location where the documents might be found.

It is the integrity-checking problem that we address in this work: how to make sure that the bit-string content of a given digital document is indeed the same as the hitstring that was intended. Heretoliere, two different sorts of mechanisms have been proposed, digital signatures and oneway hash values.

Having the author or publisher of a document compute a digital signature for its bit-string content is a reasonable me of cryptographic tools for this purpose. (See, for example, [8, 95, M 94].) However, the shifty to sublette swary digital signatures requires the presence of a public-bay infrareduce, and the treatworthiness of the validation procedure rules on the assurance that the signat's privace signing key is indeed secure. For some on-line documents, the infrastructure and these assurances may not be available. For large-lived documents, the eneugity of the binding between a public key and the person or role of the putative signer becomes even more problematic. (A general solution to the latter problem is briefly described in [3,5].

Thus it mould be sauful to have an integrity mechanism, depending on the exact contents of the bit-string in question, that does not depend on the secrecy of a cryptographic leg. A navaral choice for such a mechanism is the use of a energy hath function, naming any bit-string by its bash value, (See, for example, [RID* 95].) However, while this method is intimisefully scriffable, there are several inconvenient functions:

· A desirable feature for the names given to a collection

^{*}Partially supported by NSF grant DMS-90-06116.

^{*}Sweety Technologies, I Main Street, Chatham, N.J. 87938, U.S.A.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto satoshin@gmx.com www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing

the proof-of-work. The longest chair events witnessed, but proof that it callong as a majority of CPU power is ca attack the network, they'll generate the network itself requires minimal struct basis, and nodes can leave and rejoi proof-of-work chain as proof of what h

References

- [1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.
- [2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.
- [3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.
- [4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.
- [5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

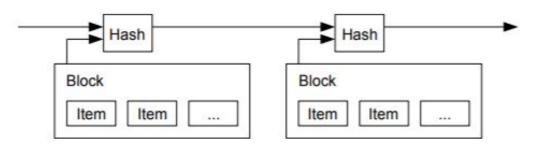


Distributed Timestamp Server

.

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



Auditable Verifiable Transparent

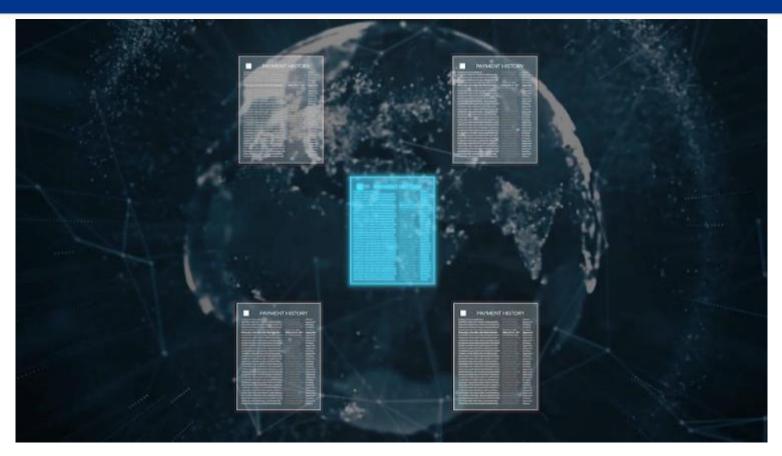


Timechain (Satoshi notes from pre-release Bitcoin source code)

```
// The timechain is a tree shaped structure starting with the
// genesis block at the root, with each block potentially having multiple
                                                                                       // A transaction with a bunch of additional info that only the owner cares
                                                                                       // about. It includes any unrecorded transactions needed to link it back
// candidates to be the next block. pprev and pnext link a path through the
// main/longest chain. A blockindex may have multiple pprev pointing back
// to it, but pnext will only point forward to the longest branch, or will
                                                                                       class CWalletTx : public CMerkleTx
// be null if the block is not part of the longest chain.
class CBlockIndex
                                                                                // Nodes collect new transactions into a block, hash them into a hash tree,
                                                                               // and scan through nonce values to make the block's hash satisfy proof-of-work
                                                                               // requirements. When they solve the proof-of-work, they broadcast the block
                                                                                // to everyone and the block is added to the timechain. The first transaction
                                                                                // in the block is a special one that creates a new coin owned by the creator
                                                                                // of the block.
// A transaction with a merkle branch linking it to the timechai
                                                                                // Blocks are appended to blk0001.dat files on disk. Their location on disk
class CMerkleTx : public CTransaction
                                                                                // is indexed by CBlockIndex objects in memory.
```



What is a Blockchain?



A digital ledger to record transactions (payments and data)

Distributed and maintained across network of computers globally (rather than kept by just 1 company)



Blockchain is a Distributed Timestamp Server

Summary

22f08eae0126009

(#651750)

Timestamp 2020-89-09 01:07:20 ①

(utc)

