Cyberscope

Audit Report

BRC-20 NAME SERVICE

August 2023

Network   BTC

Type   BRC-20

Tick   BTNS

Audited by   © cyberscope

Table of Contents

Review

Network	BTC
Token Type	BRC-20
Tick	BTNS
Status	Mint Completed
Completion Percentage	100.00%
Explorer	https://unisat.io/brc20/BTNS
Inscription	00295addc9d156eff3b625303cfa98e023754f48376c489ca27af4596833affai0
Total Supply	2,100,000,000
Minted	2,100,000,000
Limit per Mint	2,100,000,000
Decimals	18
Deployed By	bc1qvu623mrawtyp2wezf3a0u52pj3ytvrn8rmlhln
Deploy Time	5/10/2023, 5:16:34 AM
Completed Time	5/10/2023, 5:38:17 AM
Inscription Number Start	#5163805
Inscription Number End	#5170587
Total Holders (At the time of the report)	6
Total Transactions (At the time of the report)	48

Audit Updates

Initial Audit	1 Aug 2023

Source Files

Filename	JSON
inscription/BTNS	https://static.unisat.io/inscription/content/00295addc9d156eff3b62530 3cfa98e023754f48376c489ca27af4596833affai0

Overview

The BRC-20 Name Service (BTNS) is an innovative domain system designed to decentralize and expand the Web3 landscape, built upon the foundation of the Bitcoin BRC-20 Chain. The project's primary aim is to simplify the complexities associated with wallet address naming in Web3 interactions, offering users a unique and identifiable name substitution.

Domain System Feature

- Users are granted the autonomy to configure and manage subdomains as they see fit.
- Domains, represented with the suffix .BRC, can map to BRC-20 addresses, Dapp content, and other pertinent data.
- Domains, minted with individual assets and wallets, ensure unique ownership, preserving their distinct value through the blockchain's immutable nature.

BTNS Token Role and Governance

- The BTNS token serves as the lifeblood of the BRC-20 Name Service.
- The Governance Token, provides its holders with a voice in the project's trajectory, allowing them to partake in various decision-making roles.
- The team emphasizes the critical importance of the $BTNS token to the project's success and sustainability.

Airdrop Plans

1. 1st Early Airdrop: Exclusively available to those with a Mint Pass who have minted domains early in the project's inception. The vested period for these $BTNS tokens is 12 months.
2. 2nd Public Airdrop: Post the commencement of the Public Domain Mint, domain owners can claim airdrop amounts based on various criteria. These tokens also have a vesting duration of 12 months.
3. 3rd Community Airdrop: Targets those in possession of Quest NFTs or the Discord Role "NSM" issued by the BTNS Foundation. The vesting period is 12 months.

Expected Token Distribution

Category	Percentage	Total Tokens	Vesting Details
Team Supply (Core Team)	13.5%	283,500,000	10% Unlock, based on first vesting in June 2023, monthly vesting for 4 years (48 months)
Foundation	12.5%	262,500,000	Based on the first vesting in June 2023, monthly vesting for 4 years (48 months)
Ecosystem	13.5%	283,500,000	30% Unlock, 70% Others monthly vesting for 40 months
Contributors	9%	189,000,000	5% Unlock, Other 2 months Lockup Vesting monthly for the next 3 years
Community AirDrop	14%	294,000,000	Vesting over 12 months
Liquidity Supply	7%	147,000,000	Utilize exchange liquidity supply
Marketing	8%	168,000,000	5% Unlock, 3 months Lockup then 12-Months monthly vesting
Treasury	12.5%	262,500,000	-
Token Sale	5%	105,000,000	5% Unlock, 1 Month lockup then 12-Months monthly vesting
Investor	5%	105,000,000	5% Unlock, 1 Month lockup then 12-Months monthly vesting

