BRACE NETWORK WHITEPAPER V1

FUNCTION:

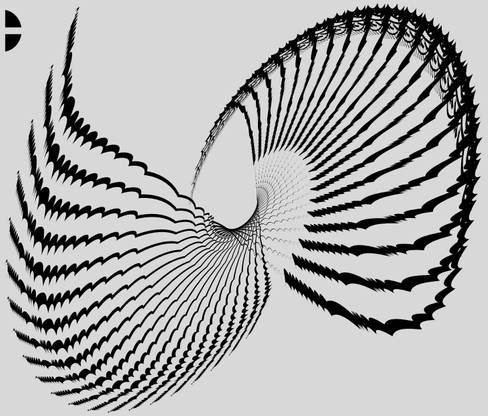
0012 7482901 2744103 0592346 8774510 7255

BRACE NETWORK

bracenetwork.io

0002849916 . 742941 . 1265330 . #18940 DO NOT DELAY

00004512 // 99374128 // 1005934



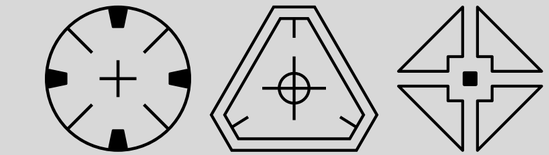
0 77832 12

BRACE
NETWORK

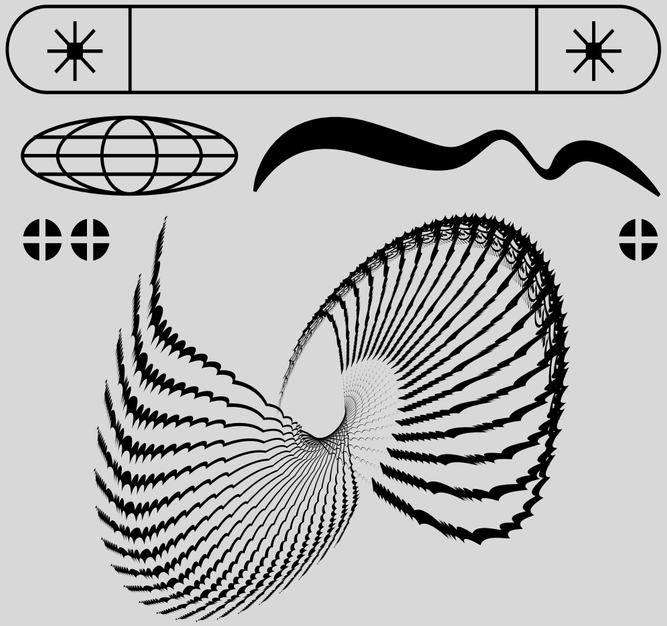
****

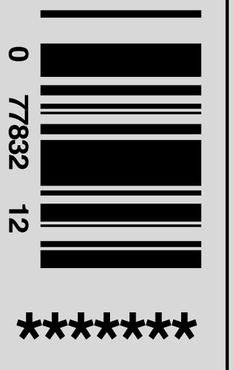
INTRODUCTION

In recent years, society has been changing at an unprecedented pace. Technological advancements in digitization and new technologies such as cloud computing, quantum computing, artificial intelligence, blockchain, Web3, virtual reality, and the metaverse are shaping a new world rich with new opportunities and business models that are disrupting the traditional centralized economy and financial services industry. These new technologies have the potential to replace the centralized financial institutions that act as intermediaries for all our economic transactions. Not only that, they offer a system that is fair, democratized, and that applies the same, or even a greater, level of integrity currently provided by mainstream financial corporations



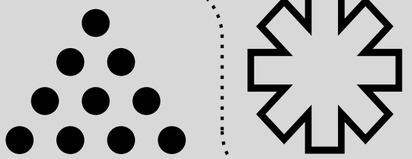
00004512 // 99374128 // 1005934





0 77832 12

****

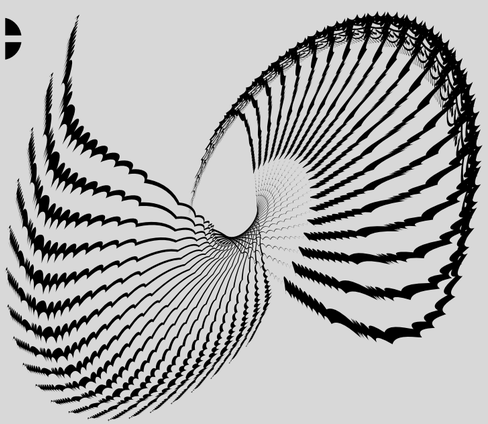


BRACE
NETWORK

INTRODUCTION

The banking sector, however, has resisted change. Their transactional processes are too slow, excessively costly, bound to too many unnecessary human intermediaries, and apply overly-complex bureaucratic mechanisms and outdated legacy operating systems. Furthermore, macroeconomic uncertainty is adding to inflationary pressure on the markets. Consequently, the interest rates offered by the established centralized institutions are too low to maintain the value of assets, resulting in the real value of assets decreasing due to high inflation. This leaves a vast pool of millions of users and affiliate partners looking for a better and more modern way to generate passive, rewarding digital assets and, at the same time, support the development of the future of Web3 infrastructure. These digital community members seek Decentralized Finance (DeFi) solutions that they can trust and easily understand. Furthermore, they want to receive an APR reward much higher and more consistent than offered by leaving their funds in traditional centralized banking solutions. Moreover, these users are looking for complete control of their digital assets and the possibility of participating in a digital economic system with secure but practical KYC requirements solution and less risk of data leakage

00004512 // 99374128 // 1005934



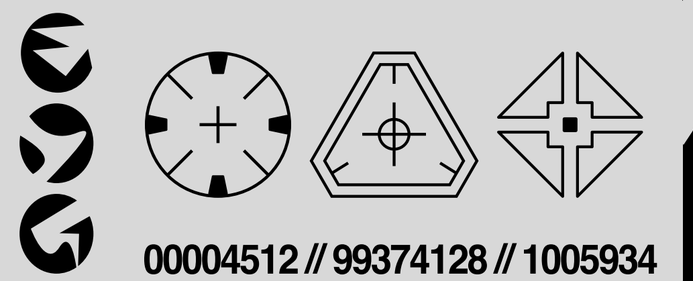
0 77832 12

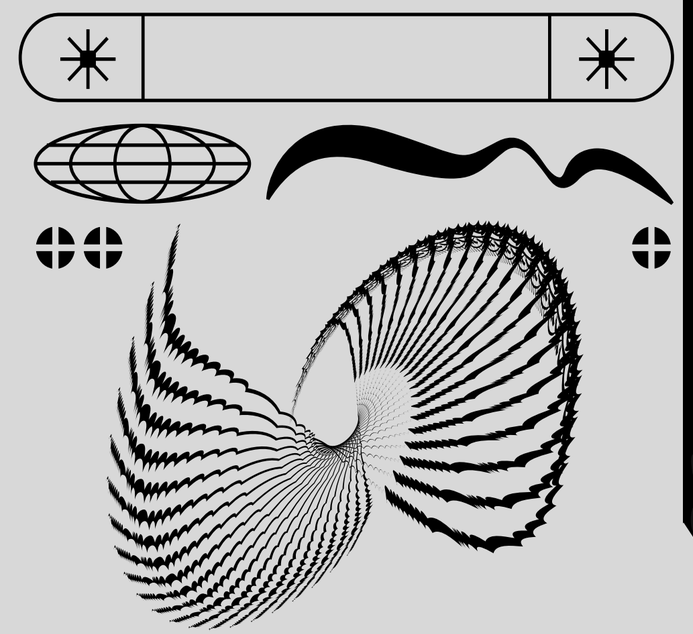
BRACE
NETWORK

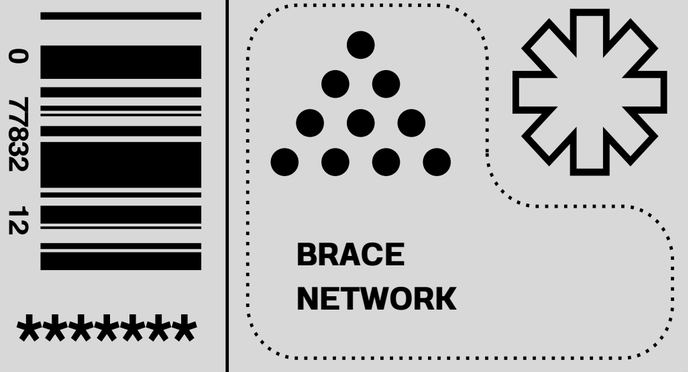
****

INTRODUCTION

To solve this issue, blockchain technology and DeFi offer superior asset preservation systems, thanks to the help of new technologies, automated market makers, and algorithmic asset management instruments that can provide economic sustainability. One of the barriers to entry, however, is that these innovative mechanisms have a very steep learning curve that prevents access to these services for most IT illiterate consumers. On one side, they offer very appealing characteristics like ledger immutability and permissionless transparency, but, on the other hand, they lack user-friendliness. Furthermore, these solutions struggle to receive trust, legitimacy, or regulatory confidence. Many also struggle to provide enough liquidity to deal with the volatility of the digital assets markets to survive and scale. While DeFi decentralized applications, or dApps, aim to replace the traditional banking intermediaries, too many projects focus on creating competing solutions with competing tokens, instead of emphasizing complete ecosystem growth by using the same native coin for the whole palette of digital asset management services. Consequently, the user journey becomes unnecessarily complex: different tokens are not always compatible and fail to synchronize effectively with each other, and understanding differences in product offerings, or service costs is challenging. Furthermore, it is difficult to economically incentivize the continuous development support of decentralized IT professionals in a sustainable manner

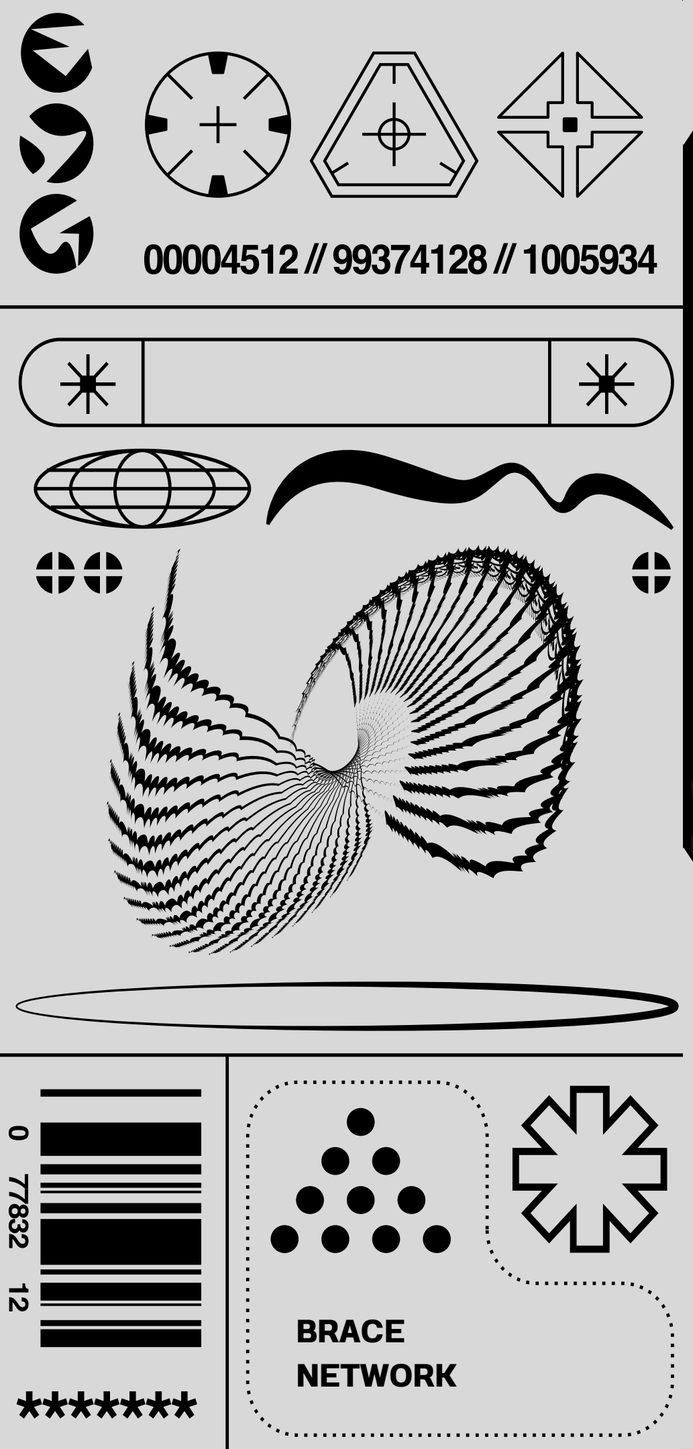






INTRODUCTION

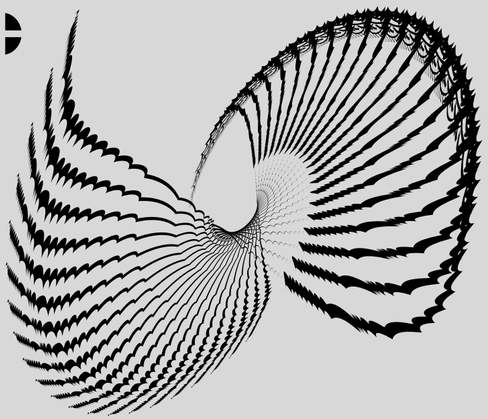
Brace fills this gap and solves these technical and economic problems by successively collating DeFi services within a supportive ecosystem that utilizes a single token. Brace's solution will be cost-effective, easy to understand, and capable of delivering the expectations of a wide and ever-growing pool of digital assets holders while mitigating risks. No matter their economic background and technological understanding, everyone will be able to participate in the future of the digital asset market. Brace’s innovation stems from leveraging the technology of the most scalable, secure, cost-efficient, and developer-friendly blockchains and crypto projects with the implementation of a unique crowdfunding solution – a Staking Hub NFT. Brace’s consensus protocol enables the Brace L1 blockchain to deliver high throughput with fast transaction speeds, low transaction costs, and deterministic finality (which means that transactions can never be reverted, with no need to wait for extra block confirmations like in networks with probabilistic finality, e.g., Bitcoin). All this is achieved while being permissionless and decentralized. The staking structures on Brace are highly dynamic and lucrative. In addition to the novel Staking Hub NFTs, Brace users can stake the native coin as validators (or delegators) and receive an APY of 5–13% APY.