Transactions 14,200

14,200 Transactions

F1 = 972882640897761a11 04f (9d70061849725a989a1985060 527 045 (1fd8070) e M

¥2 - 8aca2d211774fede9f3f049c9909c53b1d964e1ebe49ce92e1c1b24c1b3a9393 ▼

43 - 15dab8ca568†7dc0939b93c44d279748badb†b49†b4696\$†a25addac98d3552d 🔀

44 dd.a.455 (a.: 187335259) 3019) 3d0u5.4565149...95 N.c.46-404425c10109d6 No. 😕

😢 - dsea4ecvisJauge/91caba/bafdfasda/cffcsdaedbfas/e2f9dbafc3dcc2ib4

№ - ee83e599d7730129dc9711817a27598fc388c252a3f9f28r2ffca85c5600e5c8 🗸

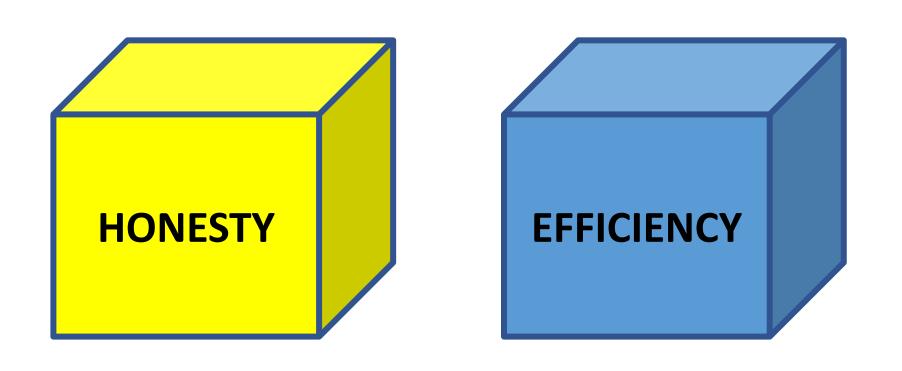
47 L006:4010206b05754c16db0ar0559007b67 .5132d37384.acf803H04016671±1d ♥

•II = Inscriba in //dis4r also //dis4/2015 also rized to to the description of the inscribed to the insc

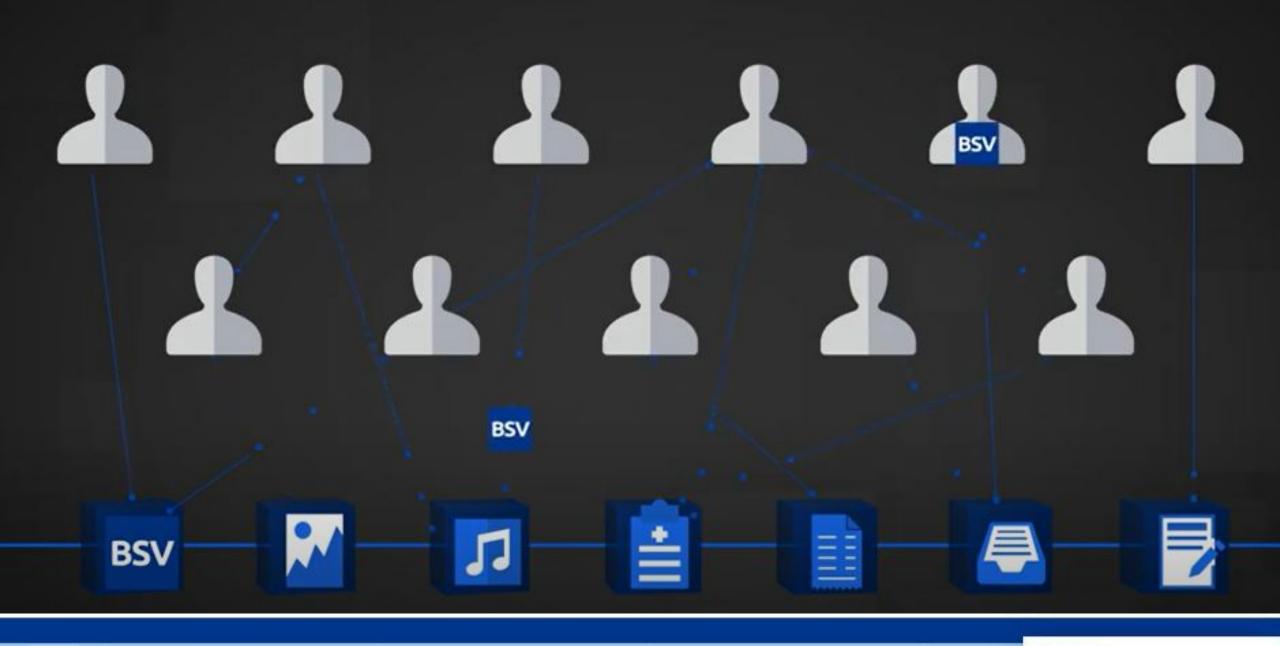
Transactions are date & time-stamped

Transaction history is publicly verifiable















2,000 txns/ second; peak 56K txns/second







2,000 txns/ second; peak 56K txns/second

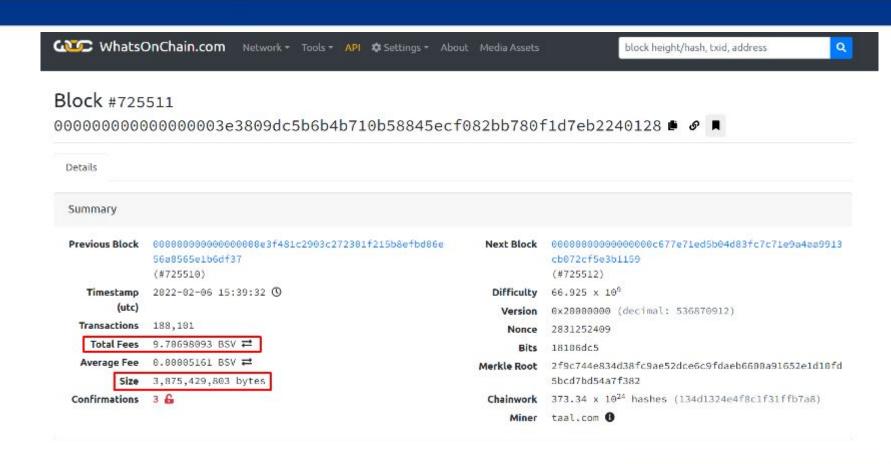
BSV

UNBOUNDED SCALING 50,000-100,000 txns/second + MORE



World Record Blocks

- 2021 mined series of2GB blocks
- 6 February 2022
 3.8 GB block at block height 725511 (new world record)





BTC transaction fees are high and unreliable

Time	10 Oct 2020	7 Dec 2020	27 Mar 2021	21 April 2021	29 June 2021	8 Sept 2021	29 Nov 2021
Next block (10 minutes)	\$3.12	\$7.16	\$9.11	\$33.94	\$6.25	\$.80	\$.71
3 blocks (30 minutes)	\$3.12	\$7.16	\$5.11	\$30.06	\$5.89	\$.80	\$.14
6 blocks (60 minutes)	\$2.89	\$6.19	\$3.04	\$26.83	\$5.71	\$.80	\$.14

Source: https://bitcoinfees.info/



Ethereum gas fees are high and unreliable

	11 Jan	23 Feb	12 May	29 June	8 Sept	29 Nov	16 Jan
	2021	2021	2021	2021	2021	2021	2022
Average Txn Fee	\$16.52	\$38.21	\$69.92	\$3.80	\$61.00	\$45.49	\$34.83
Median Txn Fee	\$7.37	\$19.16	\$37.89	\$1.79	\$19.87	\$21.92	\$17.12

Source: https://bitinfocharts.com/

BSV transaction fees are low and reliable

1/100-1/20 cent

for payments



Micropayments – "small casual transactions" over the Internet

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.