Pie Chart of Expected Token Distribution

Total Supply 2,100,000,000

Investor
5.0%

Token Sale
5.0%

Treasury
12.5%

Marketing
8.0%

Liquidity Supply
7.0%

Community AirDrop
14.0%

Team Supply
13.5%

Foundation
12.5%

Ecosystem
13.5%

Contributors
9.0%
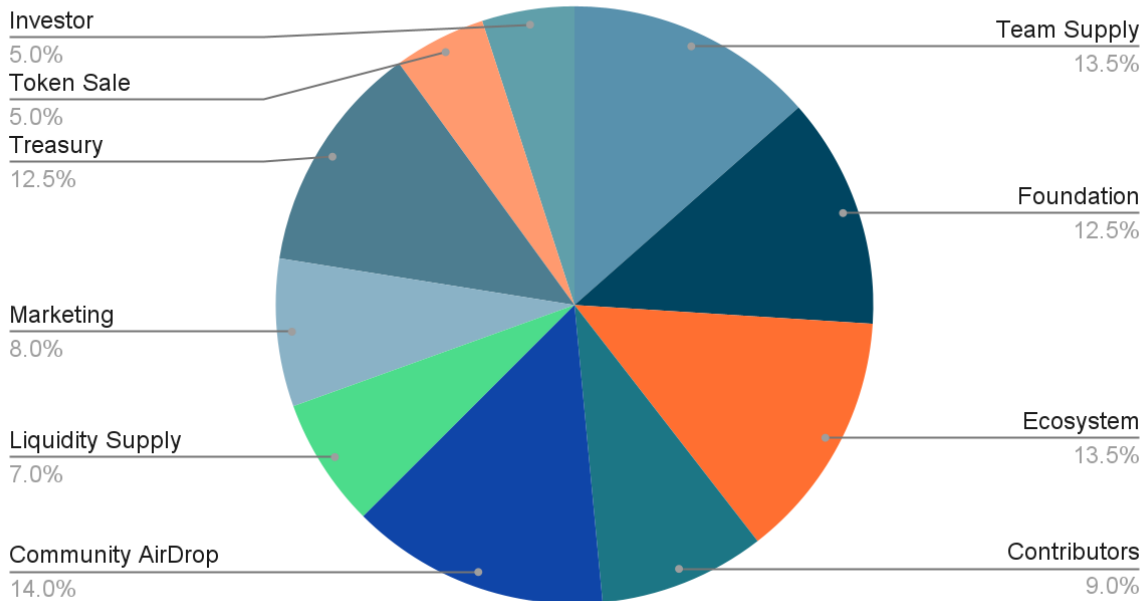
Inscription Information

InscriptionNumber	#5163805
InscriptionId	00295addc9d156eff3b625303cfa98e023754f48376c489ca27af4596833affai0
Address	bc1qvu623mrawtyp2wezf3a0u52pj3ytvrn8rmlhln
Output value	52207
Sat	899066321604222
Content	{"p":"brc-20","op":"deploy","tick":"BTNS","max":"2100000000", "lim":"2100000000"}
Content length	80
Content type	text/plain;charset=utf-8
Timestamp	2023-05-10 02:16:34 UTC
Genesis height	789008
Genesis transaction	00295addc9d156eff3b625303cfa98e023754f48376c489ca27af4596833affa
Content/SHA-256	de2aa27e7c0e57264286963d03f70f572ae139bd8f213f3c3d0dee47da6502d9

JSON Deploy Content

The deploy JSON file contains the initial deployment specifications of the BRC-20 token. The token is identified by the ticker name "BTNS". The maximum supply for the BTNS token has been set at 2,100,000,000. Additionally, the maximum mint amount per inscription, is also set to match the max supply, standing at 2,100,000,000.

```
{
    "p":"brc-20",
    "op":"deploy",
    "tick":"BTNS",
    "max":"2100000000",
    "lim":"2100000000"
}
```

Key	Value	Required	Description
p	brc-20	Yes	Protocol: Helps other systems identify and process brc-20 events
op	deploy	Yes	Operation: Deploy
tick	BTNS	Yes	Ticker: 4 letters identifier of the brc-20
max	2100000000	Yes	Max supply: set max supply of the BTNS token
lim	2100000000	No	Mint limit: If letting users mint to themsleves, limit per BTNS mint