INTRODUCTION

By using a single native Layer 1 (L1) BRACE coin, the Brace community will be able to access a wide variety of decentralized digital asset management services and, at the same time, benefit from the ever-growing dApp services resources offered by an invigorated ecosystem

00004512 // 99374128 // 1005934



0 77832 12

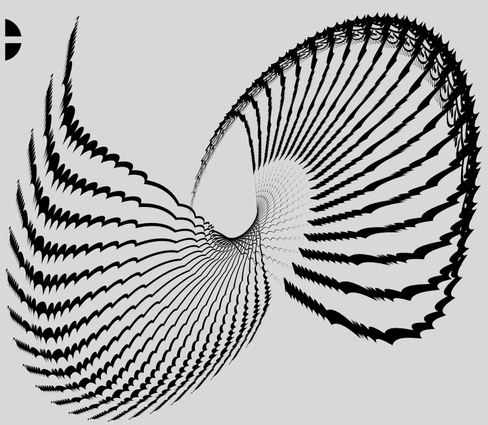
****

BRACE
NETWORK

BLOCKCHAIN CHALLENGES

Blockchain promises to mitigate against any future need for a centralized authority. It enforces digital "trust" between users that may have no pre-existing relationship or point of contact. In fact, it works by negating the need for trust by enforcing honesty in the system.However, the utility of blockchain has been restrained by real-world challenges such as transaction speed. Consider that, when a customer purchases with a Visa card, Visa is the only entity that needs to create a permanent record of this to enable the initial transaction. In contrast, blockchain provides a “distributed ledger”, i.e., a permanent record that is widely shared. The upside to distributed ledger technology (DLT) is that it provides “inclusive accountability”. So, while Visa’s transactions are managed by the central authority that is Visa, a blockchain enables anyone with the tech and an internet connection to ensure the system’s integrity. The downside is that this decentralization takes time. Early generation blockchains such as Bitcoin can process around 5 transactions per second, while Visa can achieve more than 1,500 transactions per second

00004512 // 99374128 // 1005934



0 77832 12

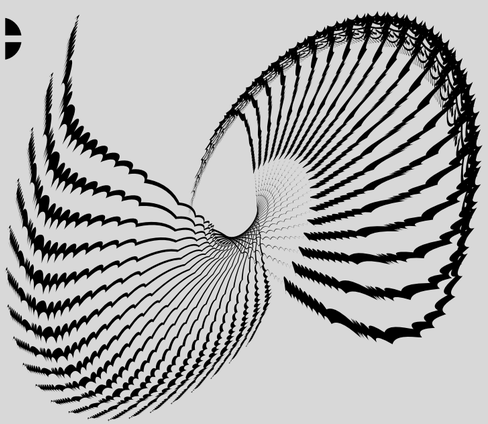
BRACE
NETWORK

****

BLOCKCHAIN CHALLENGES

Solving such issues led to developers facing the classic blockchain scalability trilemma. This trilemma states that there is a compromise between:Scability,Security and Decentralization.Even this trinity, however, does not define the limits of the technical challenges obstructing mass adoption of DLT. These include economic constraints such as high transaction fees, determining how finalization and consensus are achieved, and solving that issue discussed above – providing users with functional confirmation times

00004512 // 99374128 // 1005934



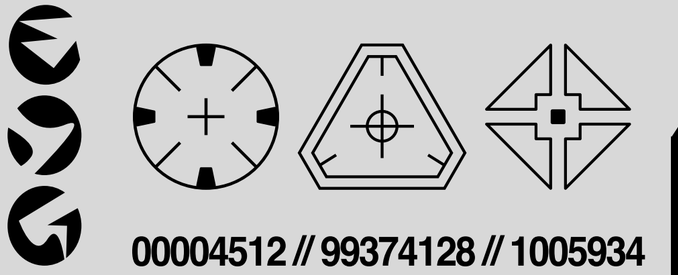
0 77832 12

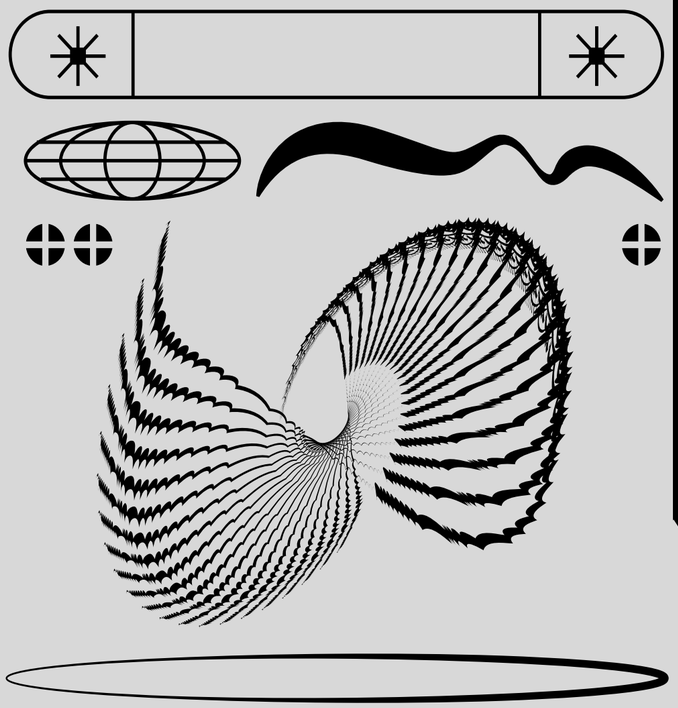
BRACE
NETWORK

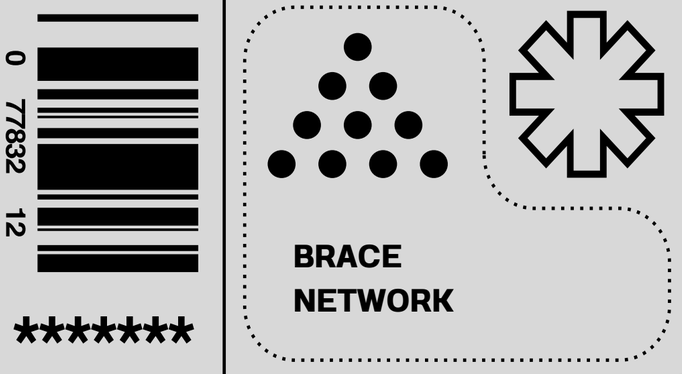
****

SCALE, FINALIZATION, AND CONSENSUS

Well-known blockchains such as Bitcoin and Ethereum allow decentralized nodes to write transactions to blocks. These transactions must then be agreed upon by all nodes and the block accepted on the chain. The strategy used is to agree one block at a time. The outcome of this approach is a compromise, in that, while a block may be approved in theory by the majority of nodes, if a transaction included on that block is later considered false, the entire block may be reverted, i.e., removed from the chain. Then valid transactions must be added to a new block. The consensus method affects issues of scale also. When each node must verify and store each block, then the dilemma that your "chain is only as strong as your weakest link" comes into play. That is, the performance of the system is limited by the transaction speed of the nodes

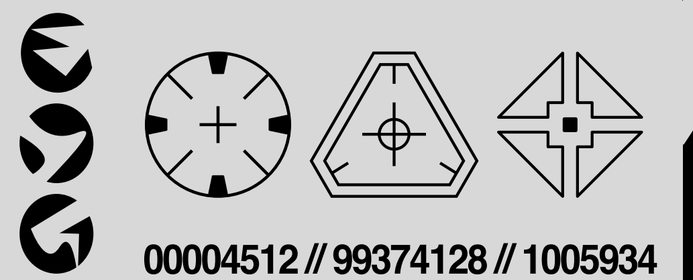


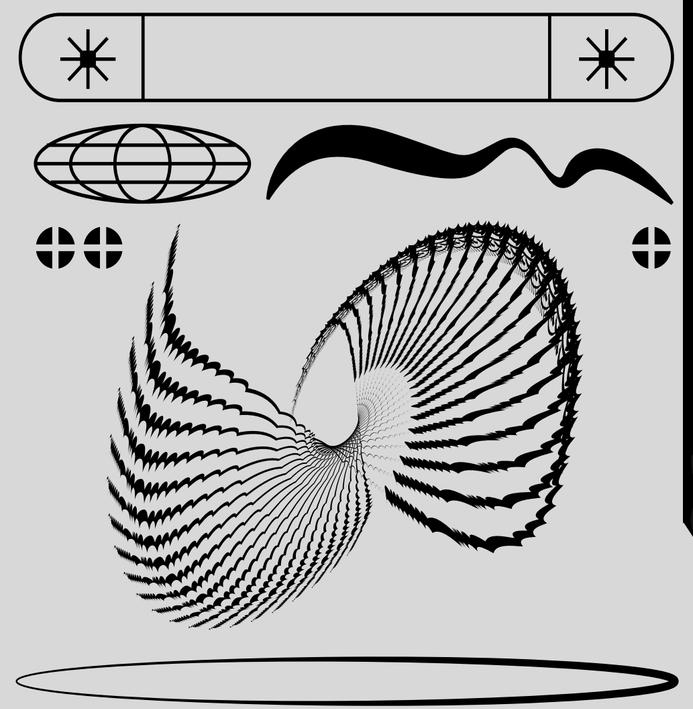


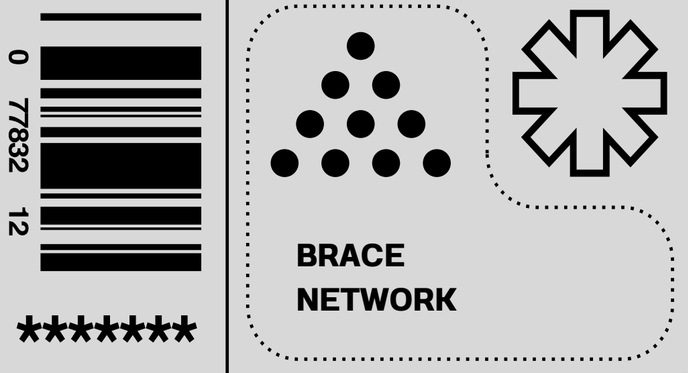


DECENTRALIZATION VS. FUNCTIONAL CONFIRMATION TIMES

The requirement to be able to revert a near "consensus" event is what dictates the blockchain finality time in distributed ledgers such as Bitcoin and Ethereum. Not only is consensus revertible, but confirmation time of that "consensus" is slow. Many blockchains, therefore, deal in "probabilistic finality", i.e., you can be close to certain that your transaction will not be reverted. This is why "centralized" chains have been adopted for DeFi, to meet customers' expectations around how long a crypto transaction should take. However, such a solution forces a compromise around decentralization – i.e., it must be given up. This makes them vulnerable to Denial of Service (DoS) attacks; see Section 3.2.1 Proof of Stake Security. A better solution is needed, and has been applied, to the Brace blockchain; see Section 3.1 for more on this Robust Blockchain Protocol.



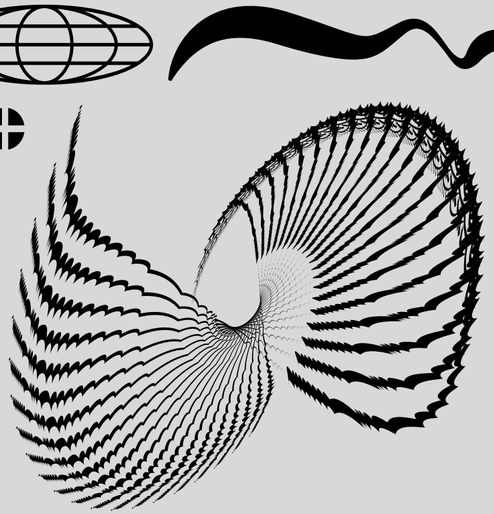




FEES

In a Proof of Work (PoW) system such as Bitcoin, and the original Ethereum model, a major cost in the system is the fees paid to block miners. It is the cost inherent to the system that protects against certain security issues. However, PoW requires powerful hardware which consumes large amounts of energy, contributing to the current energy crisis the economy faces. It also led to a form of centralization, in that the majority of mining pools came under the control of single entities. Furthermore, the fees constrain the function of the blockchain. They are simply too high to enable, for example, micropayments to support the functioning of dApps, for "trustless" gameplay, and more. This is one of the reasons why Ethereum launched its Proof-of-Stake (PoS) blockchain in December 2020 – with a full release in September 2022. PoS offers a cheaper model that also mitigates specific security issues.

00004512 // 99374128 // 1005934



0 77832 12

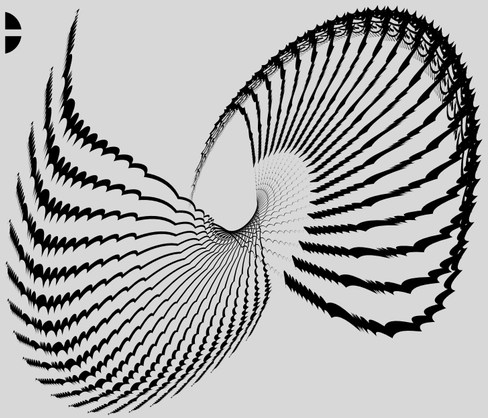
****

BRACE
NETWORK

ACCESSIBILITY

Another major challenge in the blockchain ecosystem is to overcome that barrier to entry: accessibility. DeFi’s innovative mechanisms have a very steep learning curve that prevents access to these services for most IT illiterate consumers. In fact, a double challenge presents itself; there are accessibility challenges for the IT illiterate consumers and for the developers

00004512 // 99374128 // 1005934



0 77832 12

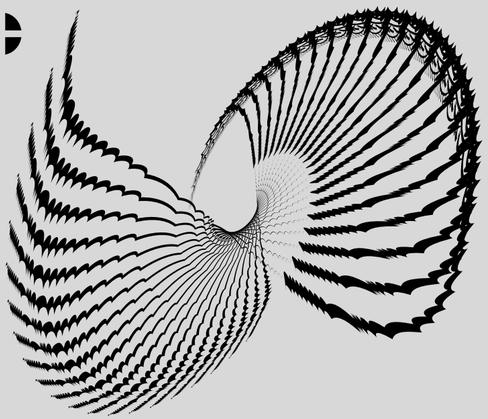
BRACE
NETWORK

****

USER ACCESSIBILITY

Highly technical people tend to already be financially stable and, typically, time-rich. They can research and troubleshoot, and have an existing community to access support from if the first two approaches fail. The economically dispossessed do not have such advantages. They are often time short, may have a poor understanding of the technology, and therefore face an apparently insurmountable barrier to entry into an ecosystem such as a blockchain DeFi marketplace. Of course, the majority of potential community members probably fall somewhere in the middle of these two extremes. It is vital that any emergent DeFi ecosystem recognizes, and works to overcome, such barriers to entry. Till now, innovators in the blockchain space have not done this well, and utilizing blockchain technologies requires that IT illiterate consumers overcome a steep learning curve.

