Smart Communications in Heterogeneous Spacecraft Networks: A Blockchain Based Secure Auction Approach

Lixing Yu, Jinlong Ji, Yifan Guo, Qianlong Wang, Tianxi Ji and Pan Li

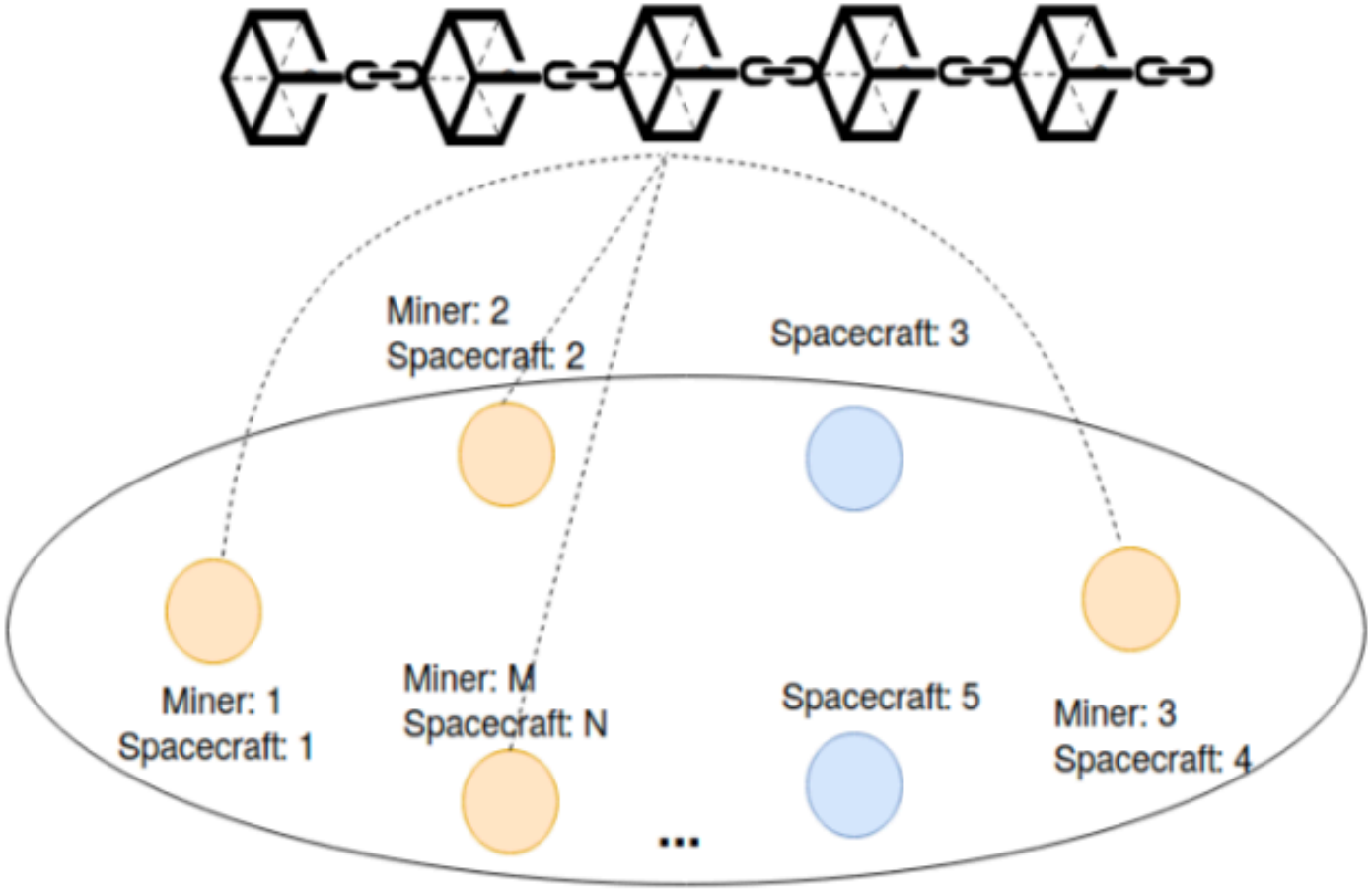
Heterogeneous Spacecraft Networks

- In the forthcoming space communications, there would be a large number of spacecrafts that belong to different organizations. Eg:Government space departments like NASA. Meanwhile, many companies, like SpaceX and Virgin Atlantic.
- More and more spacecrafts that need to communicate with each other and with the earth.
- All the spacecrafts thus form a heterogeneous network: Heterogeneous Spacecraft Networks

