B2:
Antimatter
BSC Application Sidechain

V0.1

15 June 2022

Table of Contents

Abstract

Antimatter is originally an innovative lightweight on-chain and cross-chain DeFi perpetual options protocol based on a polarized token mechanism. Antimatter ecosystem currently includes at least five main products now, Dual Investment, Sharkfin, Bull & Bear Tokens, Financial NFTs, as well as Antimatter DAO. This ecosystem will grow up with newly deployed decentralized finance applications. To run any of these Dapps with low-cost transaction fees and high-speed throughput, we propose to create a blockchain ecosystem (B2) with a BNB sidechain based on the BAS framework. Although the security of B2 will be rely on the B2 validators and their deposit, once B2 is approved by BNB sidechain, B2 will also be secured under the umbrella of BNB chain. In this proposal, we aim to solve network scalability problems by having a higher output of transactions as well as lower gas fees. B2 is built to facilitate the financial blockchain infrastructure of the Antimatter ecosystem. The validator nodes are run by community stakeholders, bringing more flexibility and decentralization to B2. Unlike BNB Chain, the gas currency is $MATTER, and the maximum total supply of it is fixed and there is no inflation in the token economy. Antimatter B2 will be the application chain for structured products and the data collection chain for market makers such as Babel Finance and TDX.

Keywords:

Antimatter; B2, Decentralized Blockchain; Low Fee; Staking; Governance.

1. Scaling and Reducing the Transaction Fees of Antimatter Products

When AntiMatter was founded in early 2021, our primary goal was to build innovative models to revolutionize derivatives in decentralized finance. Inspired by Uniswap and other similar DeFi apps, AntiMatter abandoned the traditional order book and oracle-based model and embarked on the adventure of exploring the ways to revolutionize the derivatives market. The Black-Schole model did the same for traditional derivatives, and now we are focusing on DeFi. Hence AntiMatter can be described as the realization of hub for decentralized on-chain financial products such as derivatives and financial nonfungible tokens (NFTs). One of our first innovations is the non-oracle based perpetual options. Being community driven, innovative and simple forms are the core of AntiMatter. An option contract is an agreement that gives a trader the permission to buy or sell an asset at an estimated price on a predetermined date. Although similar to futures contracts, traders who buy options contracts do not need to close their positions. Options contracts are derivatives that can be based on a wide variety of underlying assets, including stocks and cryptocurrencies. These contracts can also be obtained from financial indices. As a rule, options contracts are used to hedge current positions and for speculative trading. In some situations, options and derivatives can be highly complex financial products, which can be difficult to understand and have high barriers to entry. These kinds of products often get overlooked by many users. Moreover, achieving those options and derivatives on the smart contracts also require a lot of gas consumption. Hence, the goal of this technical whitepaper is to revisit these challenges and present a scalable solution to this bottleneck.

As Antimatter Labs, we have also been developing several options and derivative products. In these products, our vision is to introduce simplified derivatives products to serve many users more conveniently in a scalable manner. We aim to provide a good UI/UX Design to reach a wider audience and open new doors for our extensive **Antimatter Ecosystem**. However, we all know that accessibility is a key to a blockchain system. Hence, our goal is to have a universal efficient and low-cost DeFi derivatives worldwide. We believe that we are all still in the early stages of the Crypto & DeFi space and it goes without saying that we believe that this industry is going to stay here.

