Shardbits

The money play address

Introduction

The creation and subsequent release of Satoshi Nakamoto's *"Bitcoin: A Peer-to-Peer Electronic Cash System"* [1] was the world's first major foray into the world of decentralization, cryptography, and peer-to-peer networking. Not only did this new technology allow for an individual to safely and efficiently transfer a store of value across long distances without the need for a centralized institution as an intermediary, it finally allowed for one to become self-reliant in regards to managing their funds. In particular, though, the past few years have seen the value and benefits of these networks finally begun to be realized by the public. Ever since the world took notice of Bitcoin's historic growth in December of 2017, the notion of the blockchain as a technological asset has been on everyone's mind. As a result, the potential for its widespread adoption and usage is highly likely if not guaranteed. If this possibility comes to fruition, is highly likely that a large number of centralized institutions will be affected--even casinos. It is our goal with ShardBits to spearhead this decentralized revolution and put the power back in the hands of the individual.

A "blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value" [2]. The definition of such explicitly refers to a decentralized yet eminently trustworthy database organized using a chain of blocks ordered by time. Each block contains a number of transactions, the first of which is called the "coinbase" transaction, and manages the miner's reward for adding the block to the end of the current chain. In order for a miner to accomplish this, they must utilize their computing resources to compute the block hash, which in itself contains a reference to the previous block's hash. As a result, these blocks, when combined, help to form a chain of verifiable blocks that cannot be altered without reworking previous blocks added to the chain. Any attacks on the integrity of the chain thusly require a large amount of computing power, helping to act as a barrier against malicious individuals.

The ShardBit project was created to facilitate the further development of the ShardBits cryptocurrency and the ShardBet platform as a whole. Although each individual piece of the ShardBit ecosystem works in sync with the rest, both the currency and the platform are inherently separate modules. The currency in itself is solely meant to be used as a medium of payment for the platform, and supplies the main bankroll for each DApp created, which in turn gives the currency a use case.

ShardBits

The ShardBits cryptocurrency consists of several individual components that help to supply the underlying blockchain with its functionality. Each of these foundational elements are explained in depth below.

Specifications

The following outlines the major specifications of the ShardBits cryptocurrency and the individual properties of the blockchain that it's based upon.

Specification Category	**Specification**
Algorithm	C11
Type	PoW/PoS/Masternodes
Coin Name	ShardBits
Coin Ticker	SHDB
Coin Supply	2,240,300,000 SHDB
Block Time	90 Seconds
TX Confirmations	10 Confirmations
Time Drift	30 Seconds
Stake Maturity	24 Hours
Masternode Maturity	1000 Confirmations

Premine

Developing the coin, we realized that we'd require a substantial premine (400,000,000 SHDB or 17.8%) to fund the bankroll of our initial DApps and in particular support future growth and development as necessary. Regarding the bankroll, we plan to set aside the majority of the coins taken for this purpose, to not be touched by the team throughout. Any coins not sold in the presale will be added to the bankroll. The overall breakdown of the premine's projected use is as follows:

- 200,000,000 SHDB (50%) - Platform/DApp Bankroll
- 50,000,000 SHDB (12.5%) - Presale Distribution
- 80,000,000 SHDB (20%) - Marketing/Development Costs
- 50,000,000 SHDB (12.5%) - Developer/Founder Payments
- 20,000,000 SHDB (5%) - Bounty Program

Software

Each individual piece of software connected to ShardBits is absolutely essential to the functionality and efficiency of the network. The two main components that make up the base of the network--the daemon and GUI wallet--are the subject of ongoing development and will continually be improved upon as ShardBits and the project as a whole continues to mature throughout.

Any client that is communicating with the ShardBits network operates through a daemon process running locally on an individual's machine or server. This process will seek out other instances of itself, exchanging data throughout in the form of individual transactions and blocks, and are primarily responsible for managing and shaping the blockchain. Interacting manually with this daemon process is a simple process, and can be done through either the command line of the server that the daemon is running on or through the GUI wallet console.

Command	**Context**
./shardbetdd help	Command Line
help	Wallet Console

The GUI wallet is the other piece of integral software that communicates through the network using a daemon process that operates in the background. It is the main user-facing application that allows for the easy manipulation of one's private keys and assets without using the command line. In essence, it's an individual's personal "control panel" through which communicating with the blockchain is trivial. Compiled versions of ShardBet's wallets are currently available for download on GitHub for Linux, Mac, and Windows [3].

Masternodes

A Masternode is simply a full node running continuously that, through a collateral system, is trusted enough to fulfill special functions and tasks on the blockchain. It is always interacting with other nodes and helps to ensure a stable network throughout. Because of this, as well as the fact that they incur some expense and effort to maintain, Masternode operators receive a portion of block rewards. As a result, Masternodes generate a form of "passive income" without requiring specialized mining equipment, making them easily accessible and benefiting the network as a result. The more Masternodes, the more secure and decentralized the network becomes as a whole.

If an individual decides that they want to create a Masternode, they require the following items:

- Masternode collateral
- Dedicated VPS and IP Address to host the wallet 24/7
- Enough storage space and RAM on aforementioned VPS to manage the daemon/blockchain

The Masternode collateral in particular is absolutely necessary to ensure that the individual doesn't cheat the system, as it requires them to have something at stake at all times. If an individual tries to promote or engage in malicious activity, their node will be rejected by the rest of the network.