The communications in Heterogeneous Spacecraft Networks

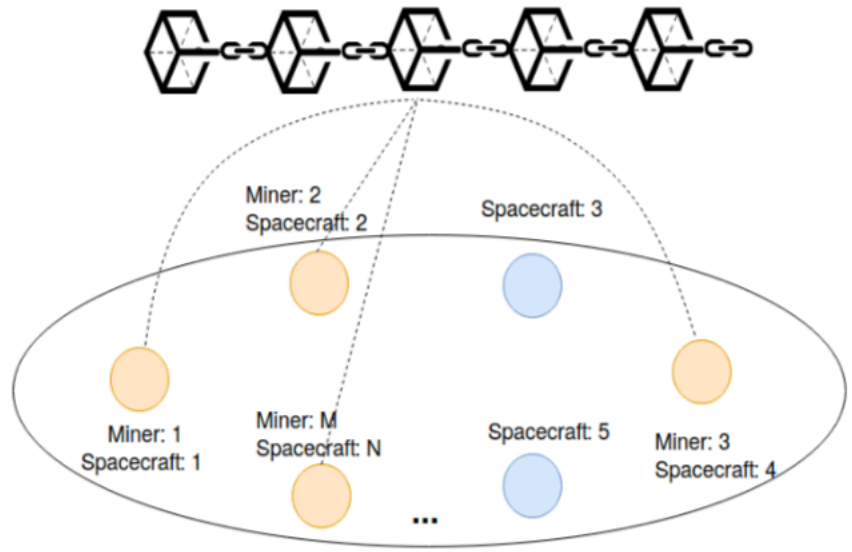
- While spectrum auction provides a potential solution to spectrum allocation, how to preserve the privacy during the auction process in the spacecraft networks has not been well studied
- We propose a secure spectrum auction scheme by utilizing blockchain and cryptography technologies

Blockchain Based Spectrum Auction for Heterogeneous Spacecraft Networks



BC Based Spectrum Auction Process

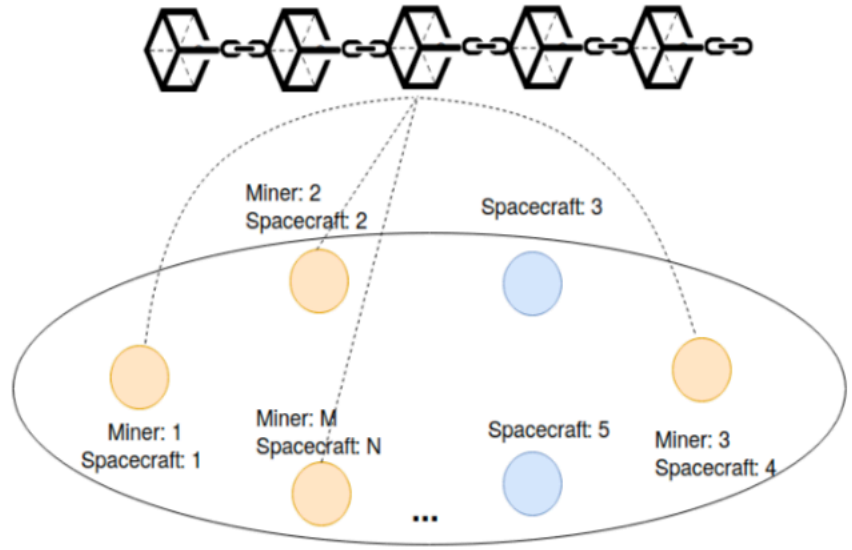
- GCC the **seller**: We consider that the spectrums in the space are regulated by an organization, say the “Global Communication Commission”
- we assume that the spacecrafts share the same set of available spectrum channels of the same bandwidth.
- The spacecrafts act as **bidders** in spectrum auctions, bidding for spectrum channels.
- In the meantime, some spacecrafts **also** act as **miners** who compete with each other to obtain the right to serve as the auctioneer, make auction decisions, and **record the auction results in the new block**.