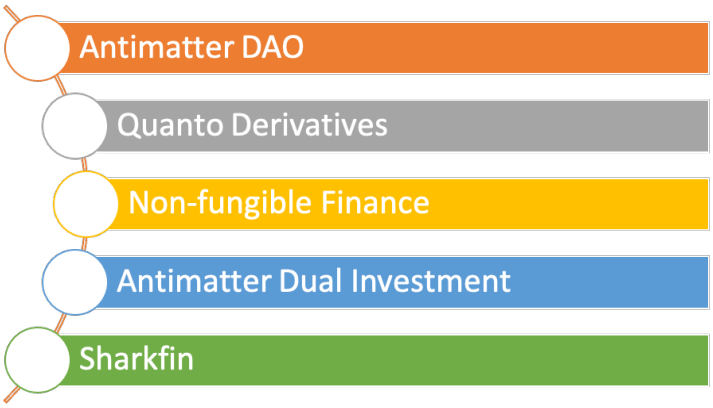

Figure 1: Antimatter Ecosystem

Running options and derivatives on standalone chains such as ETH, BSC, and Polygon requires huge amount of gas and this may yield large fee for a single transaction. Furthermore, the throughput is also another requirement for the derivatives as there are quite a lot of transactions need to processed in a very short time. Motivated by these needs, we aim to create a cheap, fast, and transparent sidechain (what we called *B2*) in BSC ecosystem where many Antimatter application products can be deployed and executed. In order to do that, we aim to use the BAS framework for creating B2 Sidechain in the BSC ecosystem. This gives the opportunity to maintain a close connection with BNB Chain (BSC) and execute all functions of Antimatter products meeting all those afore-mentioned requirements. Note that due to the BAS usage, the following implemented ready modules will only be customized according to our configurations:

- Parlia consensus engine
- Staking pools
- Governance
- Dynamic runtime upgrades
- Reward management
- Manageable blockchain params
- EVM hooks
- Deployment proxy

This modular architecture allows us to re-use or enable/disable different modules. Of course, these modules are going to be runtime-upgradable by on-chain decentralized transparent governance for reliability purposes.

2. Token Economy of B2 Sidechain

- The native token of B2 is going to be wMatter and it will be pegged (1:1) by the Matter tokens from the other chains (e.g., Ethereum, BSC).
- Currently, BAS supports Celer bridge which will also be used by Antimatter Labs.
- Since B2 will have already a cross-chain bridge, wMatter token will be minted/burned through the bridge.
- wMatter will be used as a transaction fee.
- A small amount of wMatter (e.g., 1000 wMatter) will be minted in the genesis to be used during the system setup.
- Additionally, 10M reserved Matter tokens live on other chains will be bridged to B2 and the correspondingly 10M wMatter will be minted on B2 to be used for the system reward.
- Each block producer/validator will get transaction fees along with 0.1wMatter as a reward for each block.
- There will be neither inflation nor deflation in the token economy system.
- Since the time for producing a block is approximately 3 seconds, 28800 blocks can be produced per day. Hence, 10M wMatter, can be distributed to the validators for at least 9.5 years. After approximately 9.5 years, only transaction fees in the block would be distributed to the block producers.

3. Background

In B2 Sidechain, all transactions are being signed by the ECDSA signature algorithm which is described in following subsection. The raw transaction is first digested by the hash function (Keccak), and then the hash value is signed by the sender's private key through ECDSA. The current version of Parlia consensus does not provide fast finality because one validator produces a block, and to make sure of the correctness of these operations, one has to wait for the long confirmation time, usually it is $\frac{2}{3} * N + 1$ where N denotes the active validators. Aggregated signature mechanism with Parlia's fast-finality can solve this problem because one can collect and convert many signatures into one aggregated signature and send only this aggregated signature to the chain. For the aggregated signature, some special elliptic curves such as BLS12381 or BN256 will be used.

3.1. Cryptographic Hash functions

A cryptographic hash function $H: \{0,1\}^* \rightarrow \{0,1\}^k$ takes an arbitrary-length message and outputs a fixed-length output. A hash function has the following basic properties:

- **Deterministic:** Given m, we always have $x = H(m)$ (the same input m always results in the same output x).
- **Efficient:** it is very fast to compute the hash value for any given message.
- **Pre-image resistance (one-wayness):** For essentially all pre-specified outputs, it is computationally infeasible to find any input which hashed to that output.
- **Second pre-image resistance** It is computationally infeasible to find a second message that produces the same hash value.
- **Collision resistant:** It is also hard to find two arbitrary inputs x and y that hash to the same value, i.e., $H(x) = H(y)$.