ShardBits Collateral:

- < Block #30,000 : 500,000 SHDB
- > Block #30,000 : 100,000 SHDB

We decided to increase the collateral by a factor of 5x before block #30,000 simply to further reward our initial supporters and decrease the number of Masternodes on the network before block #30,000.

Block Rewards

Starting Block #	**PoW Rewards**	**PoS Rewards**	**MN Rewards**
Block #2	125 SHDB	125 SHDB	375 SHDB
Block #1001	2000 SHDB	2000 SHDB	6000 SHDB
Block #10001	1000 SHDB	1000 SHDB	3000 SHDB
Block #100001	500 SHDB	500 SHDB	1500 SHDB
Block #1000001	250 SHDB	250 SHDB	750 SHDB
Block #1500001	125 SHDB	125 SHDB	375 SHDB
+ 500,000 Blocks	Halving	Halving	Halving

Masternode Return on Investment

Starting Block #	10 MNs	100 MNs	500 MNs	> 1000 MNs
Block #2	2,628%	262.8%	52.56%	< 26.28%
Block #1001	42,048%	4,204.8%	840.96%	< 420.48%
Block #10001	21,024%	2,102.4%	420.48%	< 210.24%
Block #100001	10,512%	1,051.2%	210.24%	< 105.12%
Block #1000001	5,256%	525.6%	105.12%	< 52.56%
Block #1500001	2,628%	262.8%	52.56%	< 26.28%
+ 500,000 Blocks	Halving	Halving	Halving	Halving

ShardBet

Shardbet plans to be one of the first online casinos to implement and accept cryptocurrencies as a method of currency, and the first to repurpose masternodes as a method to earn dividends, to be paid out monthly. Shardbet in particular is affiliated with the ShardBits cryptocurrency, which will be used within the platform. We do plan to allow BTC and ETH deposits in the future, to ensure that everyone that wants to join will be able, but these will be swapped for ShardBits to ensure the liquidity and the game mechanism.

Expansion

We plan to add quite a lot of games in the future, each with a standard similar to ShardCrash, which will launch with ShardBits, illustrated with fast-pace games, bets, and easy user-interaction. On top of our own development, we plan to offer jobs, bounties, and the like for people that want to develop their own minigames that fulfill these requirements. We will go and enable these games in our website, and give a fair percentage of the overall house profit to the creator of this game. This will lead to further development and ensure a high quality of work, as well as ensuring a large turnover in the games presented that may end up being permanent or events.

Some advantages of this strategy in the long-term include:

- Quality development as the creator is remunerated if a lot of players jump in this game.
- Outsourcing is incentivized, allowing the core team to focus on other developments.
- Quick and easy turnover of games if a decent number are created
- No need to fund for game development in the long-term as outsourcing is paid with returns on games created.

Masternode Integration

Masternodes will play a huge role in the website and the ShardBit ecosystem as a whole. Not only will they fulfill their customary purpose of securing the network and rewarding whoever runs one with coins, they'll entitle the holder to earn a percentage of the house profit, to be paid out monthly.

ShardCrash

ShardCrash will be the first game implemented in the ShardBit ecosystem, and the main use case for ShardBits initially. The functionality of such was originally designed for Bustabit, a Bitcoin casino, but was repurposed by the core team to accept and work with ShardBits instead. The game is simple:

1. Place a bet before the round begins
2. A counter will start ticking, counting up from 0.00x
3. "Cash out" before the counter "busts."
   a. If you succeed, you earn the multiplier you "cashed out" on
   b. If you fail, you lose your initial bet

The house margin is scaled between 0 and 1%, depending on how long you hold, and is hardcoded into the game. We do not have a fixed house margin, as this would prevent highly conservative play (e.g. If you were only attempting to make $2 in a $100 game, a house margin of 1 % would be 50 % of your potential profits). Our unique formula makes it fair for both highly conservative play (cash out early) and highly aggressive play (hold until you're a millionaire). All games will be fair under our "provably fair" methodology.

Exact Formula for the House's Expected Return:

- 1 % * (intendedCashOut - roomAmount) * (roomAmount / intendedCashOut)

The other important thing to keep in mind is that every game has a 1 % chance of instantly busting. Overall, though, the code that decides the multiplier for each round is simple. It basically does four things :

1. It mixes the has with the clientSeed (decided by the provably fair seeding event) using hmac-sha256
2. It gives a 1/101 chance of instantly busting
3. It works out what the multiplier would be if there was no house edge
4. It takes 1% off the multiplier and adds on 0.01x

Essentially, half the time (other than 0x bust) the multiplier will be 1.99x or more. That means if we bet 1.99x we have a 50% chance of winning (again, ignoring 0x busts).

Exact Formula/Value for House Edge:

- 100 - (1.99 * 50) = 100 - 99.5 = 0.5%

The extra 0.01 that gets added on to the multiplier is half of the 1% that was taken off in this case, leaving the house edge at 0.5%. As the multiplier gets bigger, the 1% that is taken off gets bigger, and the 0.01x that gets added on becomes less and less significant, causing the house edge to tend to 1%

Conclusion

This whitepaper helps to outline the ShardBit ecosystem and corresponding cryptocurrency, including the ShardBet module and ShardCrash, as well as our overall vision of a revolutionary casino platform that leverages the advantages and features of blockchain technology. The use of Masternodes in particular to strengthen the network while earning dividends from platform profit will be a feature that helps to set us apart and incentivizes individuals to hold coins throughout, providing a necessary use case for the coin.