BC Based Spectrum Auction Process

Recall that there are N spacecrafts and hence N bidders. For each bidder bi($1 \leq i \leq N$). We have the following definitions

- Bidder valuation v_i: the valuation, estimated by b_i, of a channel.
- Bid s_i: submitted by b_i. We denote the set of bids submitted by all bidders as S = $\{s_1, s_2, ..., s_N\}$. Each element s_i is a 2-tuple $< v_i, sn_i >$. Here, sn_i is the number of channels demanded by bidder b_i.
- Spectrum allocation a_i: spectrum allocated by the auction to bidder b_i. It specifies the number of the channels to bidder b_i. We denote the set of allocation results as A = $\{a_1, a_2, ..., a_N\}$
- Payment price p_i: the payment by b_i for one channel. We use P = $\{P_1, P_2...., P_N\}$ to represent the set of total payments of all the bidders. Thus, we have $P_i = p_i \cdot a_i$.



BC Based Spectrum Auction Process

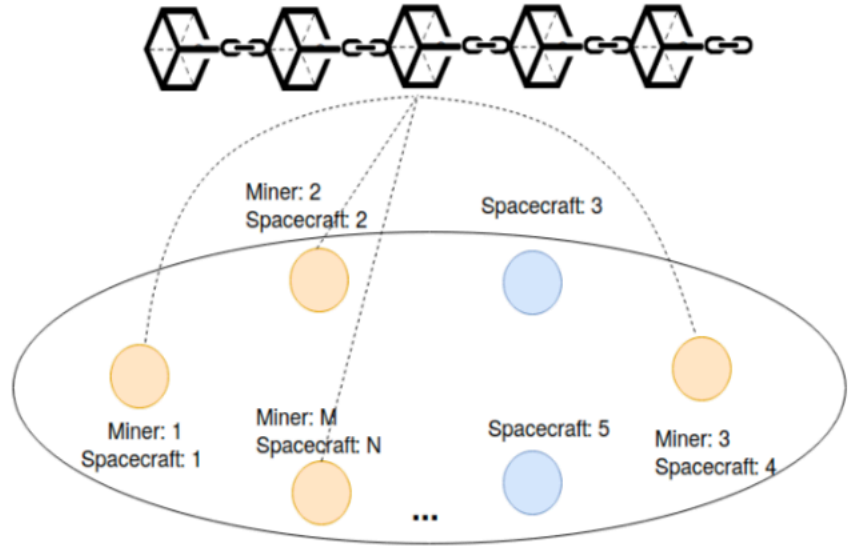
we define the cost function for the proposed framework :

$$c(A) = \Sigma_i (a_i \cdot C),$$

where $c(\cdot)$ is the cost function associated with spectrum allocation set A and C is the marginal cost of a channel.

The sellers' revenue in the auction is

$$\Sigma_i \ (p_i \cdot a_i) \ - \ c(A) = \Sigma_i \ (p_i - C)a_i.$$



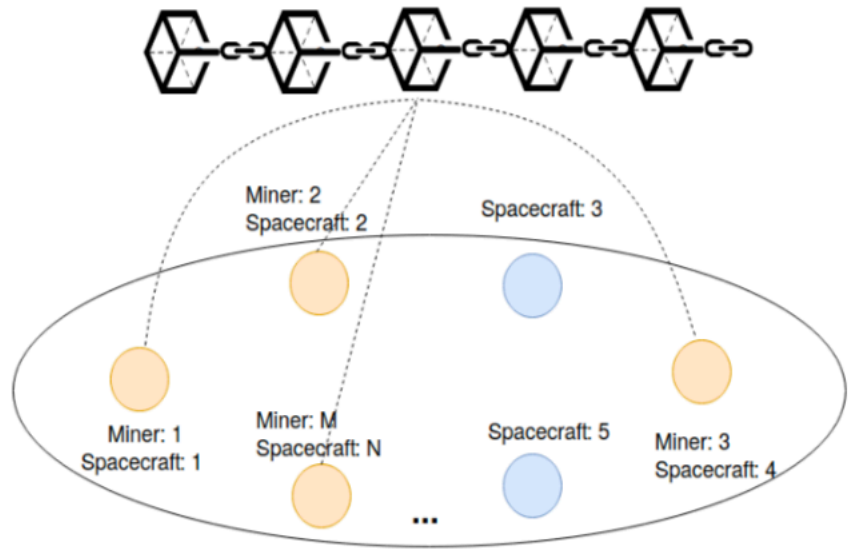
BC Based Spectrum Auction Process

The total payment of a winning bidder who obtains the demanded channels should not be larger than its total bid. Meanwhile, the payment of a losing bidder should be zero. Besides, we assume that the seller equally treats all the bidders so that they have fair price.