A New World of Micropayments

- Pay per article or blog post
- Pay by minute of video content watched
- Pay to get past key points in video content
- Pay to push email to top of someone's inbox
- Pay for Internet search
- Pay for in-game and virtual items
- Pay for social media interactions
- Pay for providing your device computing power



Non-Fungible Tokens

- Tokens (digital representation of something)
- Have value because they are unique (not fungible, not interchangeable)
- Recorded on a blockchain
 - Unique identifiers and metadata
 - Publicly verifiable, accessible and more efficient to transact
 - Reduce fraud



NFT Examples

- Digital ownership record for a real-world physical item art, clothing, collectible, car, real estate
- Digital works
 - Digital image, publishing, music, or video files
 - In-game items
 - Avatars and characters
 - Software
- Intangible rights
 - IP assets
 - Individual identities & publicity rights





JA MORANT

Dunk - Dec 11 2019, Holo MMXX (Series 1), MEM

Legendary #/25 (LE)

Lowest Ask

USD \$250000.00

Only 2 listings



VINCE CARTER

3 Pointer - Mar 11 2020, Cosmic (Series 1), ATL

Legendary #/49 (LE)

Lowest Ask

USD \$200000.00

Only 4 listings



STEPH CURRY

Assist - Mar 5 2020, Holo MMXX (Series 1), GSW

Legendary #/50 (LE)

Lowest Ask

USD \$250000.00

Only 2 listings

LEBRON JAMES

Legendary #/59 (LE)

USD \$199999.00

(Series 1), LAL

Lowest Ask

Dunk - Feb 6 2020, From the Top



DERRICK ROSE

Layup - Feb 28 2020, From the Top (Series 1), DET

Legendary #/59 (LE)

Lowest Ask

USD \$240000.00

Only 2 listing



ZION WILLIAMSON

Block - Jan 24 2020, Cosmic (Series 1), NOP

Legendary #/49 (LE)

Lowest Ask

USD \$219000.00

Only 2 listing



ZION WILLIAMSON

Block - Jan 24 2020, Holo MMXX (Series 1), NOP

Legendary #/50 (LE)

Lowest Ask

USD \$169000.00

Only 3 listings

GIANNIS ANTETOKOUNMPO

Dunk - Nov 16 2019, Holo MMXX (Series 1), MIL

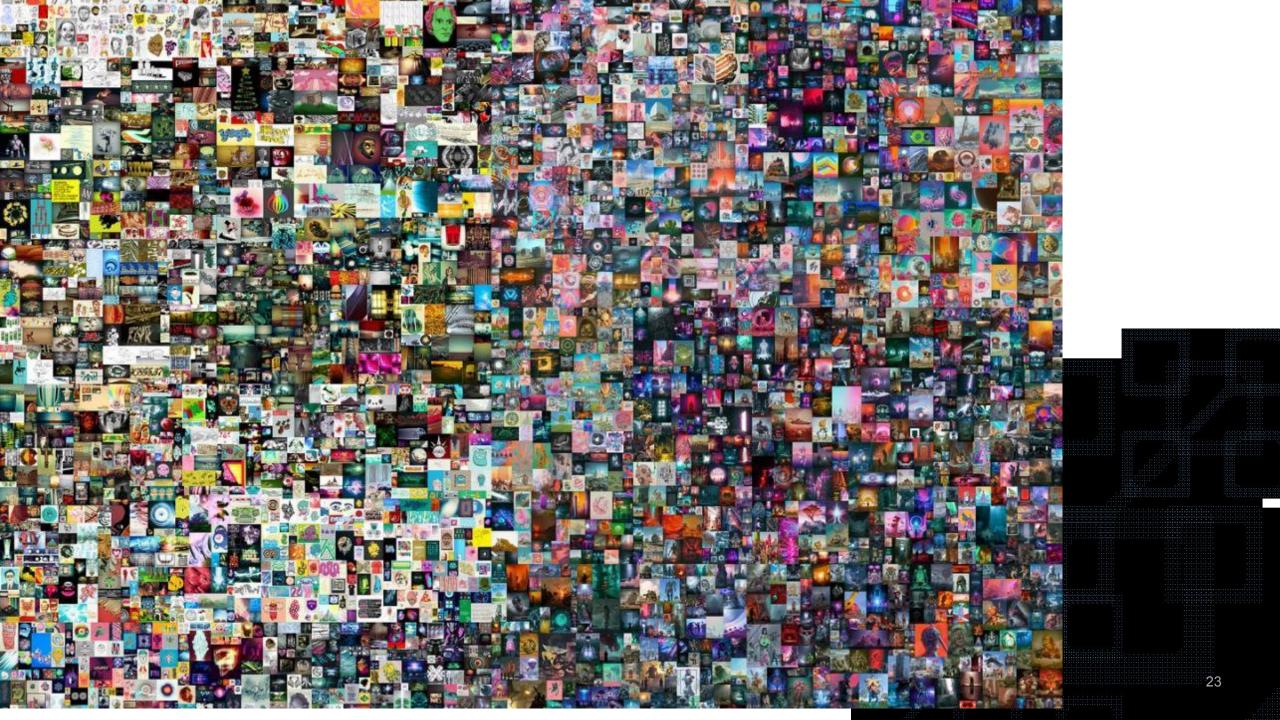
Legendary #/50 (LE)

