DEVIANT

DEV

Deviant Coin, Innovative Anonymity

A PoS/Masternode cryptocurrency developed with
POS proof of stake.

CONTENTS

03

OVERVIEW

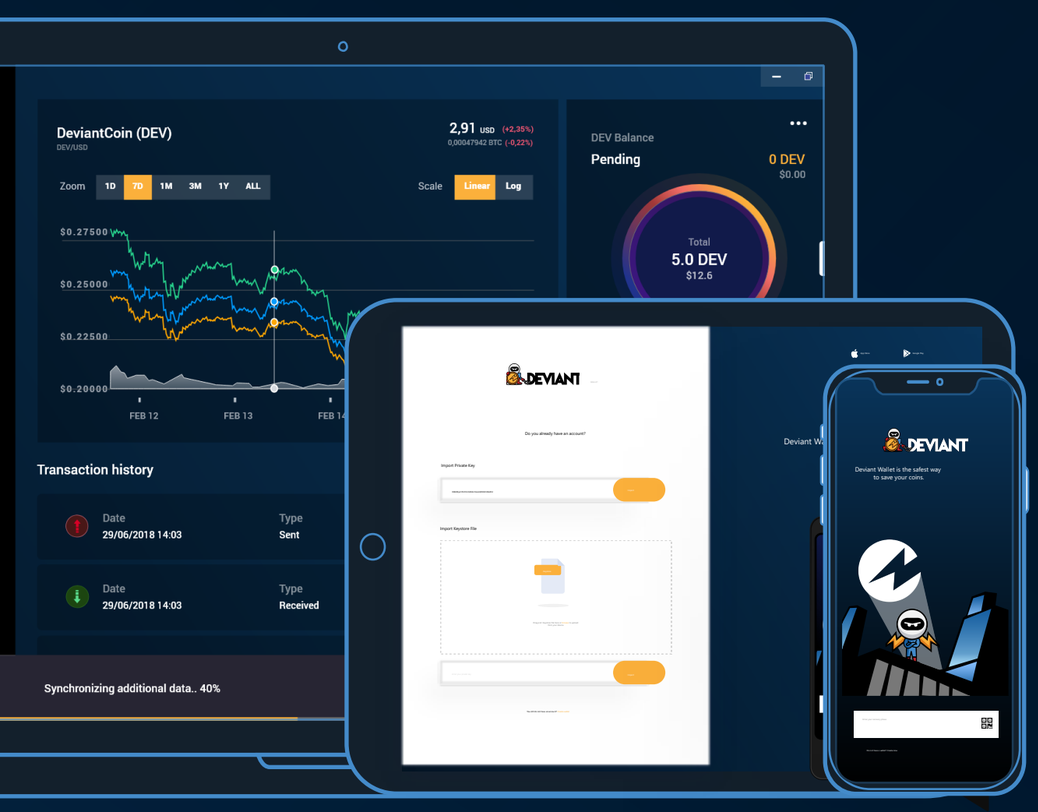
DeviantCoin (“DEV”) is a proof-of-stake blockchain offering privacy by leveraging masternodes built on the Zerocoin protocol.

DEV is a fork of PIVX, and DEV’s masternodes provide many benefits, including: secure transactions, encrypted messaging, stealth addresses for complete anonymity, low numbers of confirmations, and low fees.

The developers of DEV have aimed to provide the safest and most accessible infrastructure for coin usage. Since masternodes are connected constantly to the network and perform certain specified tasks continuously, DEV offers faster, and more private, transactions.