00004512 // 99374128 // 1005934



0 77832 12

BRACE
NETWORK

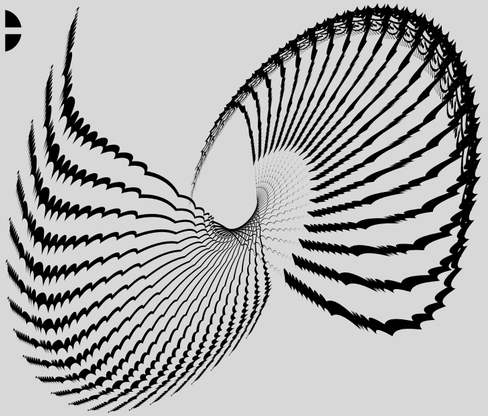
****

DEVELOPER ACCESSIBILITY

Building meaningful blockchain technology requires a developer team with deep experience in: cryptography, network security, sidechain security, the base blockchain layer, distributed systems, smart contracts, etc. However, most developers need only work with the smart contract code to develop dApps and the front-end code to enable users to interact with these. To truly remove the barriers to entry for most developers means abstracting away the requirement to work with the core blockchain to leave developers free to safely innovate in the dApp space.

00004512 // 99374128 // 1005934

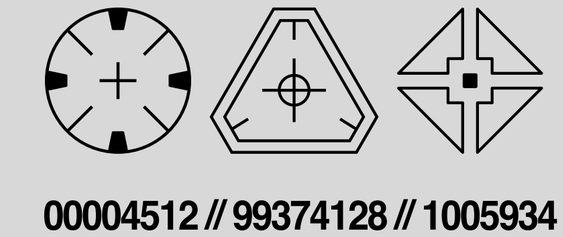
TOKENOMICS

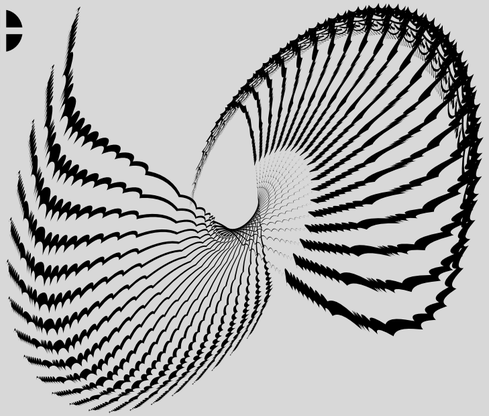


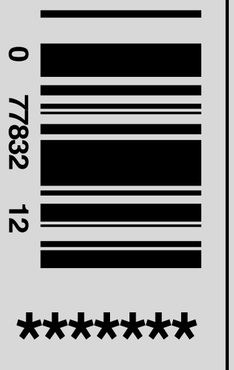
Tokenomics represent the value created by a blockchain ecosystem. They may be fungible tokens or non-fungible tokens, NFTs, or both.Not all tokens are created equal. Meme coin tokenomics, for example, exist in inflationary ecosystems, often with no limits on supply. While this might make for experimental investing and "get rich quick" at-the-cost of-others opportunities, they do not serve conservative investors who are interested in a more stable - finite supply ecosystem such as Bitcoin's or require genuine passive income

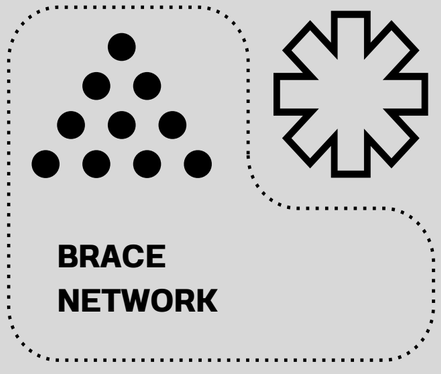
0 77832 12

BRACE
NETWORK



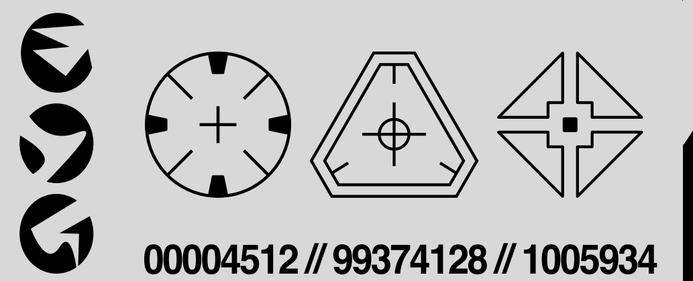


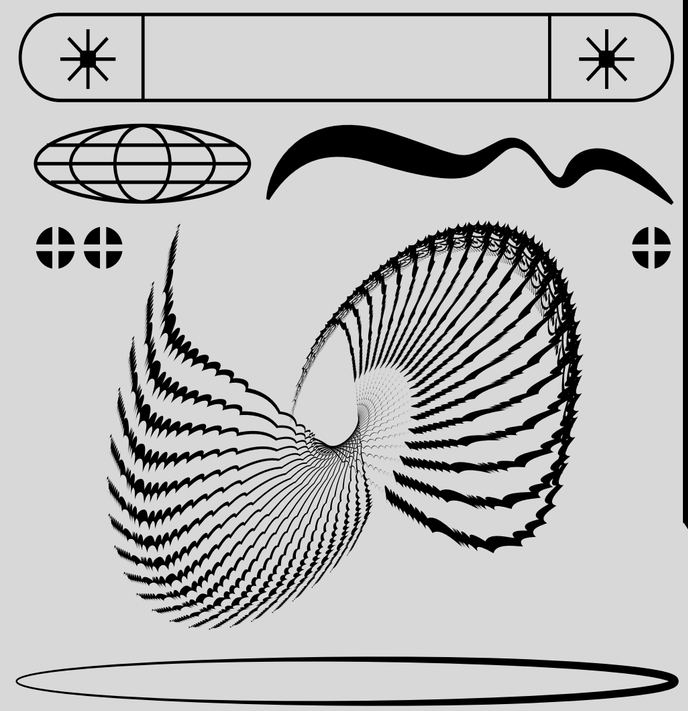


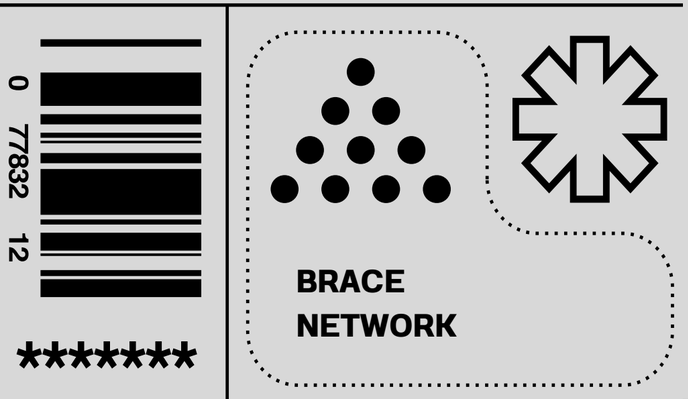


REPUTATION

One of the less tangible, but significant, challenges for any new technology is that of building a reliable reputation. The centralized banking systems that DeFi offers to replace have done an excellent job of building their reliable reputations. In a situation where a malicious player could emerge, i.e., the "take the money and run" approach, entities such as central banks have, instead, built the perception of security in that, time and again, the banks work honestly with our finances, and so we continue to trust them to do so. To leverage DeFi ecosystems, community members must be able to trust the blockchain mechanisms, the system security, the validators, and the smart contracts put into place. Therefore, a major challenge that the builders in the blockchain community must overcome is building a reliable reputation. Another issue closely related to reputation is that of legitimacy. Many single solution blockchains, such as those seeking to sell NFTs or launch new coins, fail to establish legitimacy or regulatory confidence. Furthermore, many new players in the DeFi and blockchain arenas struggle to provide enough liquidity to deal with the volatility of the digital assets markets to survive and scale.

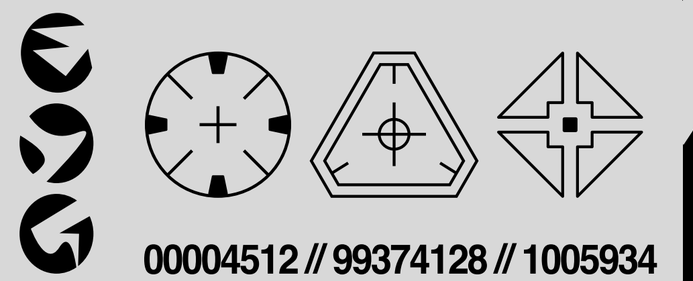


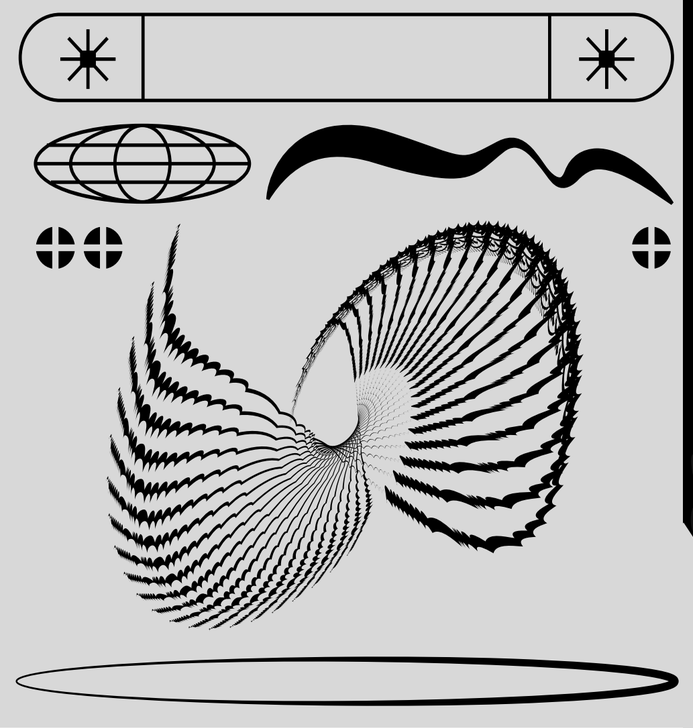


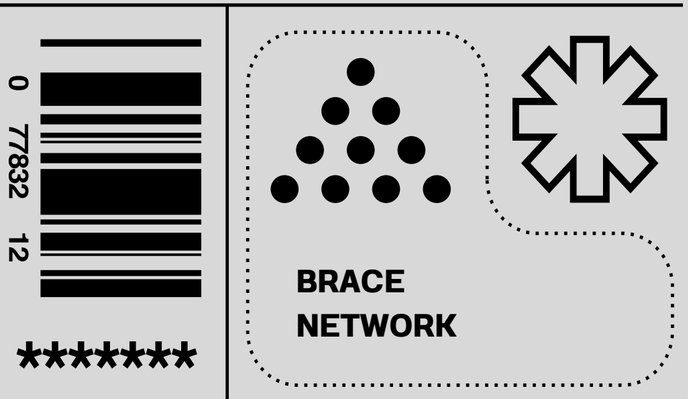


THE BRACE SOLUTION

There are significant challenges that the blockchain ecosystem has had to overcome. Brace is based on a blockchain that successively manages to solve the Blockchain Trilemma by providing, at the same time, speed of transaction, security, and significant scalability; see Section 3.1–3.2 below to understand more about the security features offered by the protocol. The Brace ecosystem also recognizes the challenges of building a reputation to establish a healthy user ecosystem and has strategies in place to mitigate these; see Section 3.3 Engaged Communities. Competing in an already competitive environment requires a solid financial base to finance the resources needed to sustain the project for the long term. The Brace Foundation has an economic strategy in place to address this; see Section 3.5 Resilient Economics.



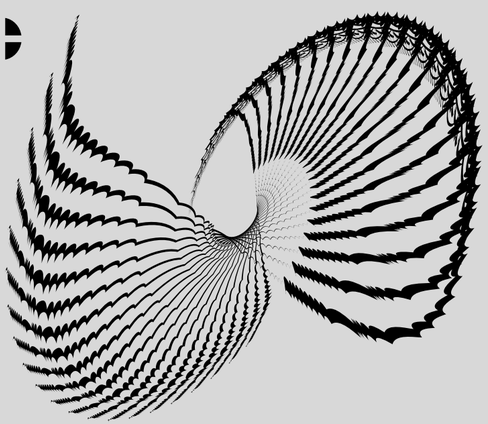




A ROBUST BLOCKCHAIN PROTOCOL

Brace leverages the best existing blockchain technology to achieve high scalability, security, and near-instant transactions. Implementing this decentralized Web3 infrastructure is only possible thanks to a solid team of in-house blockchain developers with many years of top-notch development experience in some of the best IT corporations and software development companies. As detailed in Section 2.1–2.3, significant challenges must be overcome to ensure that DLT, i.e., blockchain technology can be a functional technological solution. Brace aims to provide a decentralized blockchain with no central authority to provide irreversible and affordable transactions at scale. The Brace Network does not use Delegated Proof of Stake (DPoS), has no leader selection, and the voting process requires no “masternodes”.