3.2. Digital Signatures: ECDSA Signing Algorithm

Let's assume that n is order point, P and Q are two points on an elliptic curve, and G is a base point. The ECDSA signature algorithm can be described as follows:

Key generation:

1. Select a random number d in the interval $[1, n-1]$.
2. Compute $Q = dG$
3. Public key is Q, private key is d.

Signature generation:

1. Select a random integer k, $1 \leq k \leq n$.
2. Compute $kG = (x_1, y_1)$ and convert x_1 to an integer $\hat{x}_1$.
3. Compute $r = x_1 \, mod \, n$. If $r = 0$ then go to step 1.
4. Compute $k^{-1} \, mod \, n$.
5. Compute $Hash(m)$ and convert this bit string to an integer e.
6. Compute $s = k^{-1}(e + dr) \, mod \, n$. If $s = 0$ then go to step 1.
7. Signature for the message m is (r, s).

Signature verification:

1. Verify that r and s are integers in the interval $[1, n-1]$.
2. Compute $Hash(m)$ and convert this bit string to an integer e.

3. Compute $w = s^{-1} \, mod \, n$.
4. Compute $u_1 = ew \, mod \, n$ and $u_2 = rw \, mod \, n$.
5. Compute $X = u_1 G + u_2 Q$. 6 If $X = \theta$ then reject the signature. Otherwise, convert the x-coordinate x_1 of X to an integer $\hat{x}_1$, and compute $v = \hat{x}_1 \, mod \, n$.

3.3. Aggregated Signatures

3.3.1. BLS 12381

BLS (Boneh, Lynn, Shacham) is another digital signature introduced in 2001 and has an aggregated structure. Let $e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$ be a pairing where $\mathbb{G}_1$, $\mathbb{G}_2$ are additive groups and $\mathbb{G}_3$ is a multiplicative group. Also, let G_1, G_2, and G_3 are base elements of $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_3$ respectively.

Public and Private Key Pair $(\boldsymbol{pk}, \boldsymbol{sk})$:

- The private key sk to be used for signing is just a randomly chosen number between $[1, r-1]$.
- The corresponding public key is $pk = [sk]G_1$.

Signing:

- To sign a message m we first need to map m onto a point in group $\mathbb{G}_2$. Let's assume this mapping results in a $\mathbb{G}_2$ point $H(m)$.
- We sign the message by calculating the signature $\sigma = skH(m)$.

Verification:

Given a message m, a signature σ, and a public key pk, we want to verify that it was signed with the sk.

- The signature is valid if, and only if, $e(G_1, \sigma) = e(pk, H(m))$.

Aggregation

One of the most important properties of BLS signatures is that they can be aggregated

- To aggregate signatures, we just must add up the $\mathbb{G}_2$ points they correspond to: $\sigma_{aggregated} = \sigma_1 + \sigma_2 + \ldots + \sigma\_n$.
- We also aggregate the corresponding G_1 public key point

$pk_{aggragated}$ = pk_1 + pk_2 + … + pk_n.

- Verify that $e(G_1, \sigma_{aggregated}) = e(pk_{aggregated}, H(m))$ to verify all the signatures together with just two pairings.

3.3.2. BN256 Curves

BN256 is basically the size of the prime number of the underlying field in $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$. In a BN256 curve, $\mathbb{G}_2$is basically $E(GF(p))$, $\mathbb{G}_2$ is a subgroup of $E(GF(p^{12}))$, and $\mathbb{G}_3$ is a subgroup of $GF(p^{12})$. Elements of $\mathbb{G}_1$requires the same number of bits as p for each elliptic curve point. We would like to highlight that not all prime-friendly curves support cofactor 1. This means that we may need a larger prime for a particular group order in some cases. Elements of $\mathbb{G}_2$ require the same as pk for each elliptic curve point coordinate, where k is the embedding degree of the curve. When using twisted curves, we can reduce this by 2, 3, 4, or 6 depending on the curve. BN curves have embedding degree 12 and support twists, therefore we can use elements with the same size as $p^{12/6} = p^2$.