Lowest Ask

USD \$169000.00

Challe 2 Bullion

22







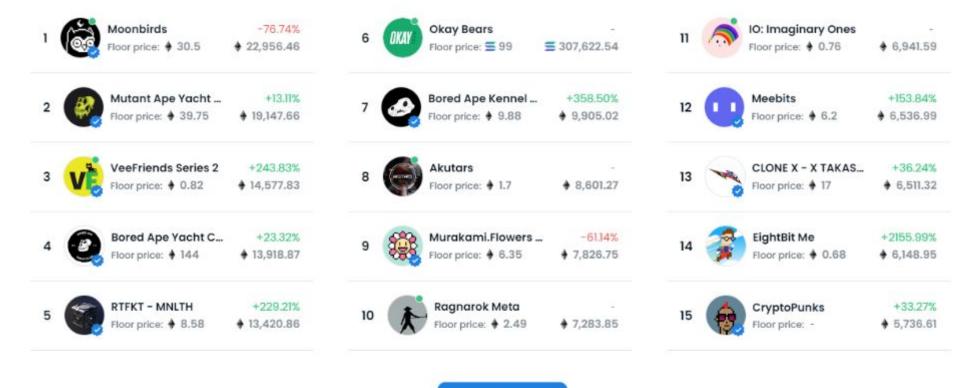
Generative Art NFTs: Manufactured Uniqueness?





Q Search items, collections, and accounts

Top collections over last 7 days v



Go to Rankings

Top collections in 1 day - All Ethereum Flow Polygon

Ragnarok

\$10,286,373



See all



Moonbirds \$7,073,048



ENS domains \$2,876,166





Akutars \$1,432,589



MutantApeYachtClub \$7,923,947



Bored Ape Yacht Club \$6,663,859



CloneX

\$2,799,865



adidas Originals: Int... \$2,070,794



Azuki \$1,368,115



VeeFriends Series 2 \$7,596,170

Imaginary Ones \$5,584,093

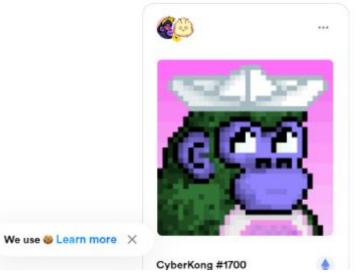


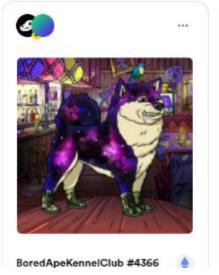
Murakami.Flowers S... \$2,611,944

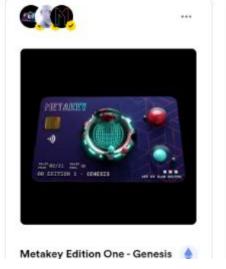
Bored Ape Chemistr... \$1,536,024

RTFKT - MNLTH \$1,195,124

Hot bids 🤚











28



wackies

Created by wackies-deployer

579 418 + 0.095 **† 11.5** items owners: floor price volume traded

MINTING NOW: https://wackies.io/ for 0.08

Wackies is an animated generative version of her portrait art with a supply of 2,500 unique pieces. Each peice symbolizes Camille's journey and expression of identity through art.



~ Activity

















vockies
Nackies #572







activa	Price
rackies #550	♦ 0.11
	Icmi + 0.119
	Ø 3



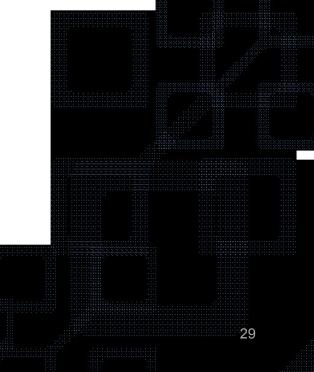






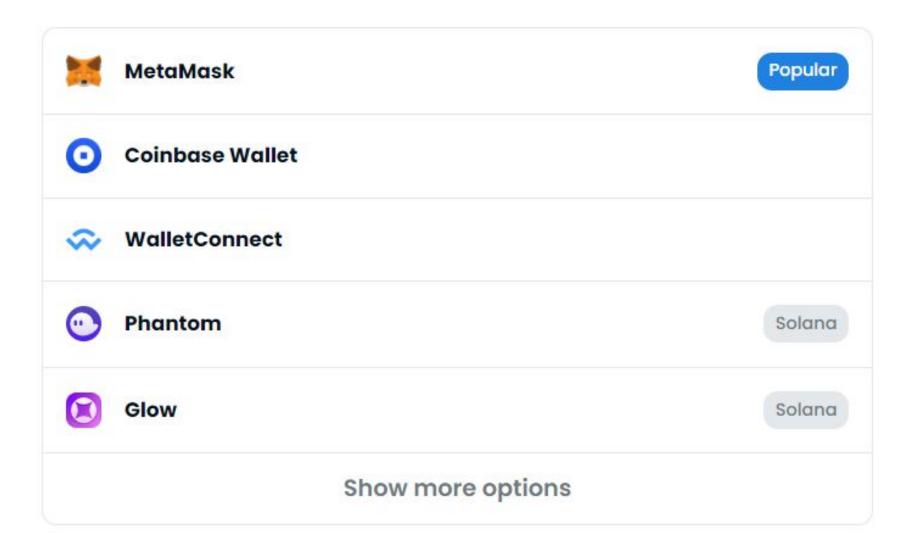


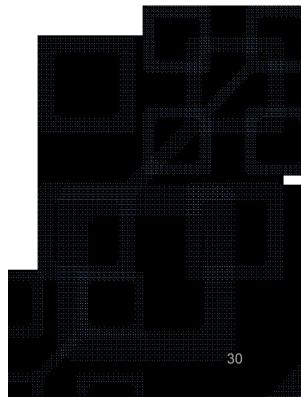




You need an Ethereum wallet to use OpenSea.

Connect with one of our available wallet providers or create a new one.