00004512 // 99374128 // 1005934



0 77832 12

****

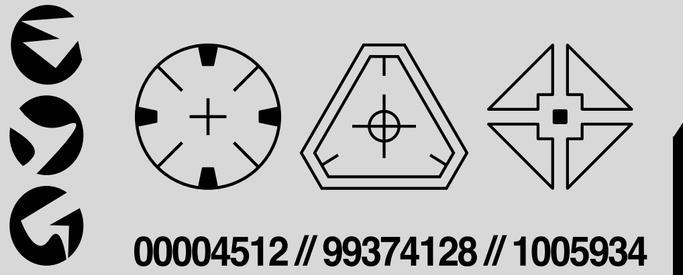
BRACE
NETWORK

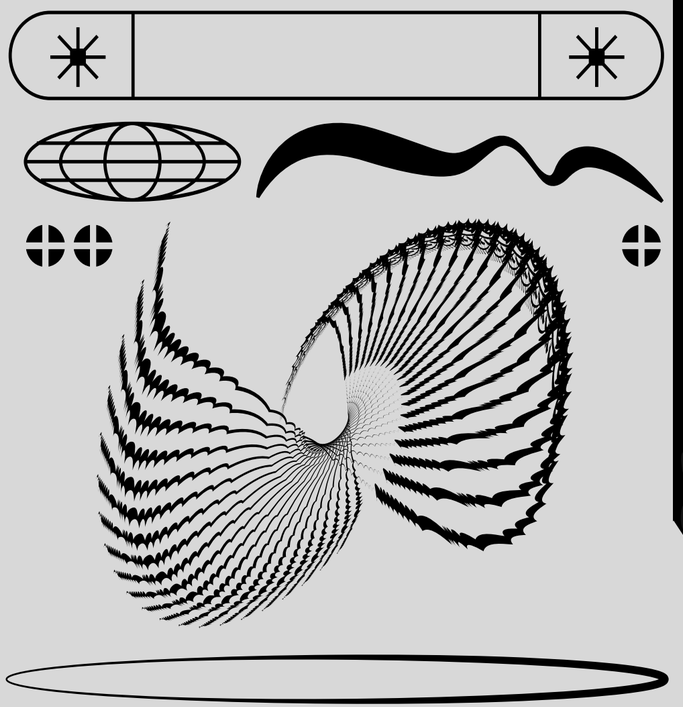
A ROBUST BLOCKCHAIN PROTOCOL

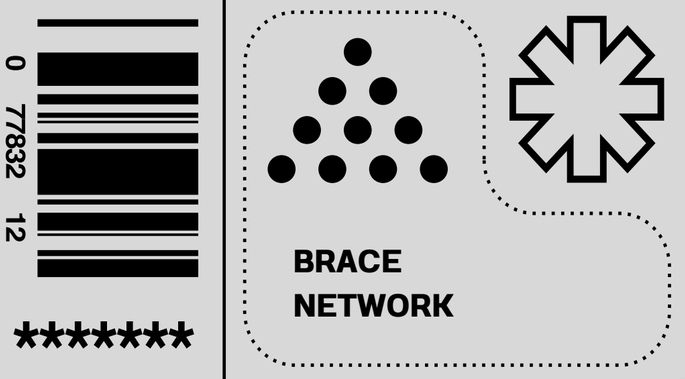
Thanks to the Lachesis Consensus Algorithm (LCA), the Brace Network implements leaderless PoS (LPoS) that supports:

Asynchronicity
Leaderless Consensus
Byzantine Fault Tolerance
` Fast finality

his leaderless consensus mechanism is integral to the Byzantine Fault Tolerance that enables the system to function even in the face of fraudulent transactions.





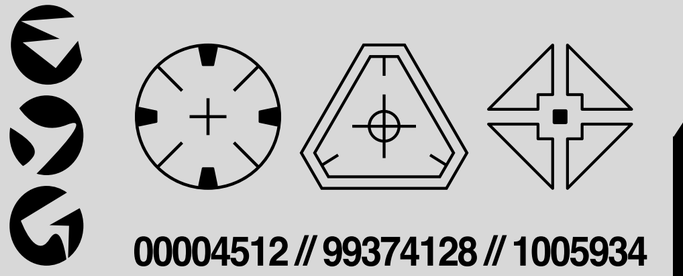


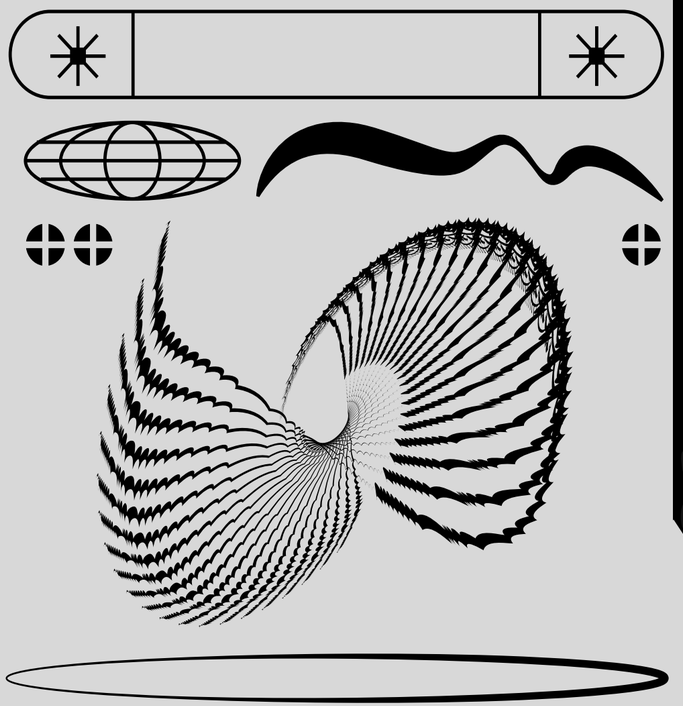
A ROBUST BLOCKCHAIN PROTOCOL

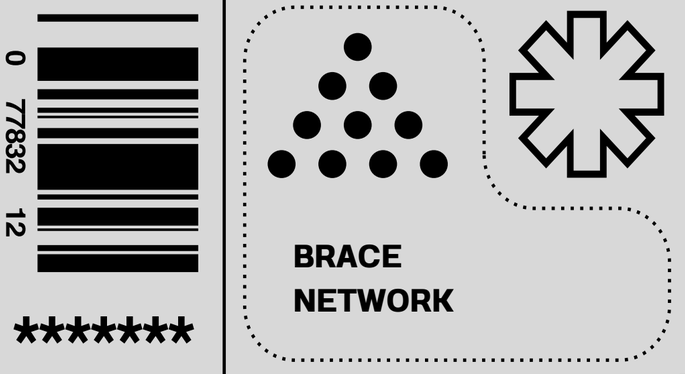
The Brace Network's asynchronous transactions are confirmed in a matter of seconds; see Section 5 for a deeper technical overview. ahis parallel processing means that the nodes are validating transactions without all having to work through the same queue. Note that nodes in the Brace blockchain do not need to pass entire blocks to each other; only events are synced between nodes. ahis consensus mechanism enables the validator nodes to scale to hundreds, or even thousands, of nodes. ahis further increases decentralization and, therefore, security. ahis PoS approach not only supports fast transaction speeds and decentralization, but it also saves both computing power and, therefore, electricity when compared to a PoW approach

SCABILITY

Brace implements a Layer 1 (L1) blockchain protocol that mitigates scalability issues. A novel model, the Directed Acyclic Graph (DAG), has been used to address the issue of scalability in a distributed ledger system. DAG's virtuous cycle enhances scalability as the network expands. The model applies a form of sharding, in which the validator set is split into groups. The validators assigned to each shard process transactions for the accounts assigned to their shard and update the ledger. See more about validating in Sections 4.5 and 5.3 below. The state (the record of accounts and transactions) and transaction processing (achieving consensus and processing messages, if required) are recorded on these disparate nodes – rather than attempting to achieve global consensus. This model has been adopted by Fantom, and the Brace network will provide an updated fork of Fantom, hence leveraging the benefits of this approach. Over time, as more independent validators deploy to the Brace blockchain, this will further secure the network and increase its decentralization



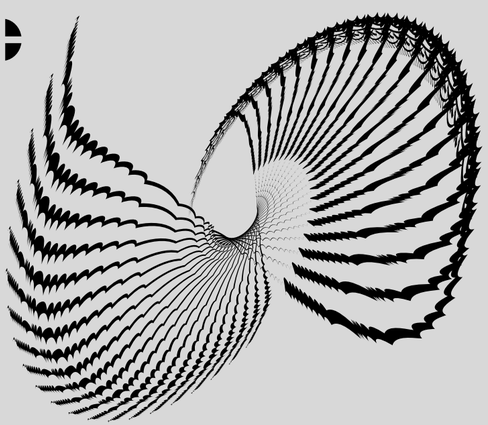




COMPATIBILITY

Brace supports Solidity, and the underlying blockchain is fully compatible with the Ethereum Virtual Machine (EVM). This means that developers can quickly port their existing Ethereum-based smart contracts and dApps to the Brace blockchain. Thanks to the EVM compatibility, BRACE will be made available as ERC-20 tokens, meaning that it conforms to the Ethereum standard supporting trading via sidechains. In May 2023 Brace successfully implemented its own ULC-20 standard. Brace also implements the de-facto industry standard Web3 API. That ensures that all existing crypto wallets are fully compatible with the Brace blockchain

00004512 // 99374128 // 1005934



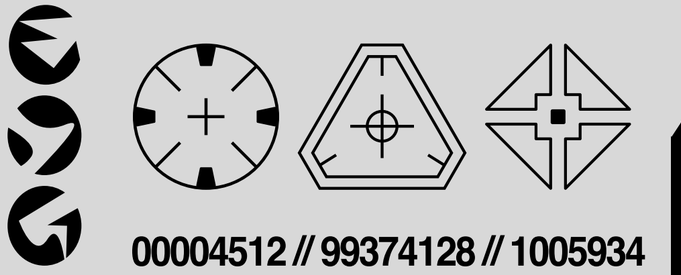
0 77832 12

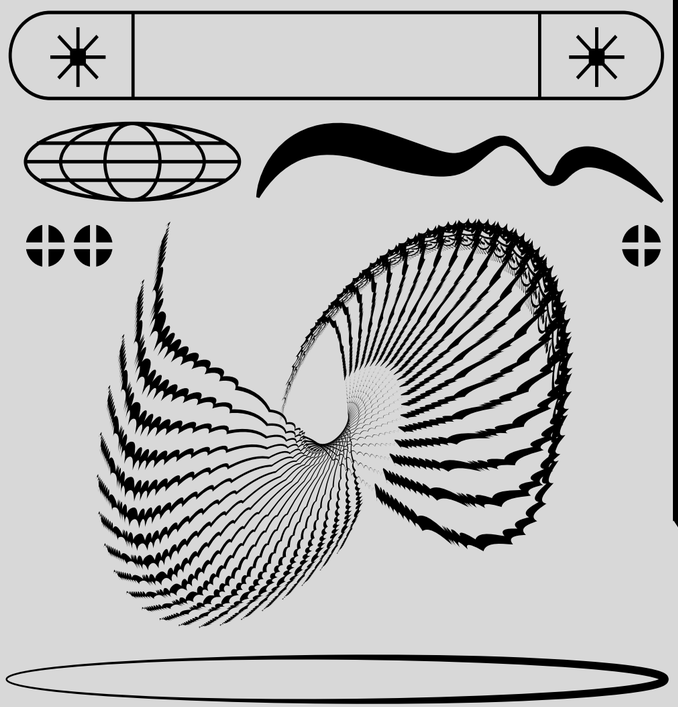
****

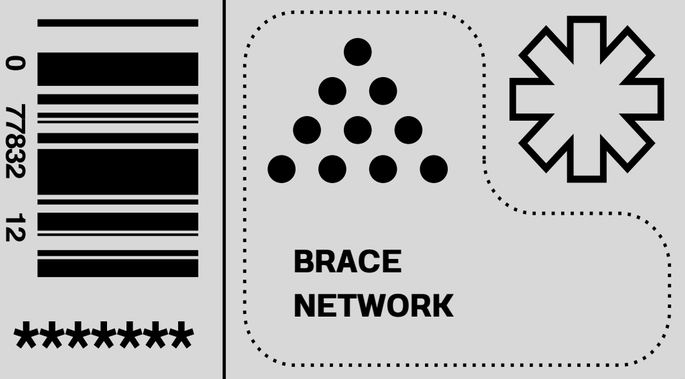
BRACE
NETWORK

PERMISSIONLESS DECENTRALIZATION

Brace blockchain is permissionless in that anyone can run a node in the network. This means that any members of the community of users with the technical know-how and capacity may run a validator node on Brace's mainnet and participate in securing the network. Even users without such capacity may assign a stake to validators and, thus, engage in the support and expansion of the ecosystem; see Section 4.5 in Tokenomics. One of the major challenges of decentralization – finality – is achieved in the Brace Network thanks to DAG registering and agreeing on the event history. DAG is used to establish the exact final order of events (in particular transactions) independently on each node.

