# Zano Marketplace

Andrey N Sabelnikov (andre@zano.org)
October 2019
www.zano.org

**Abstract**

Zano aims to create an anonymous, decentralized ecosystem that scales beyond direct p2p transactions. The private nature of the coin only solves a fungibility issue, next step should be creation of the services that would allow users to exchange coins, trade goods and services.

Zano Marketplace is a technology that allows users to list their ads in a decentralized network based on the Zano blockchain, receive responses, and make deals using built-in trustless escrow contracts in the Zano wallet.

Zano Marketplace provides a framework for developers to build their own independent marketplaces, while customizing and promoting them. The Zano blockchain insures stable, secure, and censorship resistant network.

## Storing offers

Decentralized marketplace is unique feature that is built on top of Zano blockchain. This framework allows users to publish ads, including:

- bid/ask descriptions (buy or sell offers)
- price
- type and amount of buying/selling goods
- poster name and contact information
- prefered method of payment
- expiration date and other relevant information

This ads defined as “offers”. Using blockchain as a platform for building a market structure implies storing offers data in transactions on blockchain. This could potentially be a problem, due to the temporary nature of the most ads and the blockchain history normally stored forever. In current implementation offers remain active for 2 weeks after which they need to be renewed. In order to effectively organize the storage of temporary data on the blockchain, we use the Zano’s “temporary

attachments" of the transactions. This type of attachments is stored in the transaction body only during the period before this transaction get covered by checkpoints.

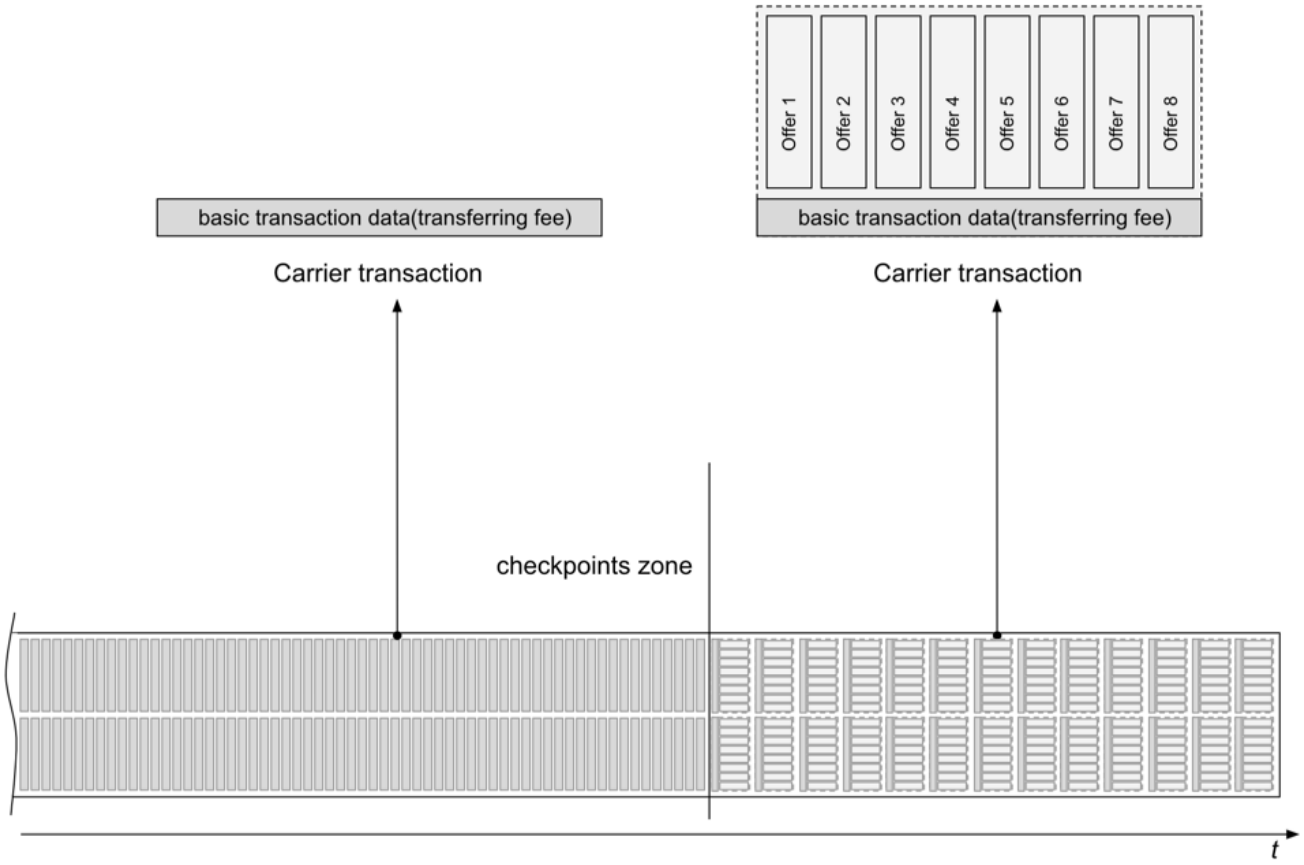


Figure 1 Blockchain before checkpoints(right), and compacted blockchain after checkpoints(left)