we set the p_i = p and $a_i = sn_i$, for $v_i \geq p_i$

$p_i = 0$ and $a_i = 0$ for $v_i < p_i$

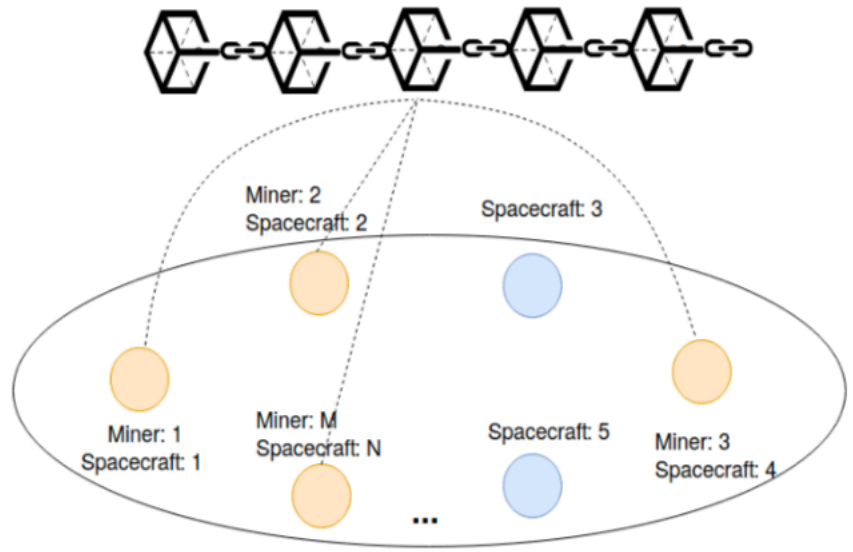
p is the clearing price.



BC Based Spectrum Auction Process

Single-round auction

The bidders first broadcast their bid to all the miners. In particular, each bidder b_i first generates its own blockchain address, for example, the SHA256 hash functions on its ECDSA public key as on the bitcoin blockchain.

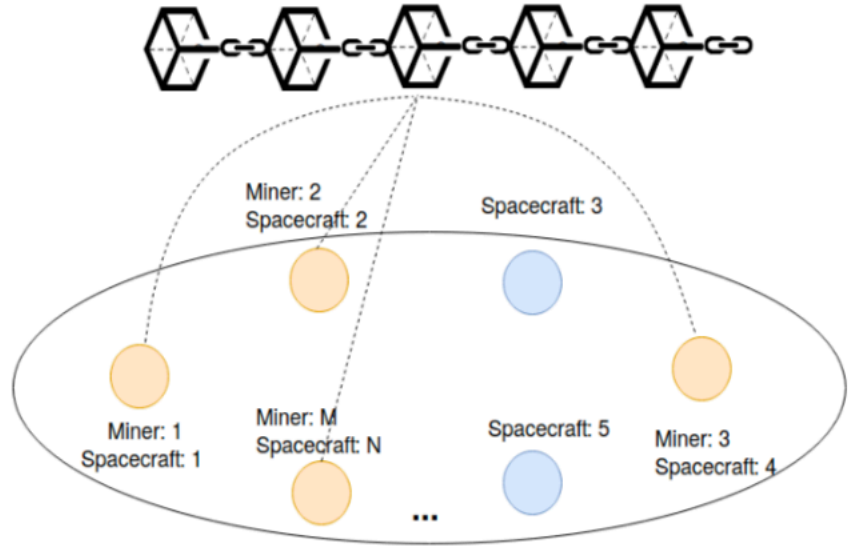


BC Based Spectrum Auction Process

Each bidder can generate an unlimited number of addresses with one given private key, for example, similar to that in sequential or hierarchical deterministic wallets, and hence use a different address for each auction, to protect its identity.