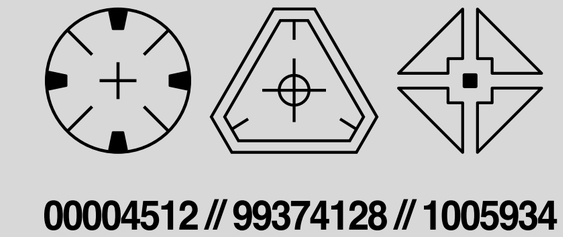


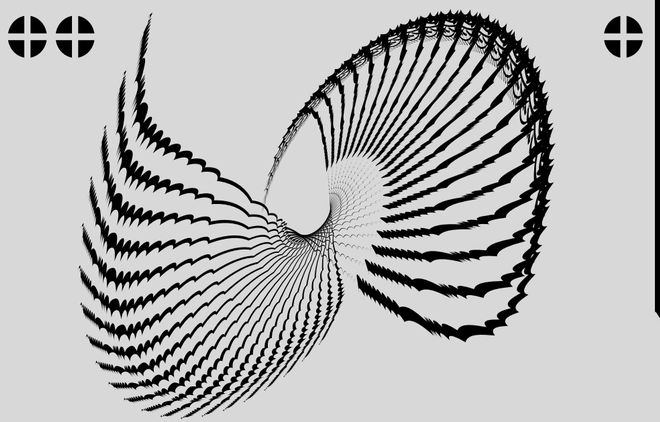


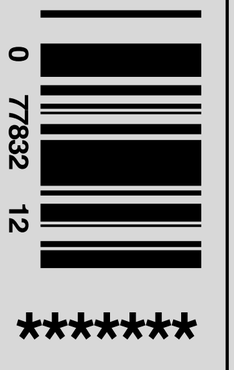


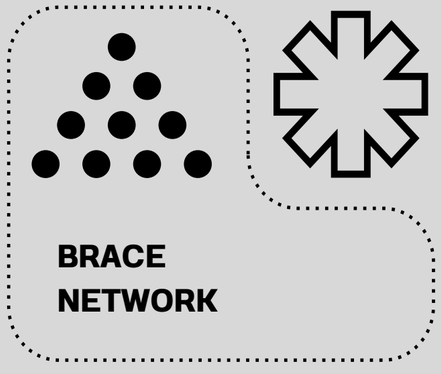
LEADERLESS PROOF OF STAKE

Staking requires that participants hold digital assets in a crypto wallet to support the operations of the blockchain network. In return, holders are rewarded for their contributions. Within the Brace Network, staking supports both the security (see Section 3.2 below) and the economics of the chain by providing a mechanism to support distributed consensus. Consensus is vital to ensure that the distributed network is both decentralized and immutable. It is achieved by the action of nodes within the chain – validator nodes. Validators commit a stake and agree to provision nodes according to a specified standard; see Section 5.3 for the technical requirements. The validator nodes are provided by ecosystem participants in return for BRACE rewards. The size of these rewards is based on a set of predetermined rules; see Section 4.5 Validator Reward Program.



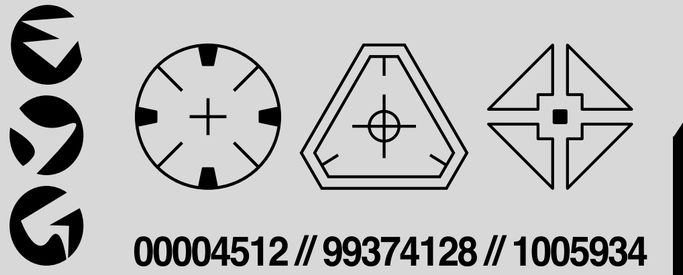


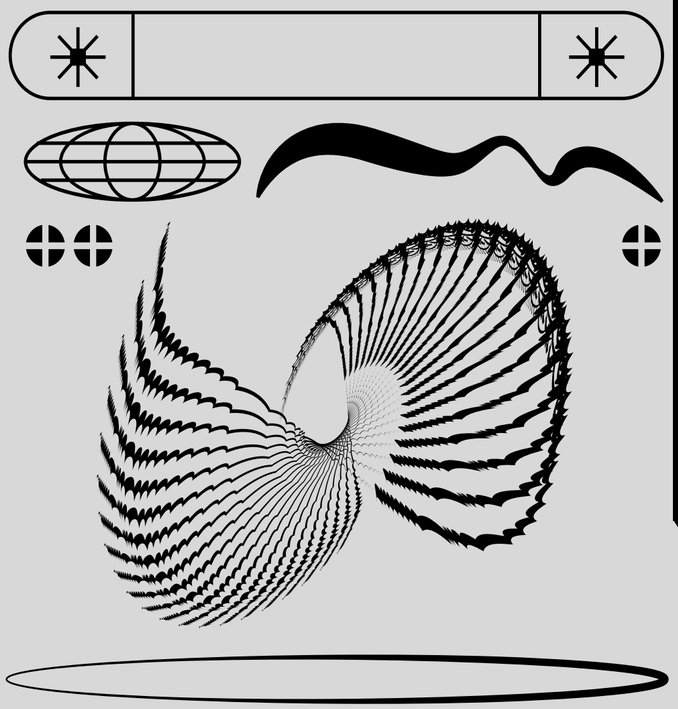


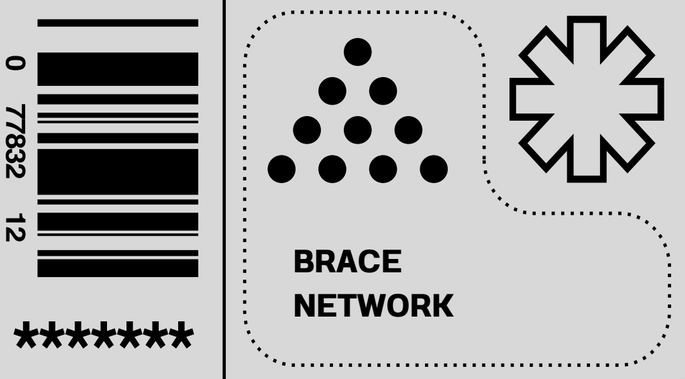


CRYPTOGRAPHY

Blockchain technology applies public-key cryptography based on elliptic curves over finite fields. Such cryptographic systems are almost ubiquitous now as this method is used to secure HTTPS connections by modern browsers. Applying such cryptography allows Brace to securely support both hardware wallets and software wallets and effectively use hardware acceleration to handle transactions.

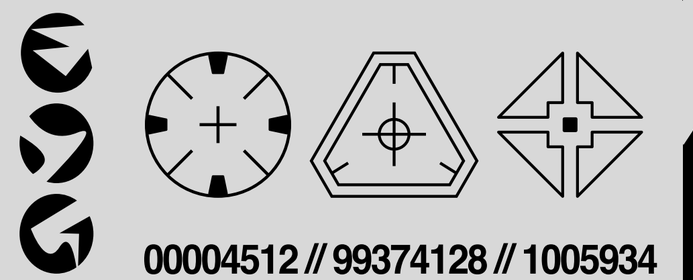


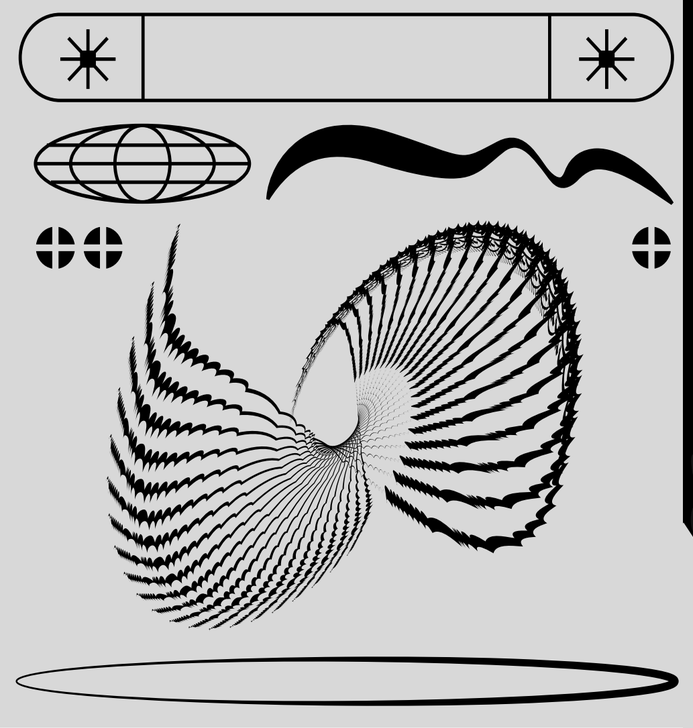


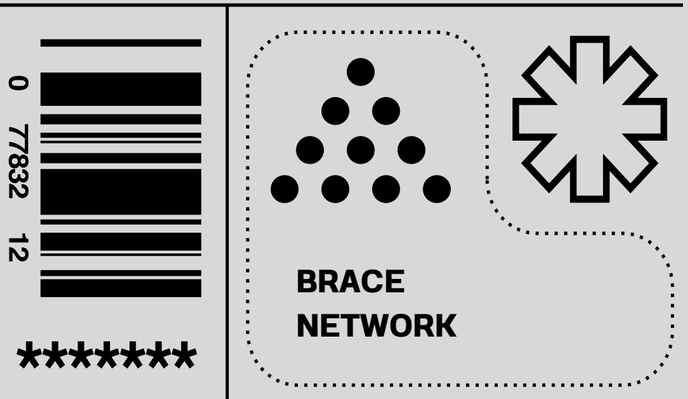


PROOF OF STAKE SECURITY

The Brace Network leverages LPoS, which is a leaderless PoS protocol, in favor of DPoS, that is, Delegated Proof of Stake. It has no leader selection or voting process and no concept of “masternodes”. The LPoS requires 2/3rd validator participation: meaning that a malicious actor would have to successfully deny more than 1/3rd of participants to successfully mount an attack. In DPoS, a fixed number of elected nodes, the delegates, are selected to create blocks. The delegates are voted for by token holders, whose voting power directly depends on the number of tokens they own. The issue is that the silver spoon effect creeps into such a system as tokens and, therefore, voting power spreads unevenly. So, while DPoS does well in terms of transaction throughput, it does not guarantee decentralization. The LPoS protocol does not have any delegates. Instead, validators lock tokens as a "stake" to be allowed to generate blocks. Restrictions are enforced within the Brace Network ecosystem to ensure that validators do not behave maliciously. That is, they have to accept meaningful levels of risks (along with their delegators). These restrictions include enforcing an upper ratio of the validator’s stake to the delegator’s stake. The upper threshold is set at 1:10, i.e., for every 1 token staked by a validator, the upper limit of its delegator pool is a 10 token stake.



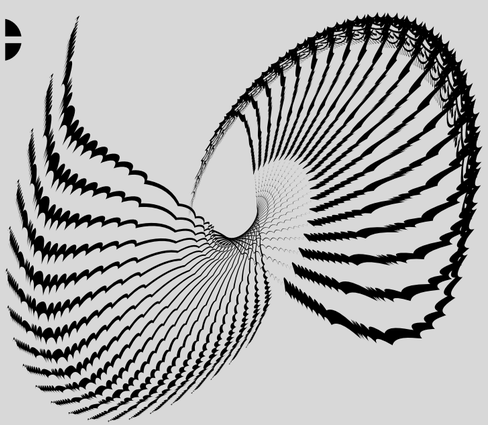




PROTECTION AGAINST SYBIL ATTACK

In the blockchain context, a Sybil attack is one in which an attacker subverts a system by creating myriad identities to run nodes, and applies them to gain a disproportionately large influence over the network. Alternatively, the attacker may run one node but attempt to operate that under multiple identities. Blockchains such as Bitcoin's PoW are theoretically vulnerable to the variant of a Sybil attack, a 51% attack aka Double Spending. Such blockchains' susceptibility to attack is proportional to the hashing power. Any agent that can hold 51% of the hashing power of the network, can overcome the security of that network. However, Blockchains such as Bitcoin are essentially protected from attack, because, to be economically viable, the market cap of the currency must be both sufficiently valuable to justify the cost of obtaining that hashing power, and affordable to the attacker.

00004512 // 99374128 // 1005934



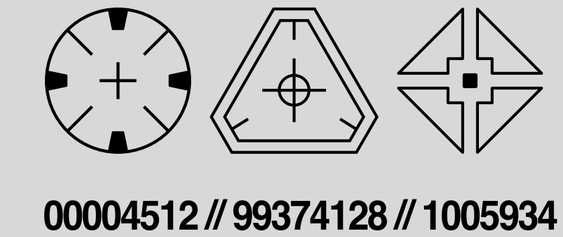
0 77832 12

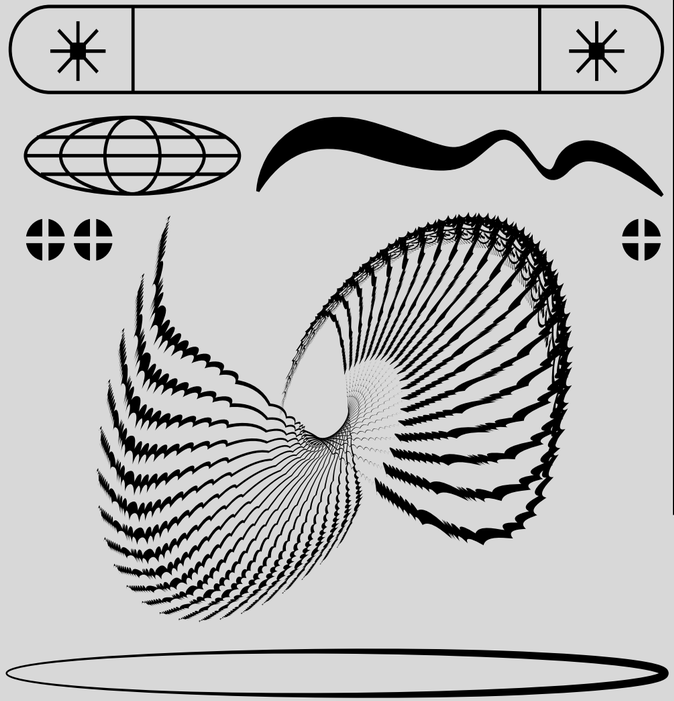
BRACE
NETWORK

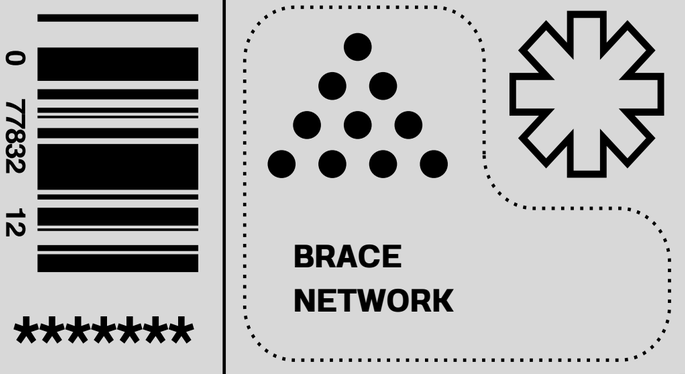
****

PROTECTION AGAINST SYBIL ATTACK

In a double-spend attack, a malicious actor attempts to spend their funds twice. Say Bob has 10 tokens and attempts to send 5 tokens to Alice and 6 tokens to Jill. While Bob → Alice and Bob → Jill are both valid transactions initially, this validity depends upon the status of the other transaction. It might be that both of these transactions of equal nonce both succeed in being entered as events – which is unlikely due to internal procedures – however, both transactions can not be confirmed thanks to the aBFT consensus algorithm. aBFT determines the event's order, which is equal on all the nodes unless more than 1/3rd of nodes are malicious. First, the order of events is determined, and only then are the transactions executed. This means that there must be an agreement that Bob sent tokens to Alice first or to Jill first. Whichever the agreement falls upon, let's say the 5 tokens sent to Alice for this example, this event will undergo a successful transaction. The Bob → Jill transaction attempt will be rejected because its nonce was already "occupied" by the Bob → Alice transaction. Agreement on timing is everything.