04

The DEV ecosystem will include the following elements:

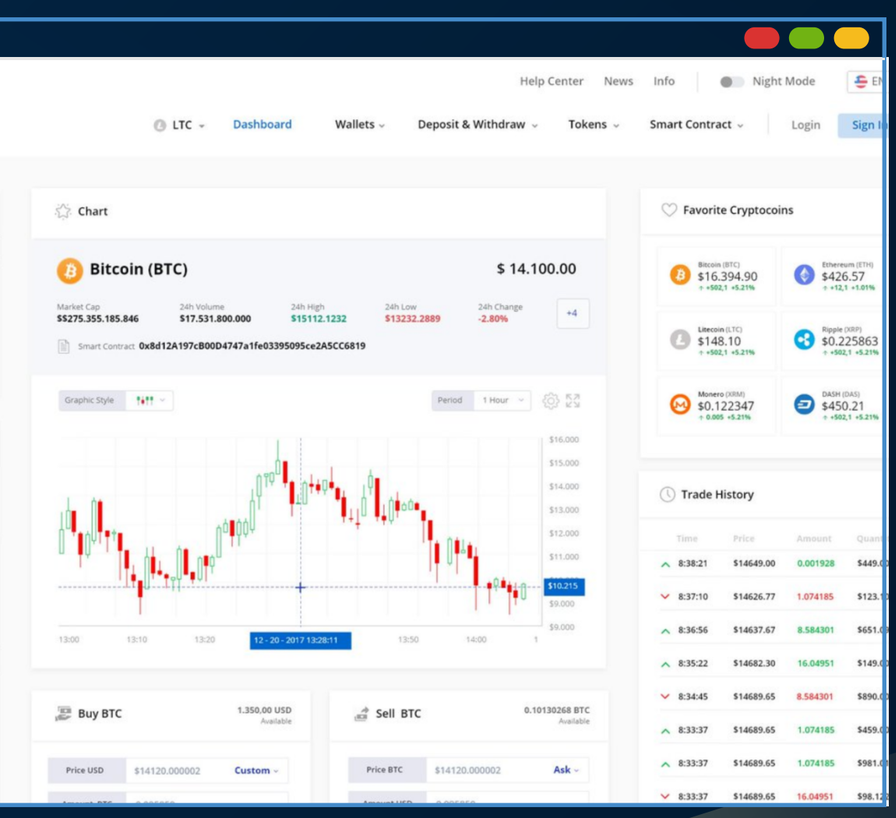


1.

Reliable user wallets on multiple platforms (Win, Ubuntu, Mac, Android, iOS)

2.

3-factor-authenticated secure platform



3.

A hybrid decentralized exchange, “DEVX”

05

DEVX will be a hybrid exchange leveraging Smartcoins on the Bitshares (BTS) blockchain, in order to get to market as soon as possible. DEVX will draw the best elements from both centralized and decentralized exchanges.

The speed, responsiveness, efficiency and user experience of a centralized exchange.

The transparency, security, integrity, accountability and user control of a decentralized exchange.

DEVX will be the first decentralized exchange with three factor authentication (3FA), provided by incorporating an external hardware device as an additional security measure. This hardware device will provide the user with an innovative decentralized hardware wallet supporting multisignature operation between each user and the DEVX protocol.

The hardware wallet will be open source to ensure this essential feature enhancing transaction security can be made available to as many users as possible.

Delivery of the first hardware wallets is planned for Q3 2019.