After passing checkpoint, this data will be excluded from the blockchain by the Zano pruning mechanism without violating its consistency and security of the network. Therefore, the blockchain size will not grow infinitely and new nodes won't need to download essentially useless data.

### Operating offers

Operating the offers is performed by "commands", which included in transaction's bodies in compact form. At this moment we have 3 types of commands:

- **"publish new offer"** - with this command new offer is published to blockchain
- **"update offer" -** this command define modifications that should be done to particular offer, that was published before.

- “**cancel offer**” - mark offer that was published before as not active

To prevent unauthorised offer update or deactivation, every offer has security field, both update and cancel commands must include proof, that it has been generated by the owner of the original post. This proof consists of reference to source transaction where offer was posted(tx_id) + number of the offer inside this transaction + information about offer update or cancelling, signed by the private ephemeral key, derived from one time transaction public key(Figure 2).

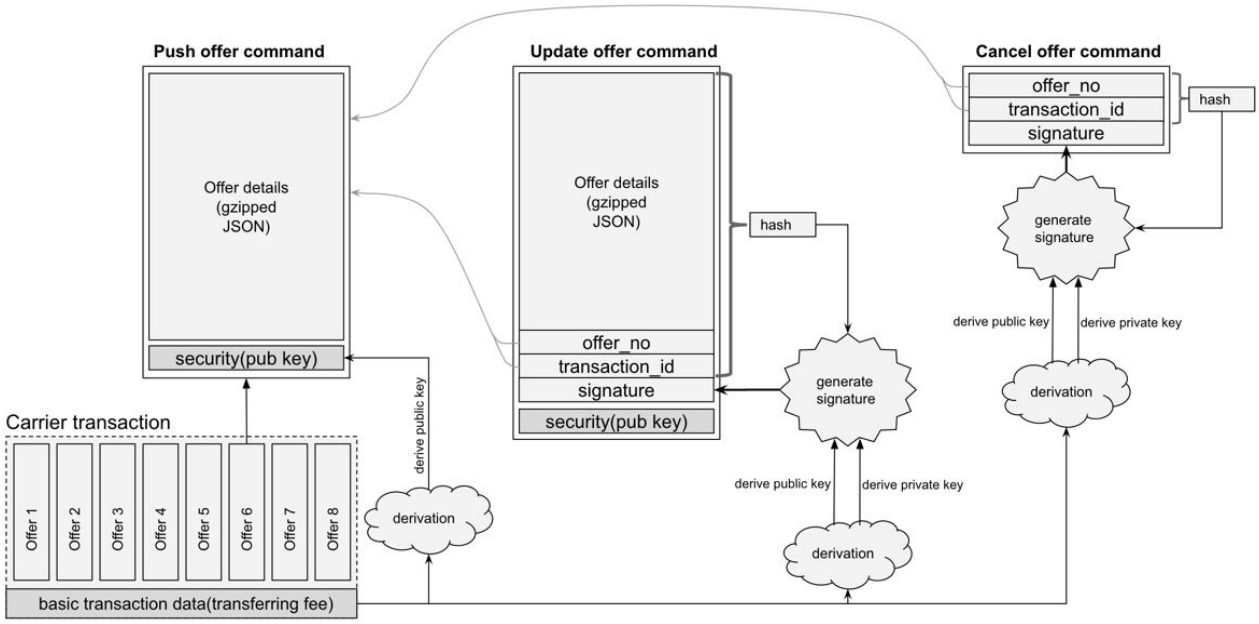


Figure 2 Generating proof for update offer and cancel offer commands.

From offers service perspective this update/cancel offer can be validated without knowing any transaction specific details, since “security” field provide public key, that should be used to validate a proof.

Offer details are stored in zipped JSON format (documented in https://docs.zano.org/docs/marketplace-api-guide). It provides flexibility to change the structure of the offer, customize it and make it easy to use for a third party developers.

Zano daemon includes module, that (if enabled) follows all offer commands and build registry of actual offers, present these offers by different indexes and has diverse filtering options in search API.

While simplewallet API should be used in order to perform the offer operations, since they require fee to be posted on the network.