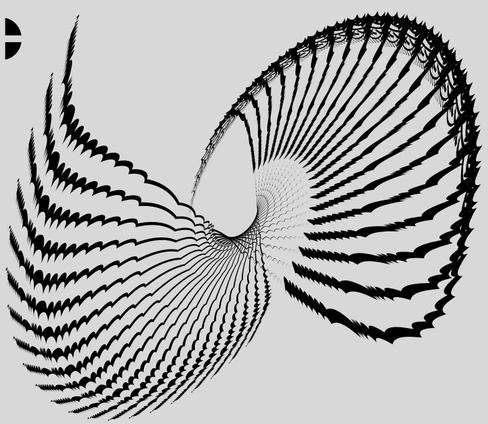




PROTECTION FROM A PARASITE CHAIN ATTACK

In one variant of a Double Spending attack, the Parasite Chain attack, a malicious actor places a transaction of a specified value in the main DAG chain, while attempting to replicate this on a thread in an attempt to double-spend the tokens. Brace's blockchain protocol does not start with a main chain. It generates the main chain from threads of chains using a graph protocol related to network analysis in biological systems. This means that, theoretically, any thread can ultimately come to belong to the main chain. So, what prevents a malicious parasite chain from making a successful attack? A thread chain must have a parent chain for whom the verification of each Event Block can be successfully performed. This means that a parasite chain with a false history – the parasite thread will not be accepted unless the history it attests to reflects that of the main chain. Also, there must be a connection between the existing main chain and any thread to be added to it – preventing a parasite thread from creating a false history of Event Blocks and successfully merging. To successfully add a false history, more than 1/3rd of the nodes would have to be malicious.

00004512 // 99374128 // 1005934



0 77832 12

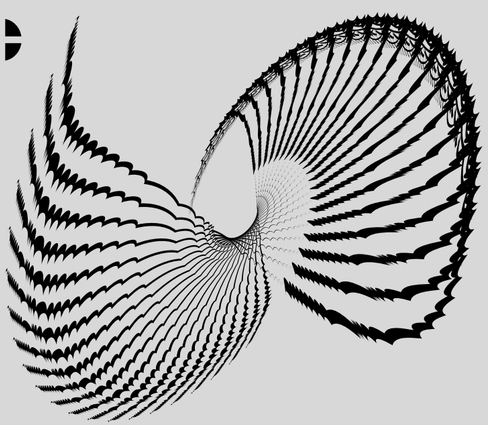
BRACE
NETWORK

****

PROTECTION AGAINST DENIAL OF SERVICE ATTACK

A DoS attack is typically attempted by flooding the targeted system with transaction requests. For example, a malicious actor may submit a large number of (valid or invalid) transactions from account/s within their control to attempt to overload the network. Distributed blockchains are, by their nature, less vulnerable to DoS attack, or Distributed DoS (DDoS) attack, than centralized systems. Not only does the aBFT protocol allow for messages to be delayed or lost entirely, but it also makes the chain resilient to DDoS attacks. This relies, of course, on the chain being of a large enough size to provide the "coverage", i.e., to offer true decentralization. This is why the more centralized blockchains have been shut down repeatedly by DDoS attacks. The coin-based system FTM, for example, has functioned on less than 100 nodes securely

00004512 // 99374128 // 1005934



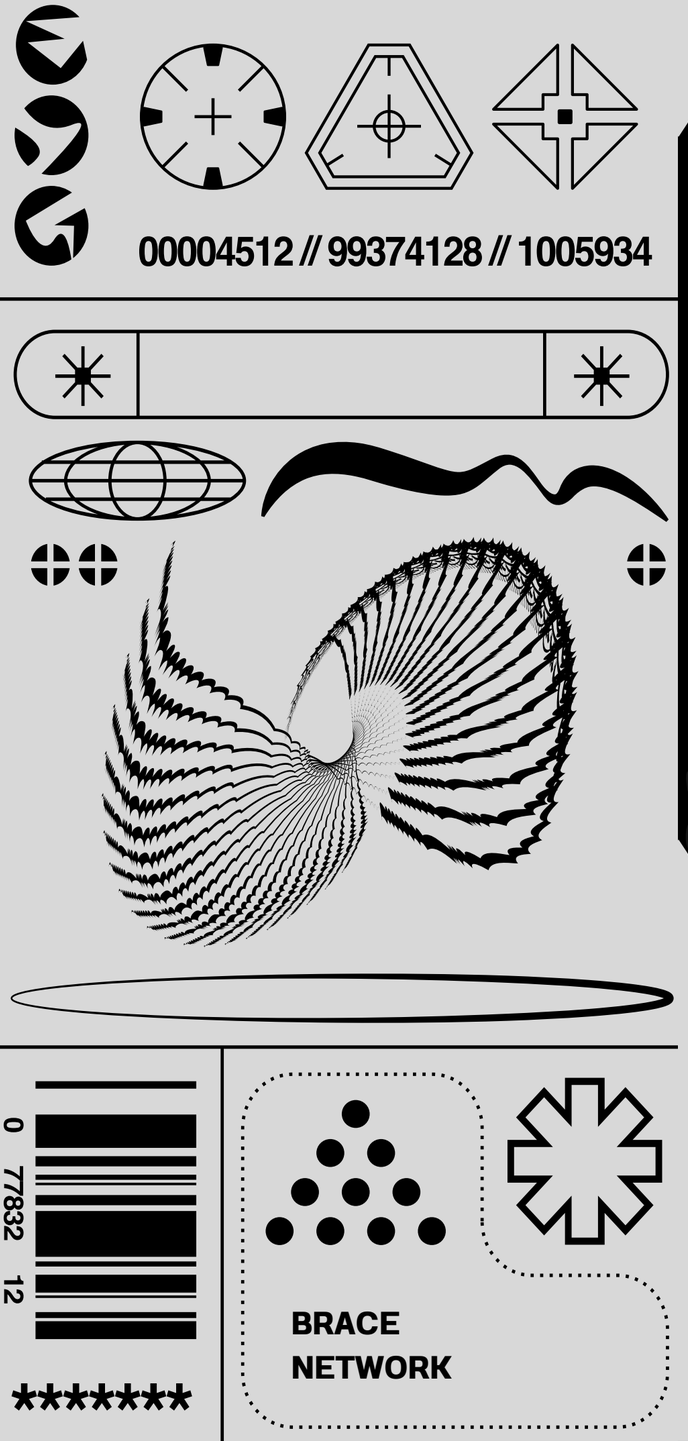
0 77832 12

BRACE
NETWORK

****

PROTECTION AGAINST DENIAL OF SERVICE ATTACK

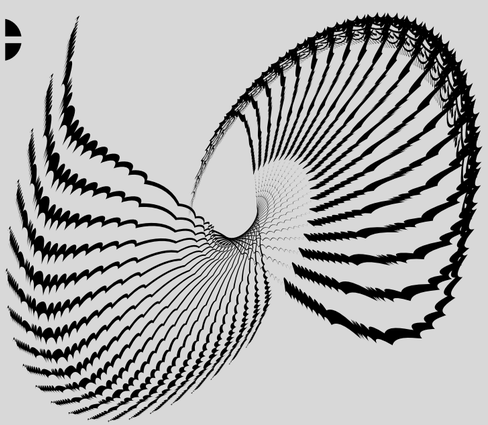
The tokenomics strategy applied by the Brace system is designed to prevent DDos attacks; see Section 4 Tokenomics. The transaction fee applied to each transaction provides a prohibitive cost to performing DOS attacks. Even a minimal transaction fee means that it is extremely costly to flood the transaction pool. A variant of the DDoS attack is to overload the validator nodes with a flood of valid events. In the Bob → Alice and Bob → Jill transaction example above, Alice pays the fee for the successful transaction, and Jill does not pay for the unsuccessful attempt. The validator, however, will see its gas power decreased by the gas limit of both transactions – as a penalty for originating conflicting transactions. The gas power value will limit the maximum number of transactions per second (TPS) that may be instigated by a validator, therefore, preventing any validator node from supporting such an attack strategy.



QUANTUM SECURE

DAG offers quantum resistance, i.e., the underlying distributed ledger is less susceptible to quantum computers with high-level computing properties. Cryptography based on elliptic curves over finite fields is a widely-used cryptographic system. The Brace Network signatures are based on the Elliptic Curve Digital Signature Algorithm secp256k1 curve. The security of this system is based on the hardness of the Elliptic Curve Discrete Log Problem (ECDLP). Theoretically, any key can be broken; however, even with today's computing power, estimates suggest that the energy required would be equivalent to that required to bring all the water on Earth to a boil. This means that, by their nature, cryptographic protocols offer security against attack. The potential threat comes from the development of a sufficiently large quantum computer. Of specific interest to cryptocurrencies is how this relates to the elliptic curve signature scheme. Experts theorize that a quantum computer could break this form of cryptography by or before 2030. As a theoretically quantum-proof cryptographic algorithm does not currently exist, the Brace Network architecture implements multiple cryptographic systems supporting a modular architecture design; thus providing layers of resistance

00004512 // 99374128 // 1005934



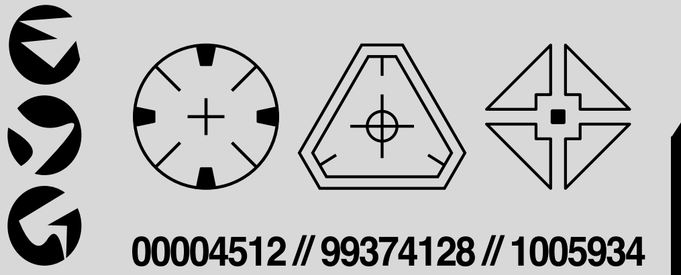
0 77832 12

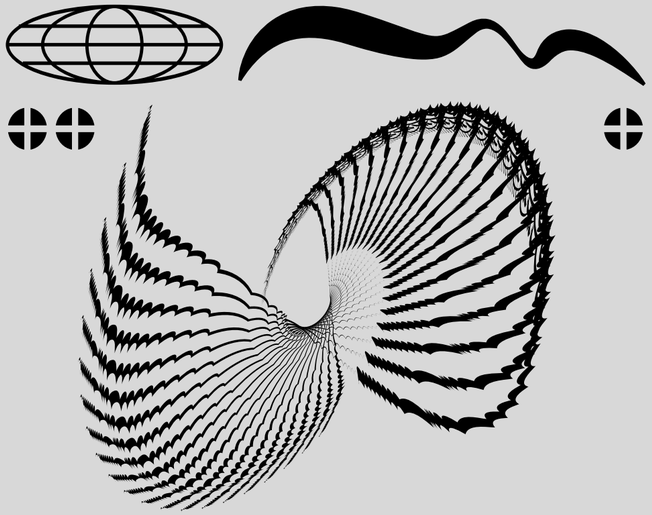
****

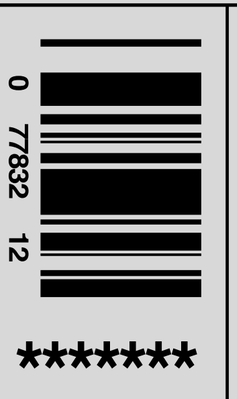
BRACE
NETWORK

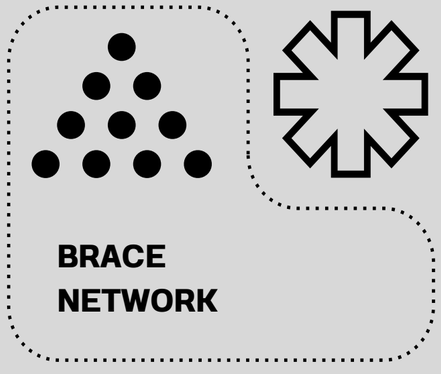
NFT MARKETPLACE

An NFT Marketplace is a gateway for users to mint, buy, create, trade, explore, sell, and exchange NFTs. These NFTs can be in the form of digital identity ownership of digital art pieces, such as paintings, 3D video graphics, collectible items, metaverse avatars, and digital audio files.