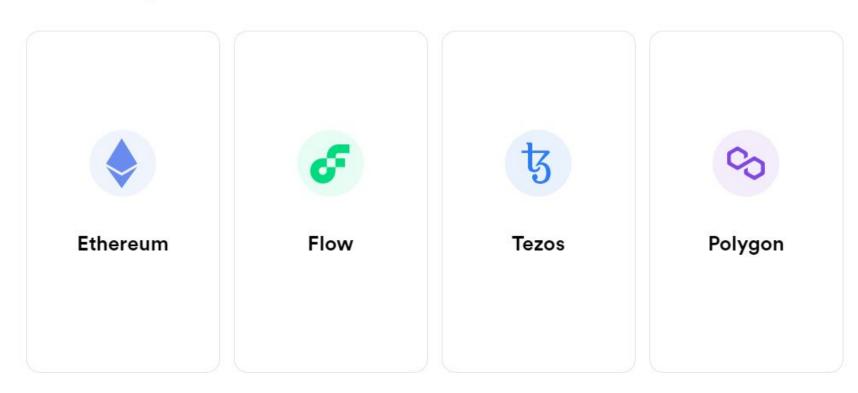




Choose Blockchain

Choose the most suitable blockchain for your needs.

You need to sign in for creation. Learn more about Blockchains



NFTs on BSV: Assets Can be Stored On-Chain







BullishArt NFT on BSV



NFTs on BSV: Very Low Fees



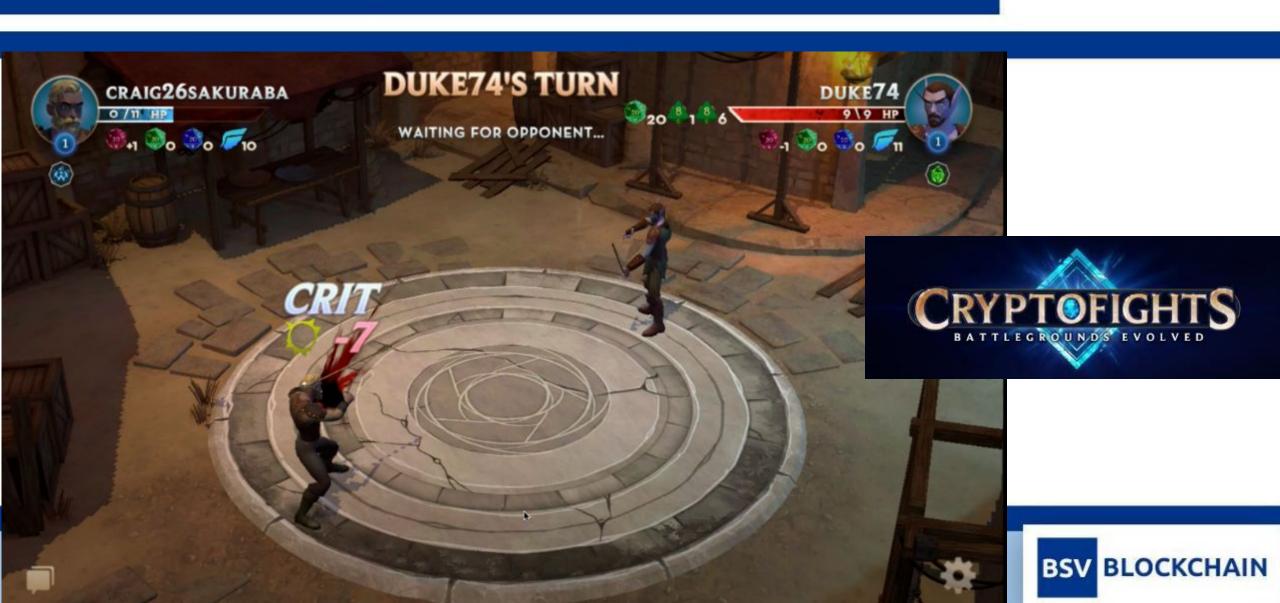
2021

minted over 175,000 NFTs

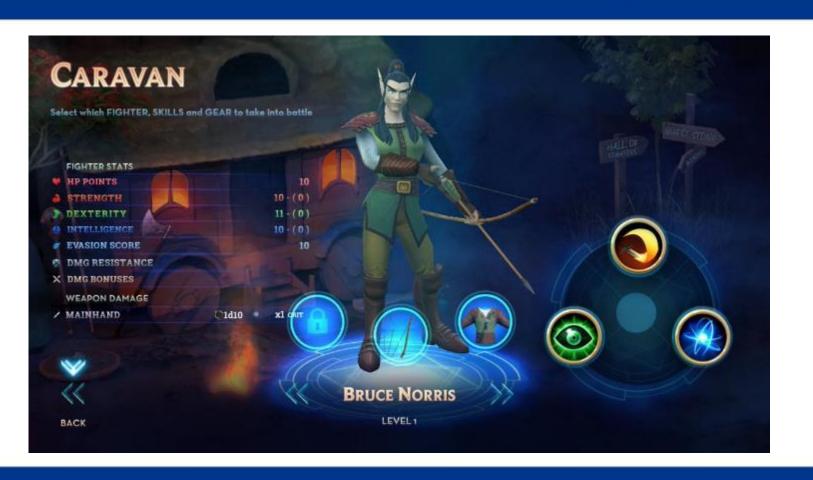
Total cost - **\$175**



CryptoFights



CrypoFights: Avatars and Virtual Items as NFTs







NFT Example: Duro Dogs







NFT items can continually accrue new characteristics







NFT characters and items can be used across different platforms

DESIGNED FOR INTEROPERABILTY

Duro Dogs' unique design allows them to easily be extended and pulled into other applications. There is no limit to where your dog can go in the metaverse.