06

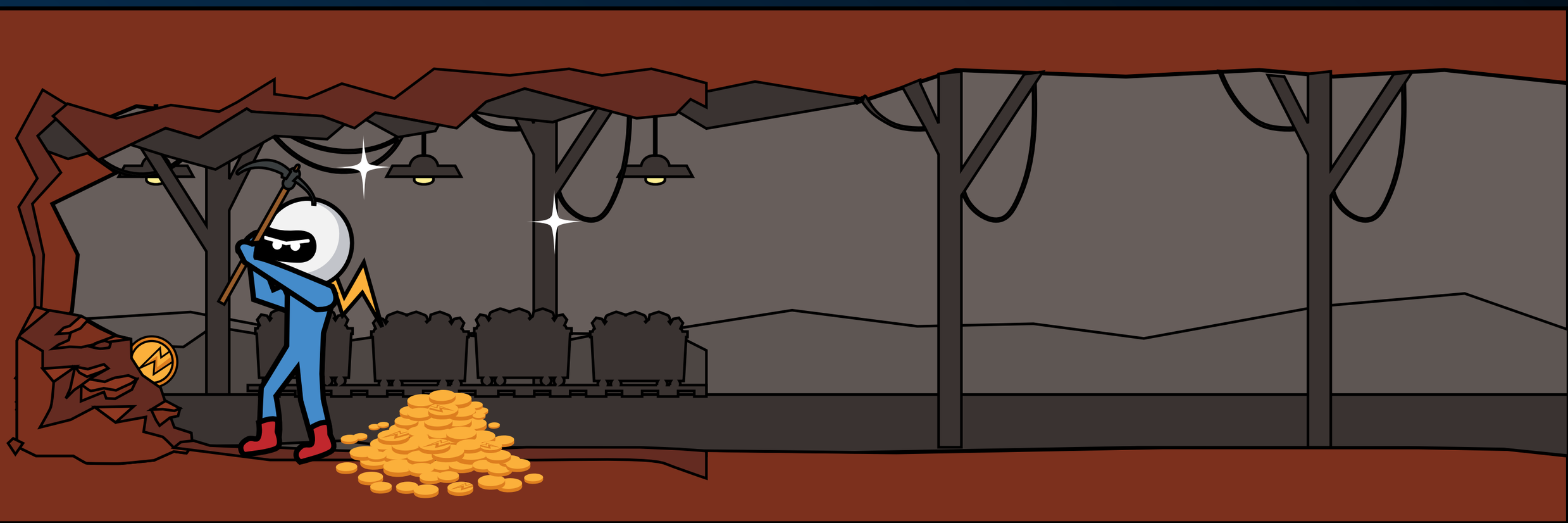
Pre-mine phase

The first 500 blocks were mined using a proof-of-work consensus algorithm, after which the network switched to proof-of-stake. **In the pre-mine phase, 4.3 million DEV coins were mined to fund infrastructure development. To date, 1 million coins have been used to fund: exchange listings, migration to a new codebase offering a more secure consensus algorithm, and development of an Android wallet and payment gateway.**

The pre-mine phase was completed using the Quark algorithm. **Quark is a hash function family which solves the problem of resource-constrained hardware environments.** Quark minimizes area and power consumption, yet offers strong security guarantees. Hash functions have many applications, including: digital signatures, message authentication codes, secure passwords storage, key derivation, and forensic data identification. Any application that uses cryptography is likely to include a hash function.

4.1 Million DEV mined
For infrastructure development

500 blocks mined
Using a PoW algorithm



07

Privacy

Public blockchains are public ledgers where transactions and encumbered transaction outputs are visible to everyone. A major benefit of public blockchains is that the above elements are transparent and verifiable by default. Indeed, this was one of the key value propositions of the earliest, pioneering crypto asset protocols, such as Bitcoin's.

However, full transparency also forces users to accept trade-offs, such as loss of privacy; specific coins become traceable from one address to another, and can lose value if tainted by suspicion if they were used for an illegal or malevolent purpose. Therefore, crypto assets are often less fungible than fiat currency, as it cannot be guaranteed always that a given crypto asset will be exchangeable with every other crypto asset. This consideration of fungibility affects crypto asset valuation; the more a given crypto asset's protocol enhances fungibility, the higher the value of that crypto asset can be. Privacy coins are a thriving branch of crypto assets where many approaches have been developed to address this issue. The Zerocoin protocol, for example, includes the DarkSend feature, which uses conservative and time-tested algorithms (RSA). Masternodes are also used to provide a mixing service for anonymizing transactions.

08

Basic Parameters

Coin Name
Deviant

Ticker
DEV

Coin Type
POW+POS+MN

Hashing Algorithm
Quark

Block Time
60 Sec

Max Supply
88,000,000 DEV

Premined
4,100,000

Min Stake Age
1 hr

Block Size
0.75MB

MasterNode Collateral
5000 DEV

Block Halving
-18%/Year

Last POW
Block 500

First POS Block
Block 501

Coin Maturity
Block 10

Zerocoin Start Height
Block 501

POS Reward
20 DEV, decreasing by 18% every year - up to the 14th year

09

POS (PROOF-OF-STAKE)

The proof-of-stake (“POS”) consensus algorithm provides a public blockchain with a means to reach consensus by relying on nodes incentivized to maintain an economic stake in the network. By comparison, under the alternative proof-of-work (“POW”) consensus algorithm, consensus is reached by nodes called “miners” competing to solve cryptographic puzzles; the miner dedicating the greatest computational resources has the highest chance of producing the next block. In POS systems, the creator of the next block is randomly selected from the list of validators that have staked their coins.