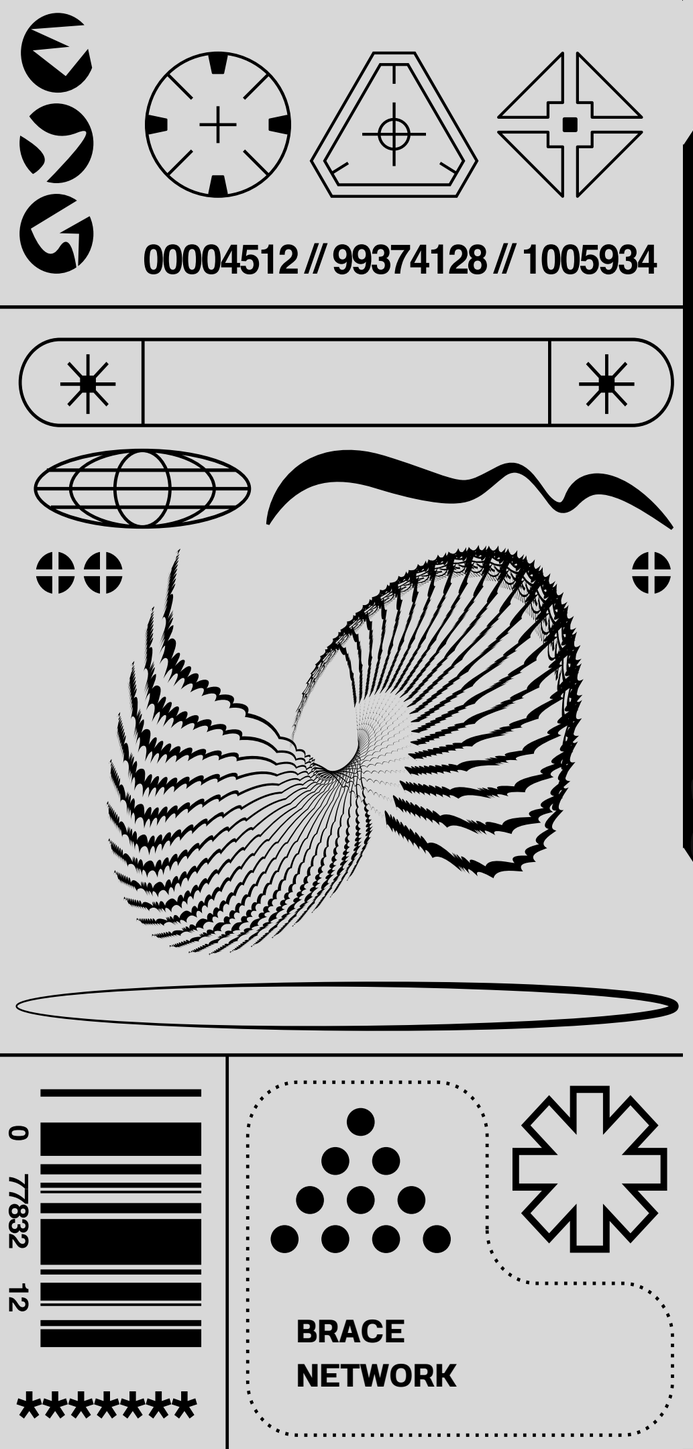






STAKING HUB NFTS

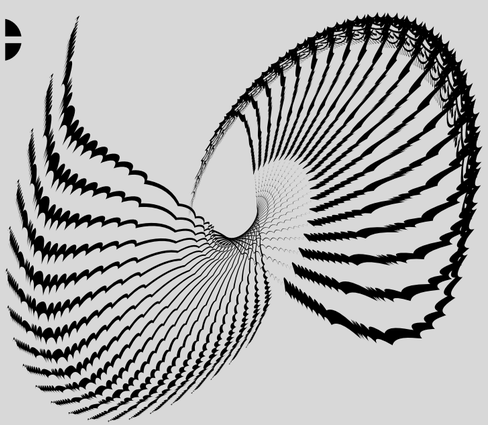
The Staking Hub NFT is an innovative digital asset management instrument developed by the Brace Foundation that enables users to acquire the ownership of a staking node that delivers APR returns in BRACE coins daily. There will be seven tiers of Staking Hub NFTs with different characteristics to fulfill the needs of multiple users. The coins generated through these Hubs will be locked for a period and gradually unlocked to enable users to exchange the coins on a secondary market while guaranteeing enough liquidity to the complete ecosystem



IDO LAUNCHPAD

An IDO LaunchPad is a system to let users participate in the initial crowdfunding fundraising steps to raise digital capital and liquidity for a new blockchain project with a dedicated utility token that is not yet listed on the open market

00004512 // 99374128 // 1005934



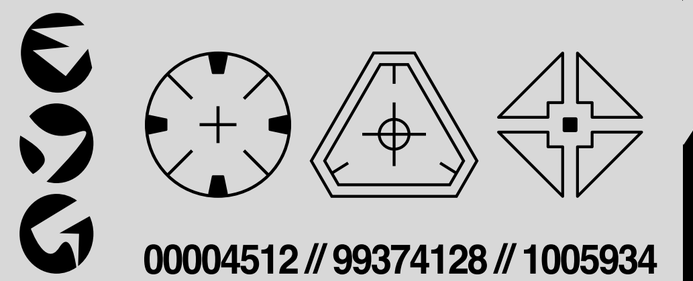
0 77832 12

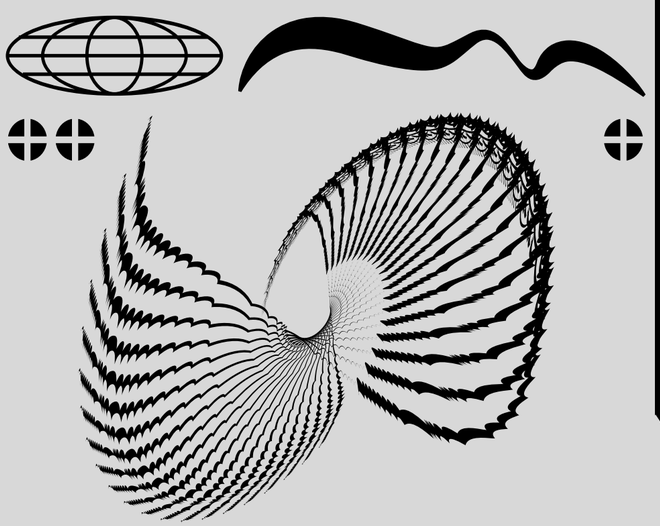
****

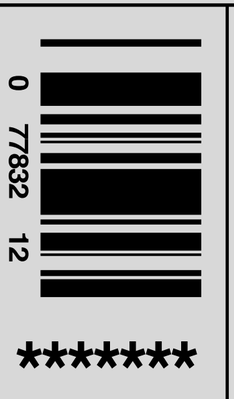
BRACE
NETWORK

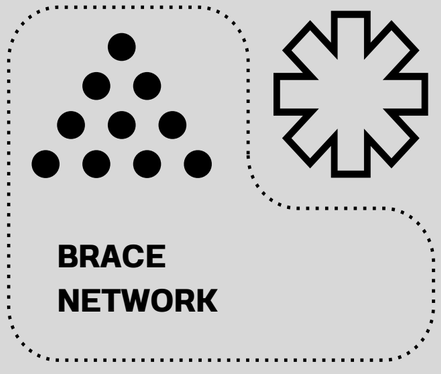
CROSS-CHAIN BRIDGES

Cross-Chain bridges are technological mechanisms to connect different blockchains by providing viable interoperable characteristics that let users transact, share smart contracts, and store different coins on versatile digital wallets of multiple chains





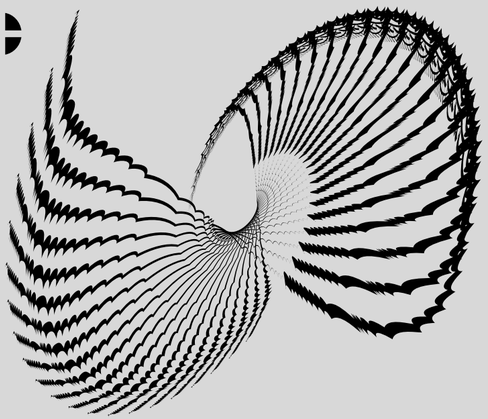




YIELD OPTIMIZERS

A Yield Optimizer is an automatic digital service that enables automated bots to exchange transactions to optimize cryptocurrency returns in a highly mathematically-efficient way.

00004512 // 99374128 // 1005934



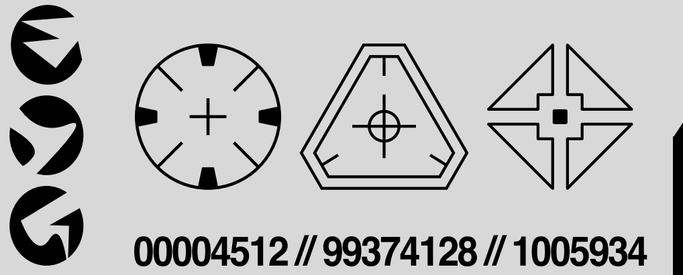
0 77832 12

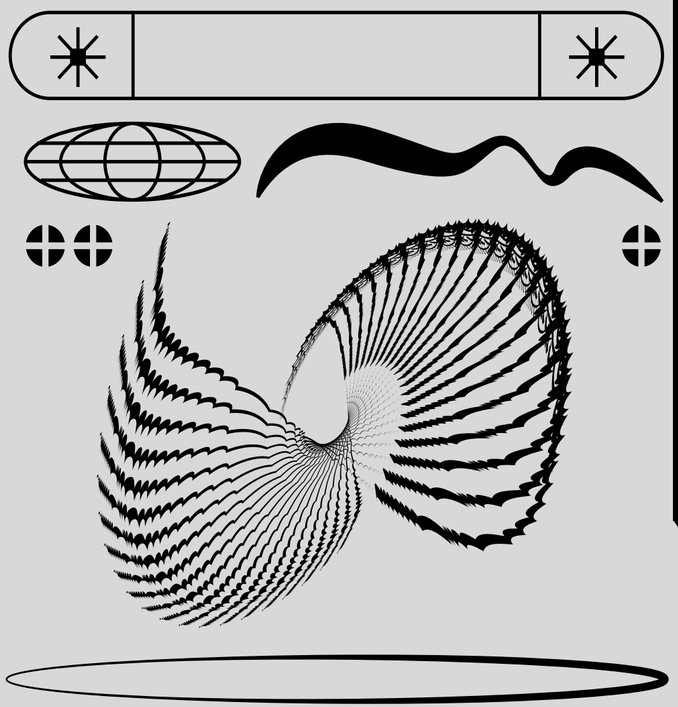
****

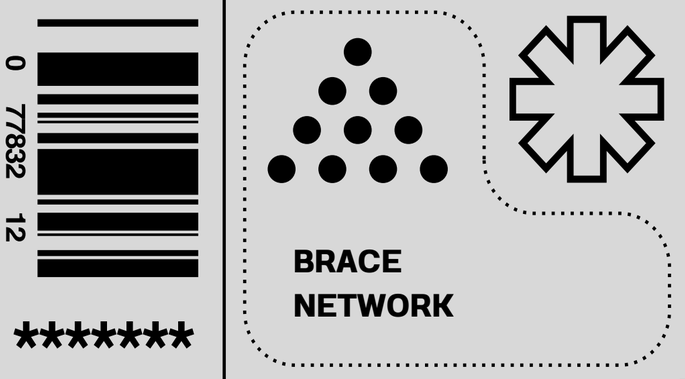
BRACE
NETWORK

LENDING-BORROWING PORTAL

A Lending-Borrowing portal is a platform that enables P2P lending and borrowing of crypto funds that are intermediary-free and deliver much higher interest rates than traditional banking institutions

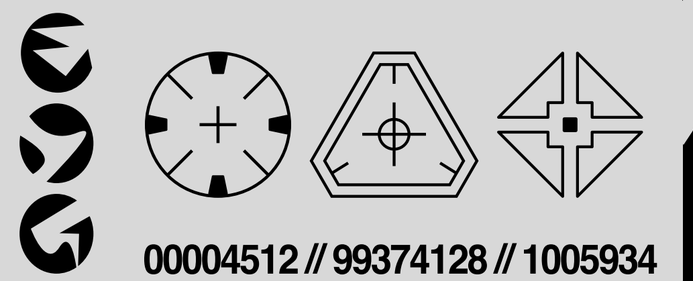


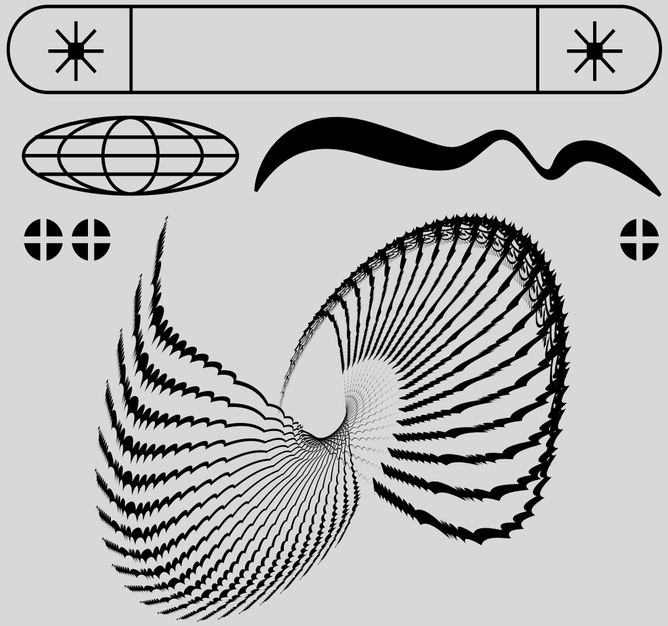


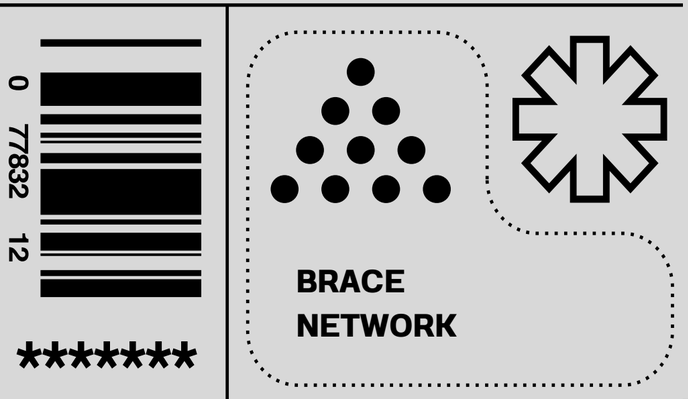


BRACE SWAP (DEX)

A DEX is a digital platform that enables the efficient exchange of multiple crypto asset pairs without intermediaries. The trading pairs will cover the major stable coins like USDT, DAI, USDC, and the native BRACE coin. The transaction fee will be as low as 0.3% per transaction. The Brace team will continuously monitor the blockchain ecosystem, in particular, DeFi, and if other new revolutionary products start to gain enough traction, they will be included in the deployment pipeline. Furthermore, Brace is also actively looking into incorporating NFT-based games and GameFi applications in the dApp’s palette.