4. Antimatter B2 Chain Architecture

BAS framework has already been providing development-ready EVM-compatible features like staking, RPC-API, and smart contracts. Also, BSC does not rely on the BAS security model and there is no default embedded production-ready bridge solution between the BSC and BAS networks. Therefore, to achieve a bridge between B2 and BSC, we aim to use either AnySwap or Celer Network Bridge (cBridge).

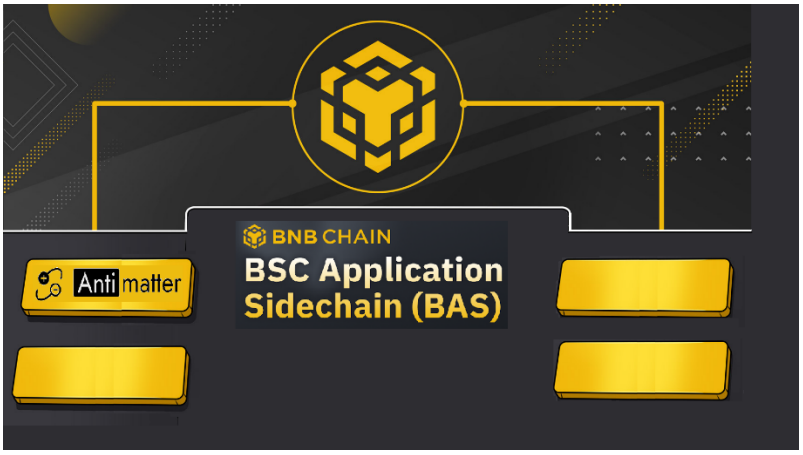

Figure 1: Antimatter on BSC Application Side Chain

Later, once the native bridge between B2 and BSC is ready, we also aim to support the native bridge mechanism. B2 will be built with the BAS template (which was already developed by Ankr) with B2's configurations.

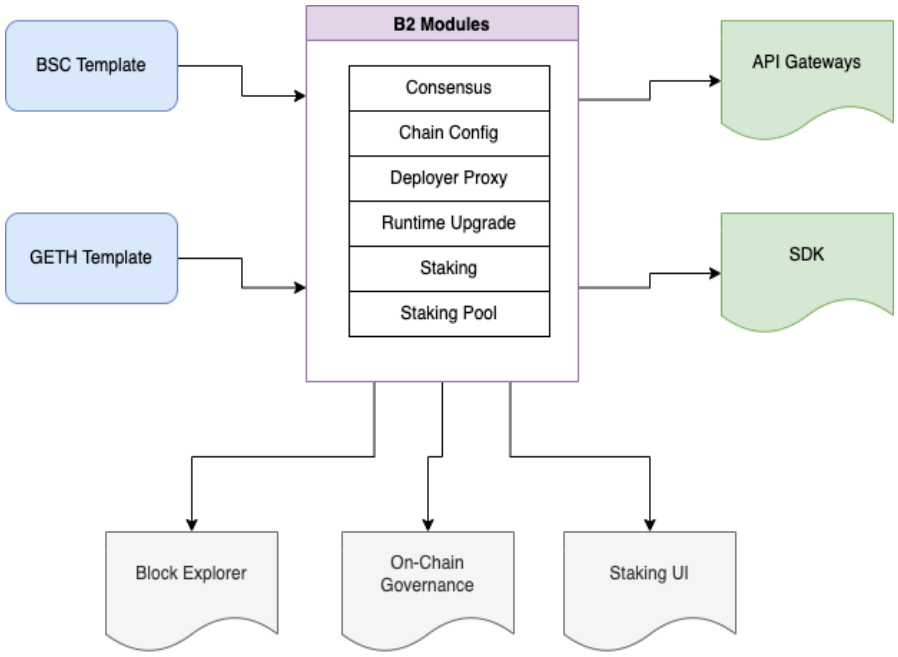

Figure 3: B2 Modules (Borrowed from BAS modules)

4.1. System Contracts

B2 sidechain has an EVM execution environment with a predefined set of system smart contracts for the platform operation. Predefined system smart contracts are defined as follows:

- **Staking Contract**: Used for managing validator delegations and active validator sets.
- **Slashing Indicator Contract**: Used for slashing not active validators.
- **System Reward Contract**: Is a treasury for the system rewards to cover relay fees and others.