JSON Mint Content

This mint JSON file provides details on the minting procedures for the BRC-20 token. The token, identified by the ticker name "BTNS", had its entire supply of 2,100,000,000 minted in a singular transaction as specified by this JSON mint file. The mint was set to the amount of 2,100,000,000, which is equal to the max supply of the BTNS token, and was executed in one transaction.

```
{
  "p":"brc-20",
  "op":"mint",
  "tick":"BTNS",
  "amt":"2100000000"
}
```

| Key	Value	Required	Description
p	brc-20	Yes	Protocol: Identify & process brc-20 events
op	mint	Yes	Operation: Mint
tick	BTNS	Yes	Ticker: 4 letter identifier of the brc-20
amt	2100000000	Yes	Amount to mint: States the amount of the BTNS to mint. Has to be less than "lim" stated in deploy file

Token Holders

At the time of this report, the distribution of BTNS token holders is as follows:

Rank	Address	Percentage	Value
1	bc1px...6pf0w	99.86%	2,096,987,864
2	bc1pz...wne3f	0.08%	1,610,116
3	bc1qz...sjflk	0.07%	1,400,000
4	bc1p2...cremc	0.00%	1,000
5	bc1p2...rp5kp	0.00%	1,000
6	bc1qw...0nuxg	0.00%	20

This distribution represents the token holdings at the specific time of our audit. Changes in distribution may occur due to subsequent transactions.

Findings Breakdown
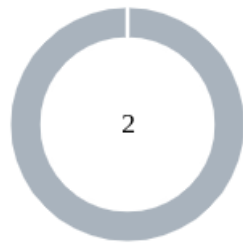
	Critical	0
	Medium	0
	Minor / Informative	2

Severity	Unresolved	Acknowledged	Resolved	Other
● Critical	0	0	0	0
● Medium	0	0	0	0
● Minor / Informative	2	0	0	0

Diagnostics

● Critical   ● Medium   ● Minor / Informative

Severity	Code	Description	Status
●	CR	Centralization Risk	Unresolved
●	PFU	Potential Functionality Usage	Unresolved

CR - Centralization Risk

Criticality	Minor / Informative
Status	Unresolved

Description

The token was initially deployed by the address `bc1qvu623mrawtyp2wezf3a0u52pj3ytvrn8rmlhln`. This address initially minted the entire token supply of the `BTNS` BRC-20 token. After the minting, the deployer address transferred the entire token supply to the address `bc1q30fqd978h0fcfw73tcfpk8tu99kaae26trzqdd`.

Following a series of transfers, a significant portion of the tokens ended up in the address `bc1px9qdte7ltd6g9xq86mzwuaaprzwdedgq08j9dlfqr64jlz2lt5tqw6pf0w`. As a result, this new address now holds a significant portion of the total supply. Specifically, this address holds 99.86% of the total tokens, amounting to 2,096,987,864 BTNS tokens. Such a large concentration of tokens in a single address poses centralization risks, leading to potential market manipulation and other adverse effects on the ecosystem.

Number	Method	Quantity	Balance	From (Address)	To (Address)	Date	Time
#5176675	send	-2,1B	0.00	bc1qv...mlhln	bc1q3...rzqdd	5/10/2023	7:30 AM
#5176675	inscribe-transfer	2,1B	2,1B	-	bc1qv...mlhln	5/10/2023	6:05 AM
#5170587	inscribe-mint	+2,1B	2,1B	-	bc1qv...mlhln	5/10/2023	5:38 AM
#5163805	inscribe-deploy	0.00	0	-	bc1qv...mlhln	5/10/2023	5:16 AM

Recommendation

It is recommended to distribute the tokens more broadly to achieve a more decentralized token holding structure. This can mitigate the risks associated with centralization and ensure a more stable and secure ecosystem for all participants. If the new address consists of a team's wallet address, then the team should carefully manage the private keys of that account. We strongly recommend implementing a robust security mechanism to prevent a single user from accessing the contract admin functions, such as a multi-sign wallet so that many addresses will confirm the action.

PFU - Potential Functionality Usage

Criticality	Minor / Informative
Status	Unresolved

Description

The token is designed to serve as the foundation for the BRC-20 Name Service, aiming to provide users with a decentralized unique domain system. Within this system, domain owners can configure and manage subdomains as they see fit. As detailed in the project's documentation, `BTNS` will act as the Governance Token of the BRC-20 Name Service, granting token holders participation in decision-making roles.