Inaugural Duro Dog Show



Theme: Spring Enter Thru April 12



Prizes 1st: \$100* 2nd: \$50 3rd: \$25

-Top 3 will also receive rare NFTs

-Finalists earn 1000 treats





How to Enter

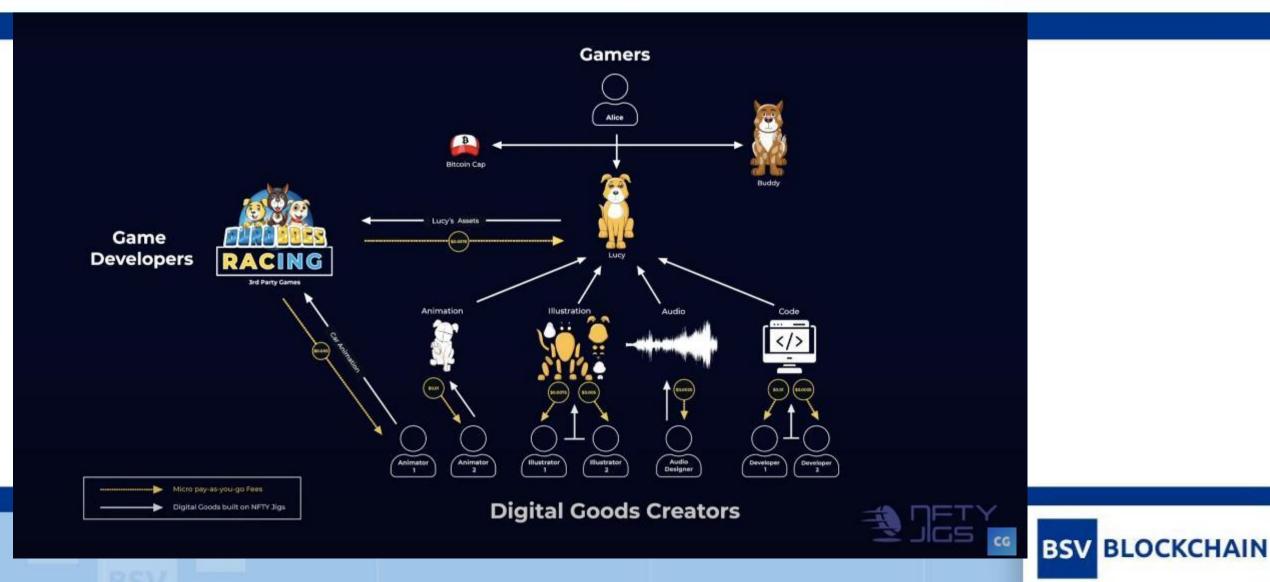
-Tweet a photo showing off your dog(s), item(s), and creativity -Use the hashtag #durodogshow -Include your HandCash \$handle

Learn more at medium.com/nfty-jigs





With micropayments, connect 3 sets of actors: gamers, game developers, digital goods creators



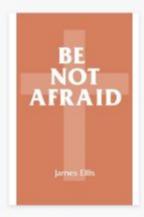
NFTs on BSV: Books



Books NFT market How to buy

Books

Buy self-published books on Bitopin



Be Not Afraid

James Ellis



Missing Axioms: Philosop...

Samuel Barnes



THE WHITES - Season 1, E...

Freddy Moya & Peachy Keenan

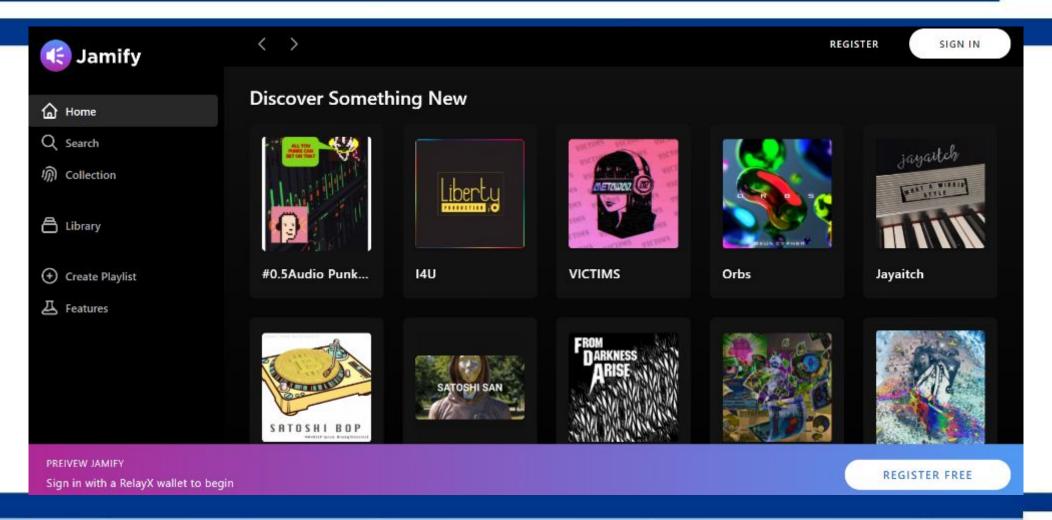


No Domain: The John McA ...