B2 also has the following upgradable contracts (which can be improved later if required):

- **Staking Pool:** Provides cheaper access to the staking contract.
- **Governance:** A default on-chain implementation by Compound's Alpha governance.
- **Chain Configuration:** Used for the consensus that is managed by on-chain governance.
- **Runtime Upgrade:** Allows upgrading system contract runtime.
- **Deployer Proxy:** Used for managing deployers of the smart contracts.

Using the Parlia consensus mechanism encourages users to deposit their funds and vote for honest validators, and this will make the B2 sidechain more decentralized and reliable. It also helps share-holders get rewarded from their stakes by earning commissions from block producers. From a technical point of view, the B2 sidechain involves staking smart contracts on Solidity for the EVM runtime. This smart contract is an extension of IValidatorSet and allows users to manage active validators based on the total delegated amount and distribute rewards among stakeholders.

4.2. On-Chain Governance

B2 also has an online governance, hence the community users will be able to vote on a new proposal on the chain. Management will be based on the Compound's Alpha Governance, and the validator holders in the chain can create and vote on new proposals. Voting rights are allocated based on the total amount transferred to the verifier. Once a 2/3 majority and >51% vote is reached for a proposal, the proposal can be executed by anyone in the chain. The community can manage rate parameters such as felony threshold or jail time.

4.3. On-Chain Staking

B2 sidechain provides an on-chain staking system and uses the PoSA (Proof-of-Stake-of-Authority) staking model. It allows users to delegate their tokens to the specific validator and share the validator's rewards based on the total staked amount. B2 has the following staking roles:

- **Validator**: A node that produces new blocks and validates existing blocks.
- **Delegator**: A user who participates in validator election.

A validator is a node that runs the validator node software, in a special validator mode. This mode allows the node to connect to boot nodes and produce new blocks. Once a block is produced by a validator, it propagates it through the network to other validators using boot nodes. Other validators must verify and add this block to the chain. Unfortunately, the Parlia consensus engine does not support fast finality today, but still this feature is under development. That's why to prove the correctness of the produced block, the user must verify $\frac{2}{3} * N + 1$ blocks. To become a validator, the user has to satisfy the following requirements:

- Have their own, fully synchronized, node running in the full-sync mode, with an unlocked validator private key.
- For registration, the user must specify the validator's address and commission rate.
- Request from one of the existing validator to propose the user become a validator.
- Wait until 2/3 of the validators support the candidate.

Staking pool contract allows the chain to use a different staking model. Namely, instead of delegating tokens to a validator, the user buys a share of the pool, and validator rewards are distributed between delegators based on their share. Since all the users use the same pool, the cost of reward-claiming transactions on average is shared by all the delegators in the pool.

4.4. Slashing

- If a validator does not produce blocks, it will be slashed and its missing block counter increased by one.
- If a validator misses a block, another validator can slash them. They will not receive rewards for the missed block.
- If a validator misses blocks for misdemeanor threshold times, then this validator lose the reward for the entire epoch. The default value of misdemeanor threshold is 50.
- If a validator misses blocks for felony threshold times, then this validator goes to jail and will not be able to produce rewards for the jail period (usually around 1 week). The default value of the felony threshold is 150.