In summary, **POS proceeds as follows: Any wallet holder can stake coins by submitting a special transaction.** This transaction results in coins being “locked up” as a stake, and the stake owner becomes a network “validator”. Periodically, the protocol selects a validator randomly to propose a new block. The whole set of validators then votes on whether it accepts the proposed block, with the weight of each validator’s vote depending on the size of its deposited stake.

10

The benefits of POS compared to POW

POS provides several benefits over POW:

POS block generation requires less power consumption than POW (more power is consumed securing the Bitcoin and Ethereum POW-based blockchains than is consumed in all of Ireland, for example).

Reduced centralization risk (POS can incorporate mechanisms that discourage stakers from forming cartels, e.g. masternodes).

Reduced “51% attack” risk (POS can incorporate various mechanisms to make such attacks much more expensive).

11

MASTERNODES

In POS blockchains, wallet holders can stake their coins to become validators and participate in block creation in return for a reward. The bigger the stake, the higher the chance of a reward.

Unfortunately, there are situations in which “centralisation” of stakers could arise. Wallet holders may form pools to share block rewards, or a single wallet holder may amass and then stake a disproportionately large amount of coins. In such cases, a single pool or entity might gain significant influence over the reaching of consensus in the network, increasing the attack surface. Centralization, therefore, poses a risk to network censorship resistance and security.

12

Masternodes were introduced to address this issue. A masternode is a full node, running on its own server, which must be online and functioning 24/7, and which operates as a validator. To operate as a masternode validator (as opposed to as a non-masternode validator), there is a requirement to stake at least a specified minimum amount of coins. In the case of DeviantCoin, the minimum masternode collateral is 5000 DEV. The intention in requiring masternode operators to hold a minimum amount of coins is to ensure they have a stake in the blockchain and are incentivized to run the node to the benefit of the whole network. As a reward, every block reward is split among all stakers, with 90% distributed to masternodes, and 10% to the remaining non-masternode stakers.

13

Planned reward distribution by block height

Block Height	PoS (%)	MN (%)	Block Rewards	POS Rewards	MN Rewards
501-100001	20	80	20	4	16
100001-225650	10	90	20	2	18
225650 – 751300	10	90	16.4	1.64	14.76
751301 – 1276950	10	90	13.45	1.34	12.1
1276951 – 1802600	10	90	11.03	1.1	9.92
1802601 – 2328250	10	90	9.04	0.9	8,14
2328251 - 2853900	10	90	7.41	0.74	6.67
2853901 - 3379550	10	90	6.08	0.61	5.47
3379551 – 3905200	10	90	4.99	0.5	4.49
3905201 – 4430850	10	90	4.09	0.41	3.68
4430851 – 4956500	10	90	3.35	0.34	3.02
4956501 – 5482150	10	90	2.75	0.27	2.47
5482151 - 6007800	10	90	2.25	0.23	2.03
6007801 - 6533450	10	90	1.85	0.18	1.66
6533450	10	90	1	0.1	0.9

14

In addition to participating in the reaching of network consensus, masternodes provide additional services to the network:

Anonymous transactions via Zerocoin

This feature is intended to increase the fungibility of crypto assets. Fungibility describes the extent to which every coin is exchangeable for any other coin. This property can be ensured only by making every coin untraceable to its previous owners. This is a natural property of physical fiat cash, but not of public blockchains, where every transaction or transaction output is traceable to its origin.

Masternodes provide a “coin mixing” service. They mix transactions between multiple senders, making it very difficult to establish the precise origin of any coin spent in a transaction.