To further enhance the utility of the `BTNS` token, the JSON mint and transfer files could be expanded to encompass multiple and varied governance voting power and domain information. Specifically, the governance power functionality could be implemented by the addition of an extra field. Similarly, the domain could be included in the JSON file, allowing for the permanent storage of the domain name on the blockchain. By doing so, each token holder would be endowed with additional functionalities and advantages, such as specific governance voting power and unique domain names. This enriched information would be leveraged by the project to offer each token holder added utility based on their specific governance power and domain ownership.

Users will benefit from these utilities, enabling them to `mint` specific tokens with distinct governance vote power and domain names. Additionally, they will have the ability to `transfer` the token along with its proportional utility, either the voting power or the domain name, or both of them. This enriched functionality would be leveraged by the project to offer each token holder added utility based on their specific `BTNS` information.

Recommendation

The team is advised to take into consideration the inclusion of additional functionality to the `BTNS` BRC-20 tokens during the `mint` and `transfer` phases. By integrating more detailed Governance voting power within the JSON files, the project can better cater to the diverse needs of its community, ensuring that each token holder can access the benefits and utilities associated with their specific voting power. Furthermore, by storing the domain name permanently in the blockchain, users are granted a consistent and immutable reference to their domains, ensuring long-term reliability and security. This enhancement not only adds value to the token but also strengthens the project's commitment to a decentralized and user-centric ecosystem, ensuring that domain information remains transparent, permanent, and tamper-proof.

JSON mint file example:

```
{
  "p":"brc-20",
  "op":"mint",
  "tick":"BTNS",
  "amt":"2100000000",
  "votePower": "1000",
  "domain": "myDomain"
}
```

Deploy Transaction Flow

Transaction

Transaction	00295addc9d156eff3b625303cfa98e023754f48376c489ca27af4596833affa
Block	789008
Timestamp	2023-05-10 05:16
Features	SegWit, Taproot, RBF
Fee	47,793 sat ($13.24)
Fee rate	268 sat/vB

Input

bc1p63y499asduhz2pelq996lnjq8vr7htqdk…ns7a9w8m	0.00100000 BTC

Outputs

bc1qvu623mrawtyp2wezf3a0u52pj3ytvr…n8rmlhln	0.00044546 BTC
bc1qd9q7hm9p3htdw8ntwndqewpjww7dtn…3yysgx3u	0.00007661 BTC

Details

Size	375 B
Virtual size	178.5 vB
Weight	714 WU
Version	2
Locktime	0
Transaction hex	020000000001014fd3d190f0137563854ed25737d6f6dabf14043d0abad3243aa41981837e53ce0400000000fdffffff0202ae0000000000000160014 6734a8ec7d72c8153b224c7afe51419448b60e67ed1d00000000000016 00146941ebeca18dd6d71e6b74da0cb83273bcd5ce240340fb3b81a3d 6b51cd7816af5be1b528ae2be29a2b39e9372de753f2dac58ec30c3e9a d8f9d00b051f17a1fdedf16f65590f6002feaf338aa390edf44bf4a6432e79 f20117f692257b2331233b5705ce9c682be8719ff1b2b64cbca290bd6fa eb54423eac0649a15c038801750063036f72640101187465787742f706c 61696e3b636861727365743d7574662d38004c507b2270223a22627262 32d3230222c226f70223a226465706c6f79222c227469636b223a224425 44e53222c226d6178223a22323231303030303030303030222c226c696d6d22 3a2232313030303030303030303030227d6821c1117f692257b2331233b5705c e9c682be8719ff1b2b64cbca290bd6faeb54423e00000000

Summary

The BRC-20 Name Service, is a groundbreaking domain system built on the Bitcoin BRC-20 Chain. It offers users a platform where they can own, configure, and manage unique domain names, seamlessly connecting their information and assets across various Dapps. The BTNS token, a BRC-20 token, plays a pivotal role in the governance and functionality of this service. The BRC-20 Name Service is a holistic ecosystem that intertwines domain ownership with governance, aiming to revolutionize the way users interact with Web3, all while ensuring a decentralized and user-centric approach. The audit report investigates the present state of the BTNS token. It analyzes the deploy and mint transactions, examines the current distribution of the token, and presents findings along with suggestions for potential functionality updates.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io