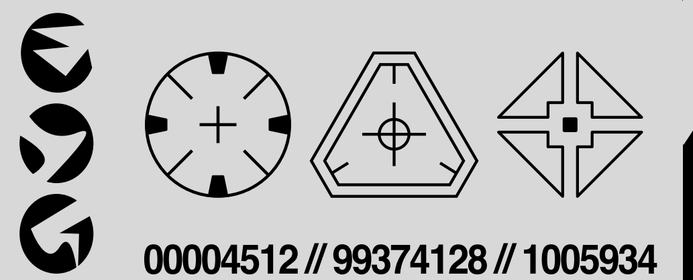


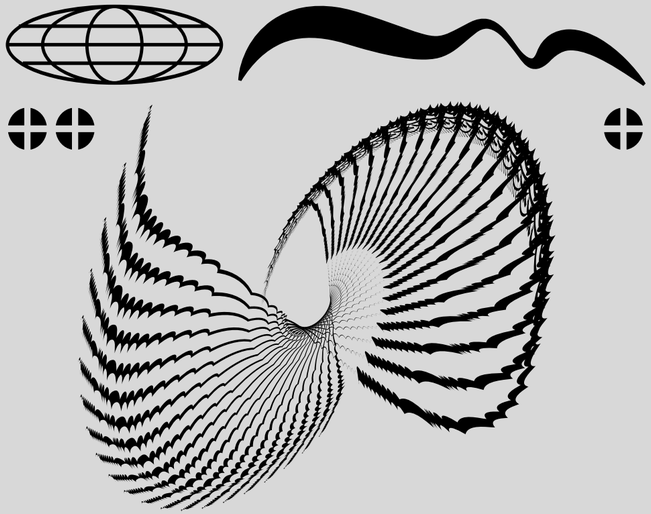


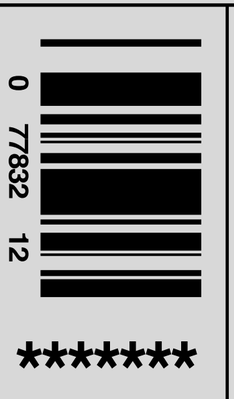


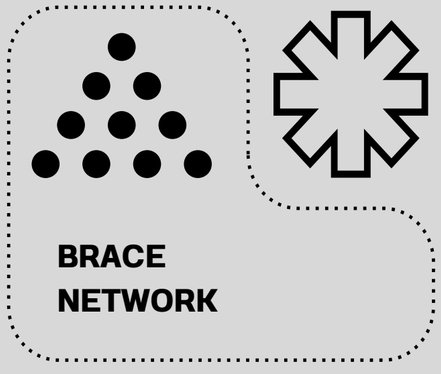
FAMILIAR LANGUAGE SUPPORT

Brace will support Web3 API for multiple widely-used standard programming languages like C#, Python, Go, Java, JavaScript, and smart contracts written for EVM-compatible frameworks like Solidity and Vyper, to leverage existing libraries of smart contract templates. Moreover, Brace will also encourage further development and integration with well-known tools such as Truffle, MetaMask, and Remix.





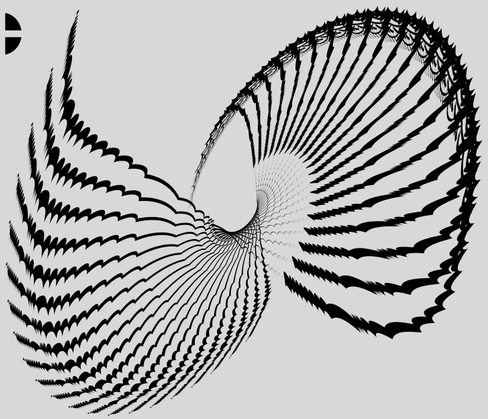




EVM-COMPATIBLE

The Brace blockchain is compatible with the EVM: the runtime environment for smart contracts applied to Ethereum. Because it is sandboxed, this means that code running inside the EVM has no access to the network, filesystem, or other processes. Smart contracts even have limited access to other smart contracts. This provides both a level of security and familiarity for dApp developers

00004512 // 99374128 // 1005934



0 77832 12

BRACE
NETWORK

****

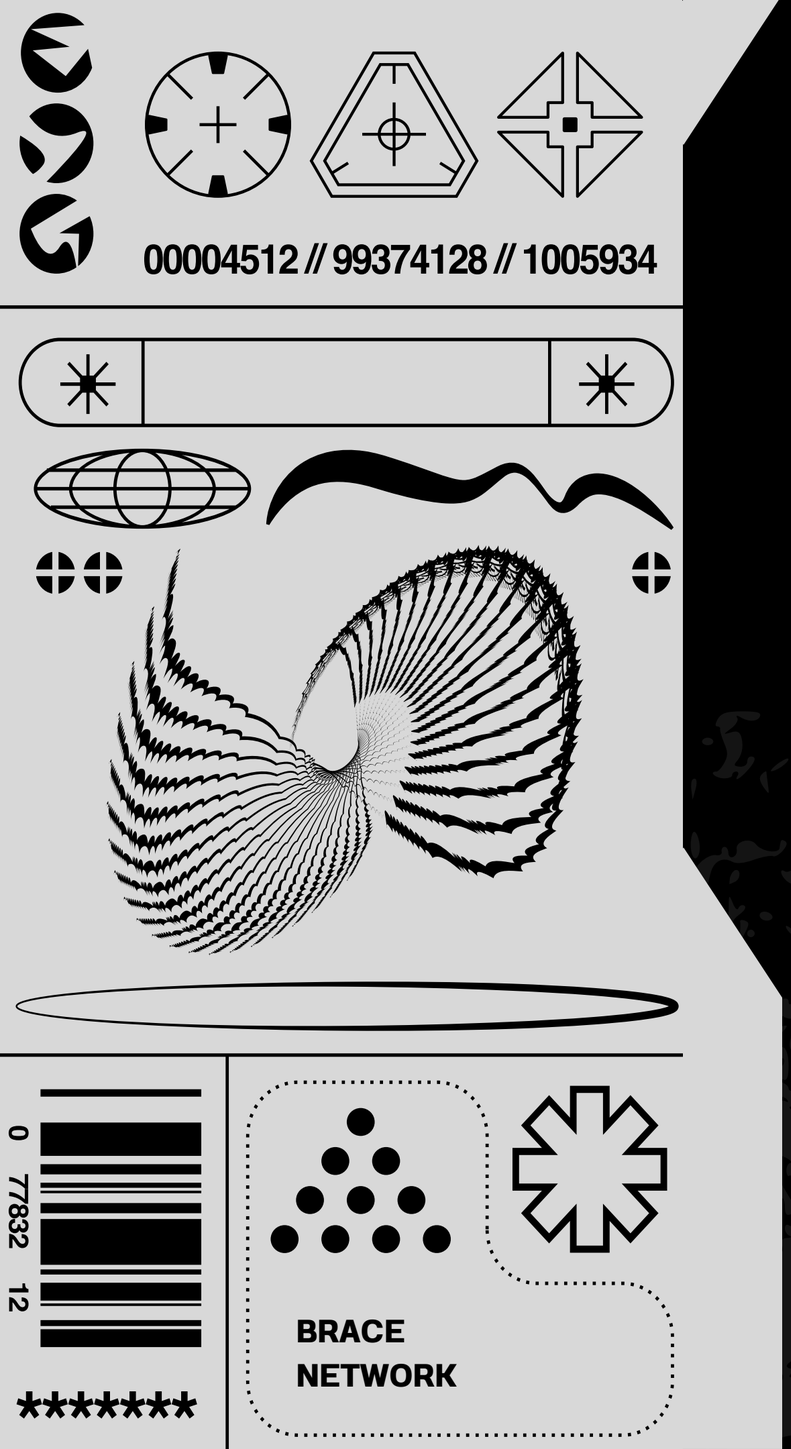
FUNCTIONAL UTILITIES OF BRACE

1. Securing the Network: Validator Staking

The most important utility of the BRACE coin is securing the network via the PoS system. Stakers can participate by setting up a validator node or delegating their stake to a validator and then locking their coins for a specified amount of time. Stakers earn rewards proportionally, according to the number of coins delegated and the duration of the lock-up, depending on the validator’s uptime and stability.

2. Securing the Network: Fees

On the Brace protocol, there are fees for transactions and smart contract interactions. These fees are tracked with BRACE and are very low – but sufficient to make it extremely expensive for a malicious actor to carry out an attack



FUNCTIONAL UTILITIES OF BRACE

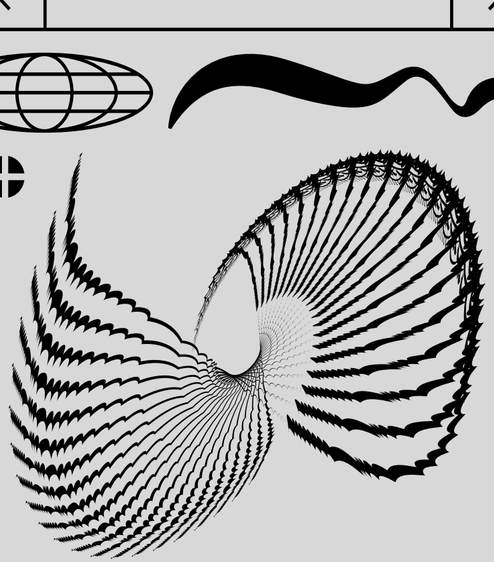
3. Payments

Brace's network executes thousands of transactions every second, keeping transaction cost inflation at scale and payment costs to a minimum – making Brace a suitable choice for transactions.

4. Native dApps

BRACE is the primary utility coin of the native dApps (e.g., to repay interest on a digital assets, liquidity mining, etc.). Once released, dApps will maximize the utility of BRACE within the Brace ecosystem and, with ecosystem growth, coin holders will be involved in future governance decisions on the Brace blockchain.

00004512 // 99374128 // 1005934



0 77832 12

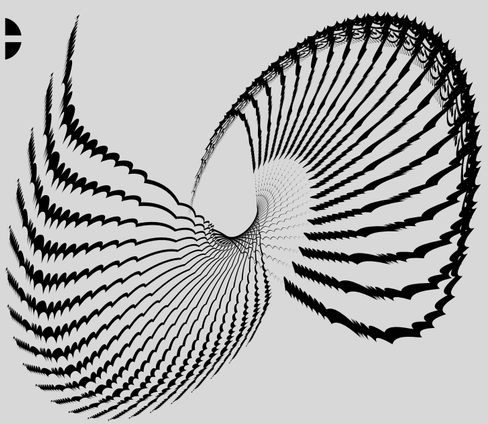
****

BRACE
NETWORK

TECHNICAL OVERVIEW

The Brace blockchain implements the Brace Network. This applies a protocol to mitigate against scalability issues and improves the processing time.The Brace Network is capable of processing both transactional information and associated metadata. This metadata storage enables historical information to be retrieved. The structure of this metadata is very similar in form to transactional data with the addition of properties such as inheritance. The Brace Network is effectively constantly building a picture of the connections between nodes, much like nearest-neighbor network analysis in biological systems. Rather than having a single chain requiring global consensus in near real time to add a new block, the Brace blockchain has many threads which are later "woven" into the chain. This strategy avoids having to undertake a reorg, i.e., a reorganization of the main chain.

00004512 // 99374128 // 1005934



0 77832 12

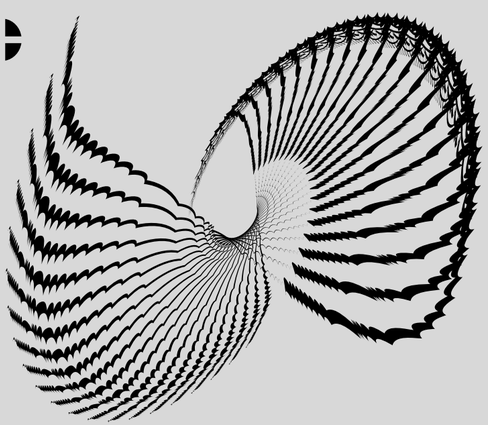
****

BRACE
NETWORK

TECHNICAL OVERVIEW

Graph theory, an established mathematical field, has been extended to be applied to DLT. The Brace Network is created from a network, also known as a graph – a mathematical approach to represent a network. The mathematics underpinning graphs captures relationships between entities or objects, known as nodes. A graph is composed of sets of nodes, i.e., discrete points that are interconnected.

00004512 // 99374128 // 1005934



0 77832 12

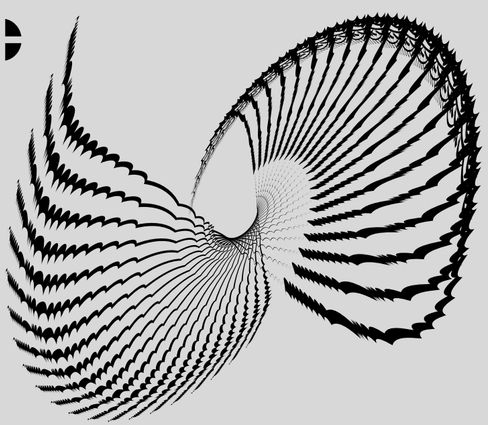
****

BRACE
NETWORK

BRACE NETWORK AND THE DIRECTED ACYCLIC GRAPH

Brace blockchain is built on a DAG-based asynchronous Byzantine Fault Tolerant consensus algorithm (DAG-aBFT). This ensures that transactions are asynchronous, leaderless, and final. DAG-based protocols achieve consensus around a partially ordered record of transactions. This creates “width”, which increases the throughput of the system, see Fig. 5.1. The blockchain is Byzantine Fault Tolerant in that it is able to function even when up to 1/3rd of the nodes are faulty – and that includes nodes with malicious behavior; see Section 5.2 The Lachesis Consensus Algorithm. The Brace blockchain is EVM compatible, supporting Solidity (and Vyper) to compile smart contract bytecode.

00004512 // 99374128 // 1005934



0 77832 12

BRACE
NETWORK

****

TESTNET DETAILS

- Network Name: Brace Network Testnet
- RPC URL: https://testnet.bracenetwork.io
- Chain ID: 489677
- Currency Symbol: BRACE
- Block Explorer URL: https://bracescan.io