As an example, say a wallet holder wishes to send 100 DEV to another party through the Zerocoin service. In addition, assume that there exist other parties wishing to transact through Zerocoin at the same time. The masternode will gather together all these network transactions into a single pool, smaller parcels that are sent to the payees of the transactions. So, the party receiving the payment will receive say ten separate 10 DEV payments originating from multiple wallet holders instead of a single 100 DEV payment from the wallet holder that initiated the transaction. This concept is based on the Zerocoin protocol described below.

15

Instant transactions via SwiftX

Blockchain transactions are usually considered confirmed after a finite amount of time has elapsed, enough for the transaction to be written into a block and then for several more blocks to be created on top of this block (i.e. at a greater height in the blockchain). Successive confirmations provide an increasing guarantee the transaction will not be tampered with, or its outputs double spent elsewhere. In the case of DEV, each confirmation takes about 60 seconds on average.

Masternodes provide a service of instantly confirmed transactions via SwiftX. Transactions sent through SwiftX are locked on the sender's account and transferred immediately to the other party. This occurs through a mechanism that utilizes amounts deposited in a masternode's stake to guarantee the payment. The list of masternodes appointed at any given time to provide the SwiftX service is determined at random by a protocol algorithm after every block round. This preserves the decentralized manner of transacting in this way.

16

Voting on network governance

Every blockchain network must innovate, implementing changes to the protocol from time to time. Clear, well-defined governance is essential to ensure the network can survive and thrive over the course of these changes, perhaps even outliving its original creators. However, in many public blockchains, governance has been informal, with governance “rules” that are simply community based. Greater formality and clarity in governance can be achieved by hard coding governance rules explicitly into the blockchain code directly. Various models have been devised for doing this.

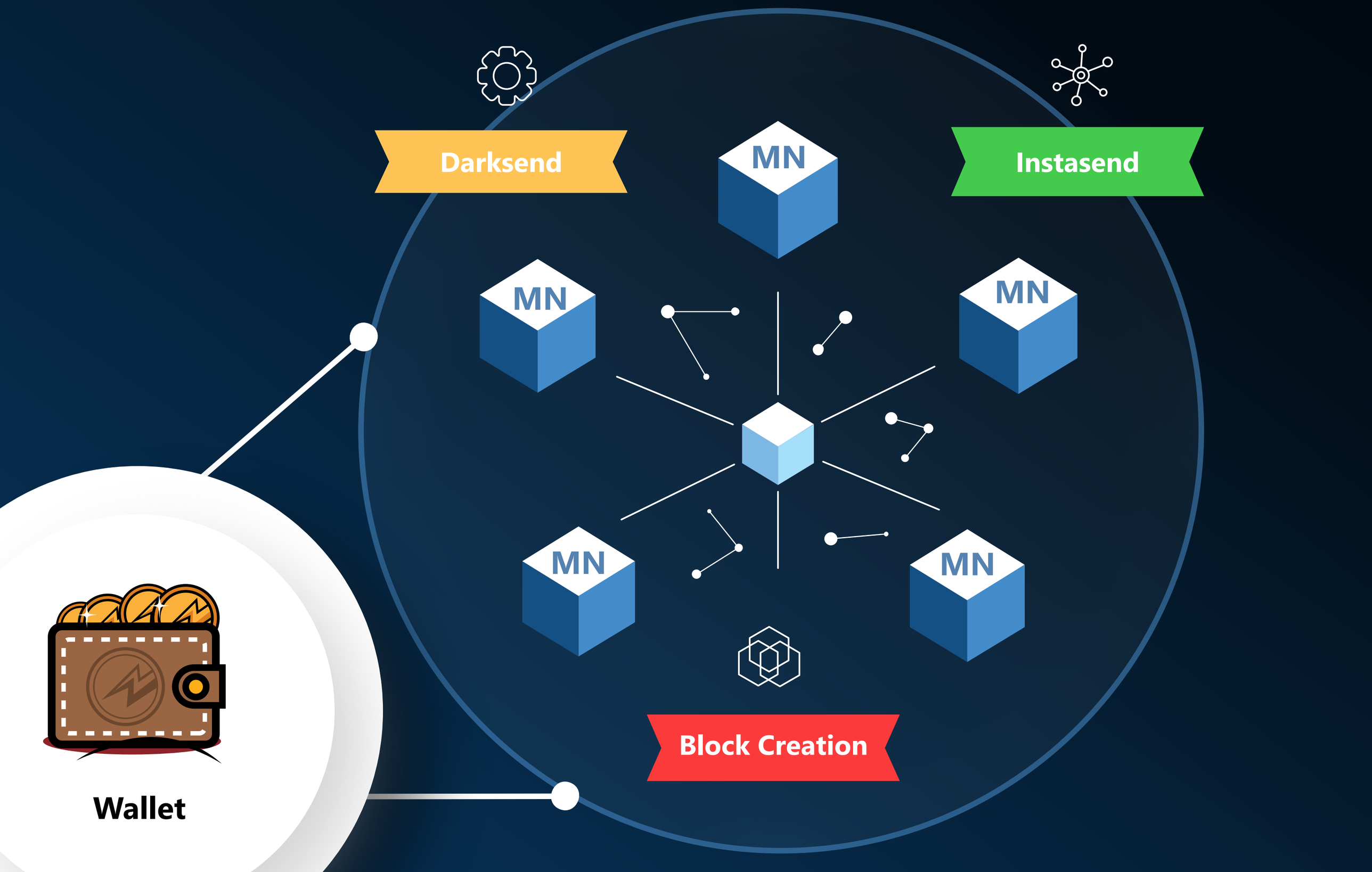
The DeviantCoin network governance model treats Masternodes as “first-class citizens” whose stake ensures they have a strong incentive to act for the benefit of the network. Masternodes form a distributed, decentralized management system that votes on network changes proposed by community members. This governance model is designed to be self-sustaining, to encourage high levels of developer motivation, and to be flexible enough to take on board and consider many diverse proposals for change.