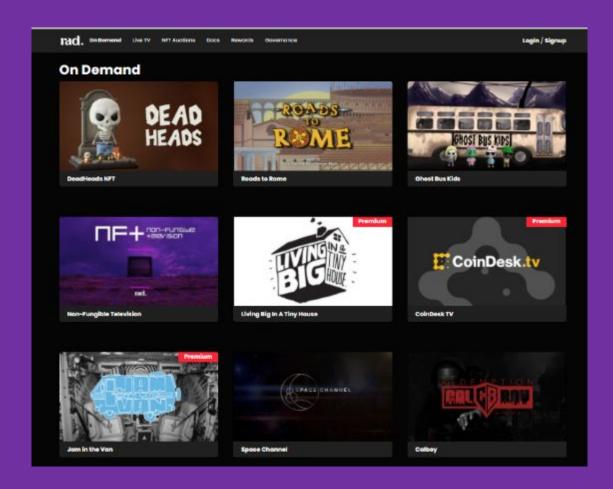
Mark Eglinton

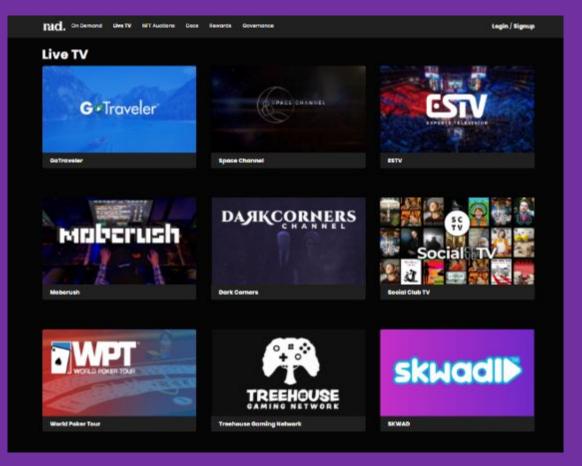


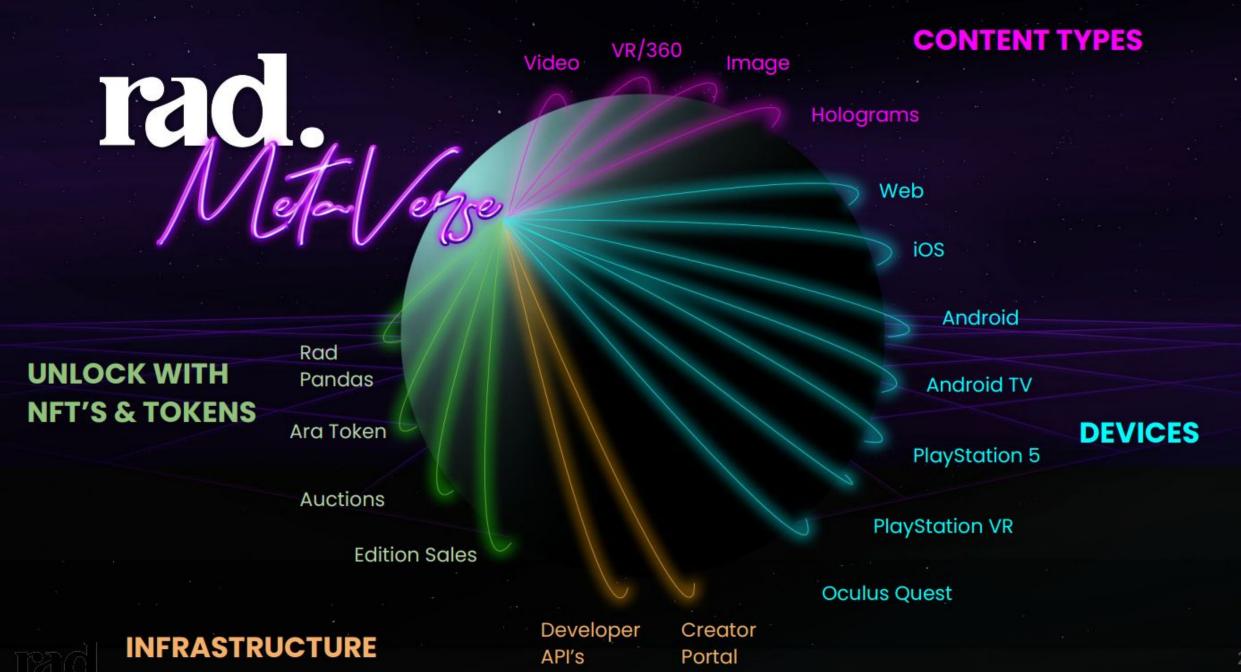
NFTs on BSV: Music Files

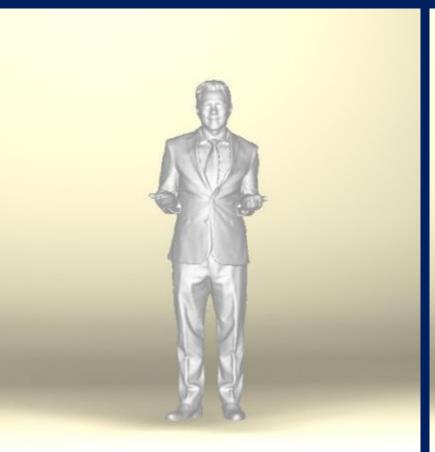


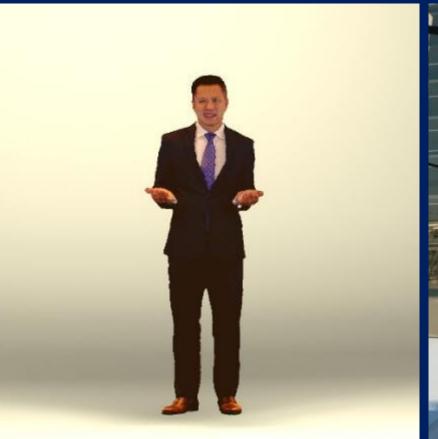














General Publications

December 20, 2021

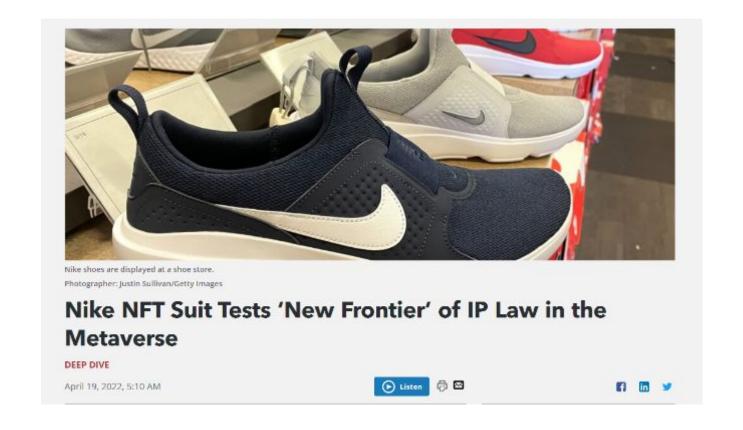
"Pulp Fiction' NFT Lawsuit Presents New IP Battleground," *Law360*, December 20, 2021.