Hence, a jailed validator loses either all their rewards for 1 week or 25% of monthly rewards. Once the jail epoch period has ended for a jailed validator and they have been released from jail, they can re-start to produce new blocks. Releasing from jail is a very important mechanism to eliminate problems with corrupted or underperforming validators that do not produce new blocks at all. In essence, it is just a confirmation from the validator's owner that the validator has recovered and is ready to continue working.

4.5. Blocks & Epochs

Whenever a delegator votes for a validator, they immediately contribute to the modification of the total delegated amount. Effectively, they also modify the share distribution between all delegators. It makes share computation very complicated and requires dynamic re-calculation of the shares for each reward distribution. This may make the entire rewards distribution process very expensive. Since we are running the staking and reward distribution models fully on-chain, we aim to realize all the computations to be optimized in smart contracts. To reach this goal, we split the staking process into epochs so that gas consumption can be reduced significantly.

- An epoch is an interval with N blocks inside.
- An epoch length can be equal to just one block. However, it can significantly increase storage size and bring no benefit.

- The average time for a block producing is 3 seconds, and 28800 (=24*60*60/3) blocks are expected to be daily produced.

B2 Sidechain will use the epoch size of 1 day. 1-day epoch allows spending only 1.7 million gas units a year per single user. Since the block size is around 80 million gas units, a delegator has ~40-50 years to claim their rewards before those can become unclaimable.

4.6. Reward Distribution

A validator can get rewards by executing transactions. Each transaction has an execution cost and $\frac{15}{16}$ of this cost goes to the validator, but $\frac{1}{16}$ of the reward goes to the system treasury that can use these funds for the system needs, such as bridging cost coverage and relaying. Not all block rewards go to the validator's owner. A share of them is also distributed between delegators.

Whenever the validator's owner creates a new validator, the commission rate must be specified. The commission rate defines what percentage of the block reward goes to the validator owner. It is limited to 0% up to 30% to limit validators from setting very high commission rates.

On the other hand, delegators' rewards are also calculated based on their total staked amount at the validator. The reward is calculated per one validator. The total rewards for a delegator, if staked at different validators, is the sum or per-validator rewards.

5. DApps in Antimatter Ecosystem

5.1. Non-fungible Finance

Nonfungible.finance a DApp (currently live on BSC, ETH, FTM, and AVAX) exploring the possibilities for NFTs as financial vehicles. Users can create Spot Index, Future Index (in development), and Lockers in a permissionless way. Creation is very simple and straightforward, just select underlying assets + asset amount and confirm. Minted Spot Index NFTs can be traded with their value corresponding to the underlying assets. Lockers can be utilized to lock-up assets for a set period or simply as gifts to friends and family. We implemented an Account System enabling users to name themselves and display the name

as the creator of their NFTs. Non-fungible Finance is not only used by individuals but also by projects like Umbrella Network, Bounce Finance, and Clover Finance.

5.2. Antimatter DAO Hub

Antimatter DAO is a club for derivatives fanatics and a collaborative workplace for innovative on-chain derivatives applications, with features including on-chain governance, multi-party treasury management, academic resources sharing, and new model experiments. Antimatter On-chain Governance Policies:

- **Voting period:** All proposals are subject to 3 to 7 days voting period. The period is set by the proposer.
- **Making a proposal:** To make a proposal, proposers need to fill out the unchain governance form with details. All content will be recorded on the blockchain and is publicly viewable.
- **Proposal creation:** To create a proposal, you need to stake 100,000 MATTER tokens into the proposal pool. The staking period is equal to the voting time period for your proposal. For example, if you create a proposal with a voting period of 3 days, your staking will be 3 days and claimable after the close of voting.
- **Proposal Creation Fee:** There is a fixed proposal fee of 100 MATTER per proposal. The fee will be deducted from the 100,000 MATTER staked when unstaked.
- **Vote for a proposal:** Each proposal has two sides: Support vs. Against. To vote for either side, voters need to stake MATTER tokens into the supported pool. The staking period is required to meet the staking period of the proposal. Once staked, you cannot unstake or change sides during the voting period, it is however possible to add more tokens to the voting stake. If you stake multiple times, the staking period will be counted from your last staking.