17

Besides being a provider of services, masternodes benefit the network in other ways, too:

They make the network more decentralized. Each masternode runs a full copy of the blockchain; the more full nodes there are, the harder it is to censor the network's transactions, and the higher the security of the network.

They reduce the supply of coins. By locking coins in a masternode stake, masternodes reduce the supply of circulating tokens; this helps to stabilize, or even increase, the price.



18

ZEROCOIN

The Zerocoin protocol is a distributed e-cash scheme that provides strong user anonymity and coin security under the assumption that there is a distributed, online, append-only transaction store like Bitcoin. Zerocoin was first described in a whitepaper, where the first proposal was suggested as a protocol implementation on top of Bitcoin, which would require a soft fork.

Zerocoin works as follows: As all coins on public blockchains are visible to everyone by default, they are traceable. However, a Zerocoin user's wallet has an option to exchange the user's traceable coins for newly minted anonymous coins. For example, public DEV would be exchanged for anonymous zDEV ("z" as from Zerocoin), which can be spent anonymously. The zerocoin extension functions like a mixing pool, temporarily pooling coins together and exchanging them for newly minted coins. Mixing pools are an established concept used by various online services on a centralized basis. Zerocoin takes this concept onto protocol level, making it decentralized, and uses cryptography to anonymize exchanges with the pool.

19

Although the first proposal was for an implementation on top of Bitcoin, the first actual implementation was a fully fledged cryptocurrency called Zcoin. The Zerocoin protocol is based on RSA cryptographic algorithms, that used zk-SNARK algorithms (which resulted in the Zcash cryptocurrency).

The DeviantCoin implementation combines Zerocoin with use of a proof-of-stake consensus algorithm. Two staking systems are run in parallel on the DeviantCoin blockchain, one with standard DEV coins, the other with Zerocoin protocol coins (zDEV).