Hermès suing American artist over NFTs inspired by its Birkin bags

French luxury brand says Mason Rothschild's furry MetaBirkins digital tokens 'rip off' its trademark







- Nike: StockX's minting & selling of NFTs is infring
- StockX: because its NFTs are inextricably linked to and intended to certify ownership of actual physical Nike sneakers, the NFTs are non-fringing fair use and a lawful exercise of the first sale doctrine

Does a digital ticket useful only for redeeming a pair of Nikes itself become a separate product if it prompts people to pay hundreds more than the shoes cost?

OpenSea • User Safety

Q Search

Articles in this section

How can I submit a copyright counternotice?

What is OpenSea's stolen item policy?

How can I revoke token approvals and permissions on Ethereum?

What is an inactive listing?

How can I migrate my Klatyn items?

Are spin-off, homage or remix collections allowed on OpenSea?

This guide looks at how OpenSea may moderate spin-off collections and homages to established NFT works such as CryptoPunks. We also introduce the concept of "Fair Use" for users to consider before creating NFTs.

What is Fair Use?

Generally speaking, fair use means using a copyrighted work (like a book, film, or character) in a **transformative way** for uses such as **commentary, criticism, education, or parody**.

Articles in this section

How can I submit a copyright counternotice?

What is OpenSea's stolen item policy?

How can I revoke token approvals and permissions on Ethereum?

What is an inactive listing?

How can I migrate my Klatyn items?

What can I do if my copyrighted works are being sold without my

What can I do if my copyrighted works are being sold without my permission?

Content that infringes on the intellectual property rights of other individuals, including copyright, may be removed for violating our Terms of Service.

Pursuant to the Digital Millennium Copyright Act (DMCA), OpenSea maintains a notice and takedown process for alleged copyright infringement. In accordance with this U.S. federal law, OpenSea allows users to report content if they believe that it violates their copyright. To request that a collection or item be taken down because you believe that it violates your copyright, please complete this form.

How does OpenSea process copyright takedown requests?

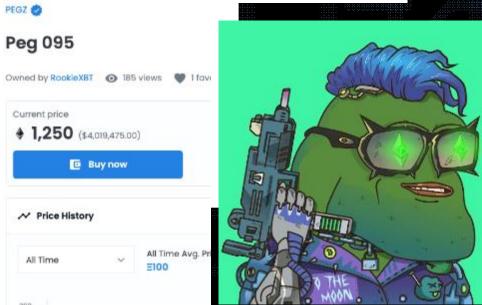
Upon receiving a copyright takedown request, we evaluate the submission for completeness and authenticity. If we determine that a takedown request fulfills the

Opensea Delists SFD: NFT Centralization and Copyright Law









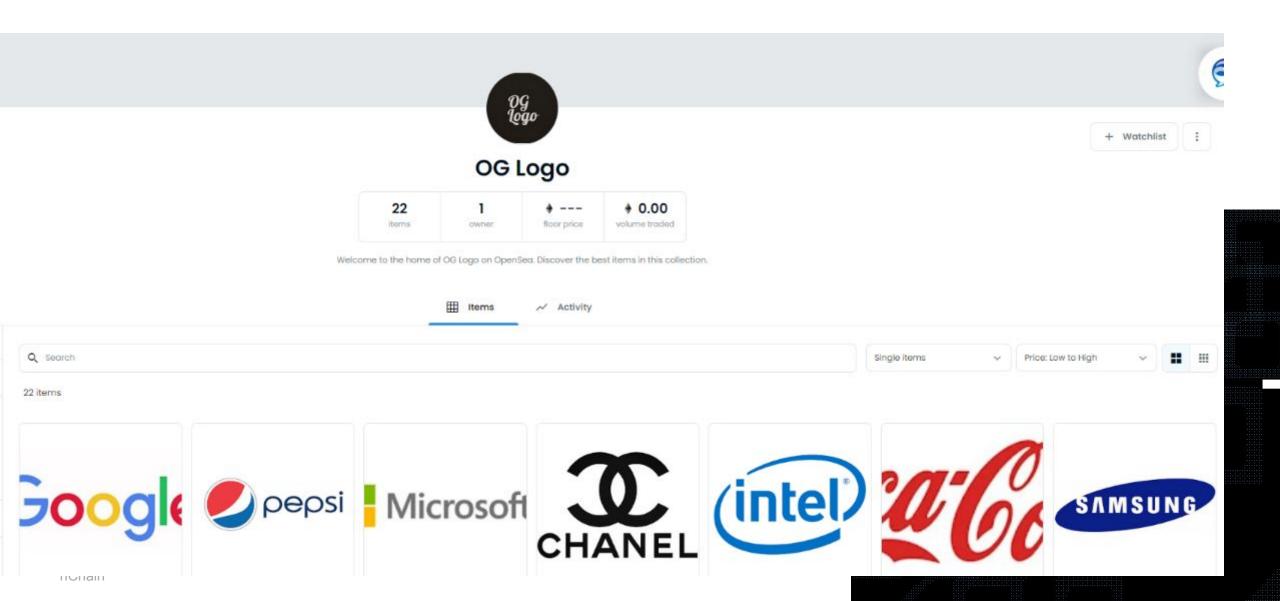


These ARE the Punks you're looking for! LegoPunks will be a limited edition of 300 different Punks. Each one is unique and will be a 1/1 series.

Created by CryptoPopz

266

items





NFT UR LOGO

17 + 0.003 + 0.00 salume traded Itamia Roor price

A logo is meaningless if its not NFT. Our project lis to ensure the validation of your product by adding your minted lags on it. Some of the popular kigas are minted in our collection. Feel free to contact us to mint your own logs (0.005 eth)

> Items ~ Activity



17 items











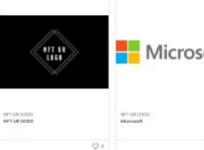


₩.0





Single items



→ Price: Low to High

Explore State Resources Create

+ Watchlist -df