5.3. BNB Quanto Derivatives

An option is a contract giving the buyer the right, but not the obligation, to buy (in the case of a call option contract) or sell (in the case of a put option contract) the underlying asset **at a specific price on or before a certain date**. Traders can use on-chain options for speculation

or hedge their positions. Options are known as **derivatives** because they derive their value from an underlying asset.

Options derivatives are highly complex financial products, which are difficult to use and have high barriers to entry. Options derivatives often deter many users. Therefore, we are introducing simplified derivatives products to serve users more conveniently. Meanwhile, Antimatter is facing a real challenge of a plain product structure and the lack of real users. Hence, we plan to develop more accessible products based on the original derivatives ecosystem to find new growth room.

An on-chain decentralized perpetual contract in which the underlying is denominated in BNB, but the instrument itself is settled in other cryptos. Essentially, a quanto has an embedded currency forward with a variable notional amount.

5.4. Antimatter Dual Investment

One of the first Structured Products we offer is Dual Investment. A decentralized alternative to Dual Invest on Binance. Antimatter Dual Investment is a non-principal protected yield generating product based on a decentralized protocol. The product has a “market-neutral, returns guaranteed” feature, where the yield is clear and fixed at the time of purchase, while the settlement currency is uncertain. At maturity, the settlement currency depends on the outcome of the settlement price at maturity compared to the strike price. This has the following business advantages:

1. First-mover advantage of “DeFi+Dual Investment”.
2. Easy and straightforward to operate.
3. Stable & higher yields.
4. Returns are guaranteed regardless of how the market goes (within a range of volatility).

5.5. Antimatter Sharkfin

A principal-protected product, where users subscribe using the required currency and earn varying yields based on a specified price range of the underlying asset. The product runs on

a weekly basis and redemption is only possible at maturity. Namely, sharkfin product has two parameters that change every week: Price range and APR range. They are adjusted to provide an attractive APR, but also low risk. In simpler words: you deposit a currency and earn yield on it, if the asset stays in a price range you get more %APR. If it doesn't, you get less %APR.

Sharkfin options are already an established structured product on various underlying assets. Antimatter is determined to bring traditional derivatives on-chain, while simultaneously innovating the space. Antimatter Sharkfin is the decentralized version of the traditional sharkfin product and will be starting out with $BTC as first underlying asset. Users are provided with attractive APR rates, while keeping a low risk profile and keeping their principal protected.

References

1. Antimatter: Enhanced Yield with Structured Products, https://antimatter.finance/, May 2022
2. Ankr Helps Bring First Game to BAS, https://coinmarketcap.com/gravity/articles/27669, May 2022
3. Ankr, Celer, and NodeReal Launch BAS Testnet, a BNB Chain Sidechain Framework, https://www.bnbchain.world/ru/blog/ankr-celer-and-nodereal-launch-bas-testnet-a-bnb-chain-sidechain-framework/, May 2022
4. BEP-100: BSC Application Sidechain, https://github.com/bnb-chain/BEPs/pull/132, May 2022
5. Ankr and Others Launch BAS Testnet, a BNB Chain Sidechain Framework, https://www.bsc.news/post/ankr-and-others-launch-bas-testnet-a-bnb-chain-sidechain-framework, May 2022.
6. National Institute of Standards and Technology, FIPS PUB 186-4: Digital signa- ture standard, 2013.
7. Ethereum Virtual Machine. https://ethereum.org/en/developers/docs/evm/, May 2022
8. National Institute of Standards and Technology (NIST). (2002) “Secure Hash Standard”. FIPS Publication 180-2,
9. Don Johnson, Alfred Menezes, and Scott Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). International Journal of Information Security, 1(1):36-63, August 2001.
10. Dan Boneh, Sergey Gorbunov, Hoeteck Wee, and Zhenfei Zhang. BLS Signature Scheme. (draft-boneh-bls-signature-00), February 2019.