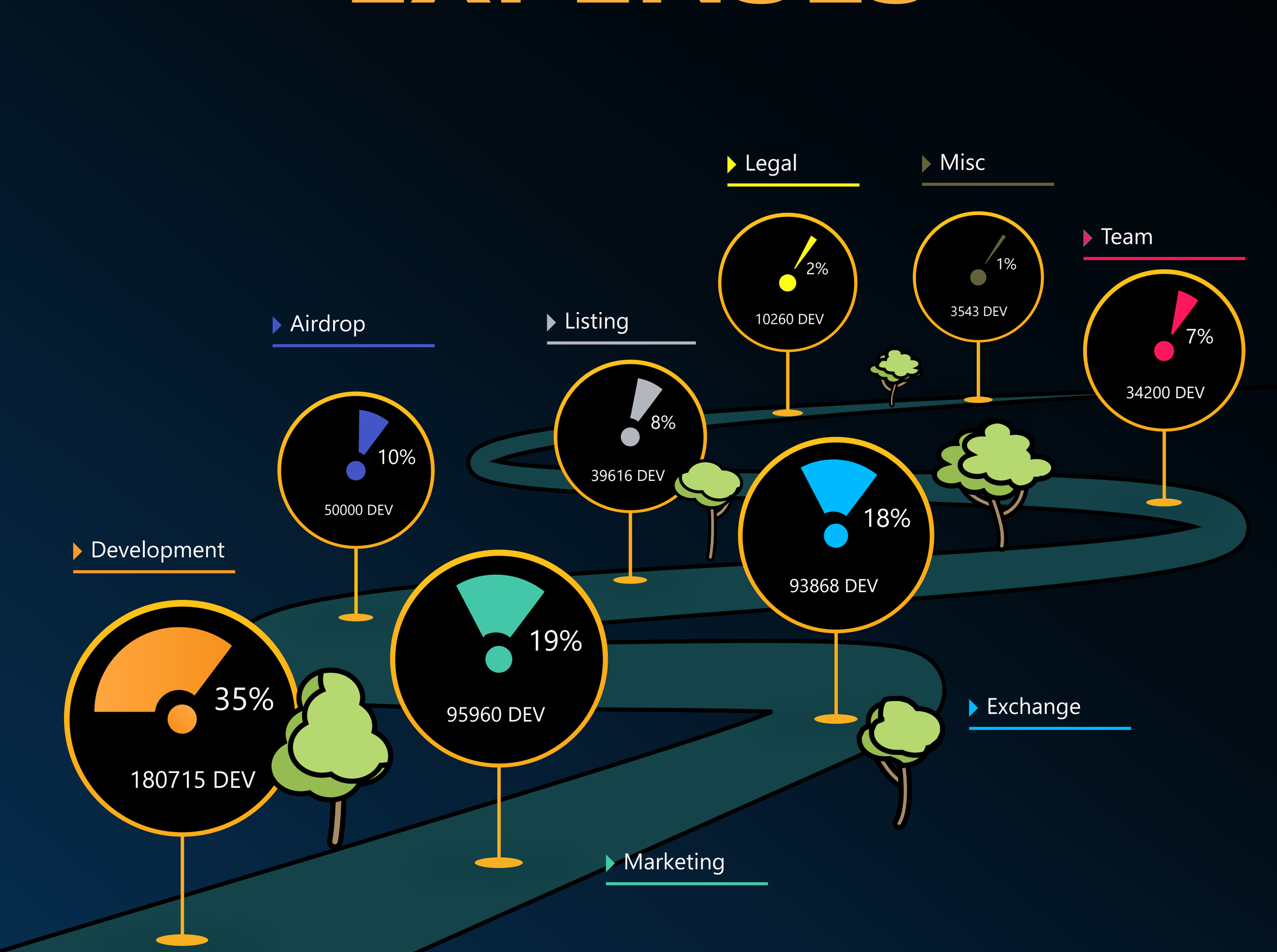
To ensure that both staking systems are covered.

The availability of more staked zDev coins ensures greater privacy.

Further information about Zerocoin can be obtained from Zerocoin's wikipedia page.

20

DEVIANT
EXPENSES



Spent till 08/08/2018: 508162 DEV

/DeviantCoin /DeviantDEV /Gp9zMXc /DeviantCoin /r/DeviantCoin