Each bidder b_i broadcasts its bid information $b_i = < v_i, sn_i >$ to all the miners on the blockchain.

The miners can compete with each other by applying PoW or PoS as the consensus protocol to decide who wins the right to "mine" the next block, and in our framework who gets to act as an auctioneer.

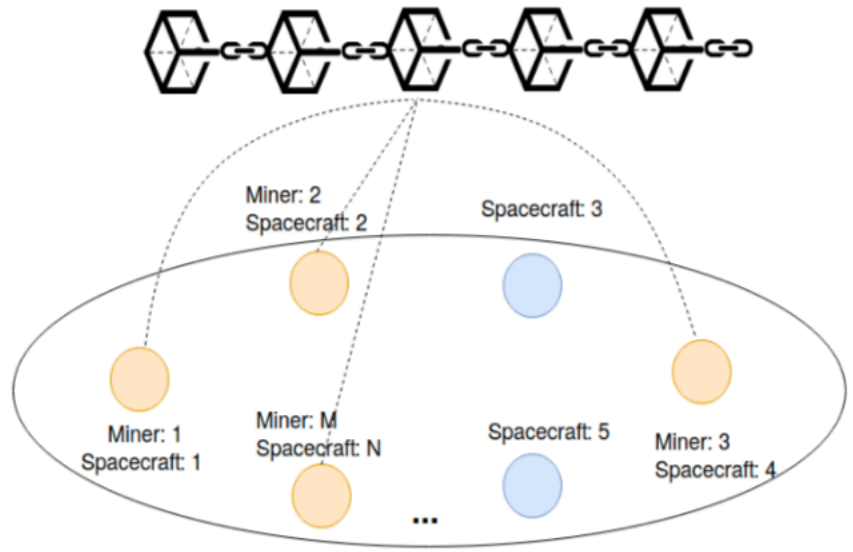


BC Based Spectrum Auction Process

The auctioneer determines the clearing price p, which along with the bidders' bids s_i's can decide the spectrum allocation vector A, as well as the set of the total payment vector P.

The winning miner spacecraft then records the information about this auction, including bidders' addresses, their bids s_i, and clearing price p, into the next block and append it to the blockchain tail.

To facilitate the auction, all the spacecrafts can use certain control channels provided by the sellers GCC.

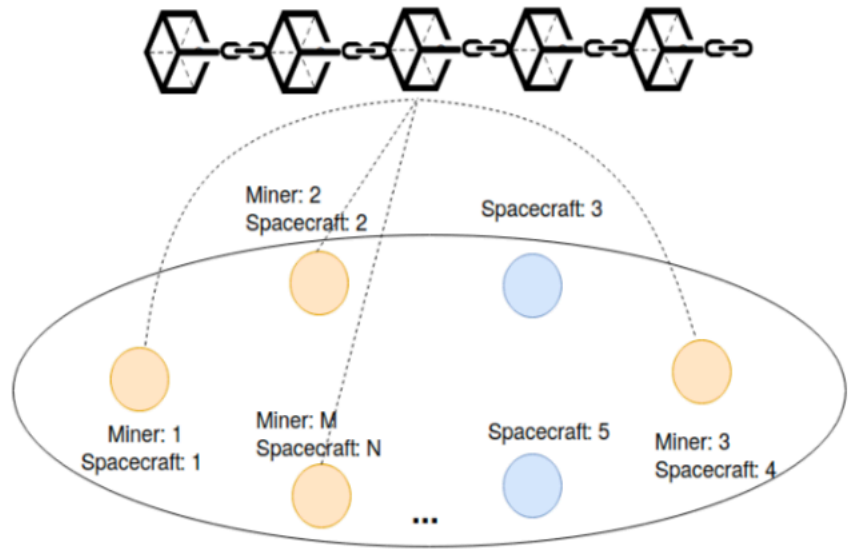


A Secure and Collision-resistant Spectrum Auction Framework

In the bidding phase, we apply the ElGamal homomorphic cryptosystem in a distributed manner for both the encryptions and decryptions.

Let p and q be two large strong prime numbers such that $p = 2q + 1$.

Let G_q be a sufficiently large multiplicative subgroup of Z_p^* of order q. g is the generator.

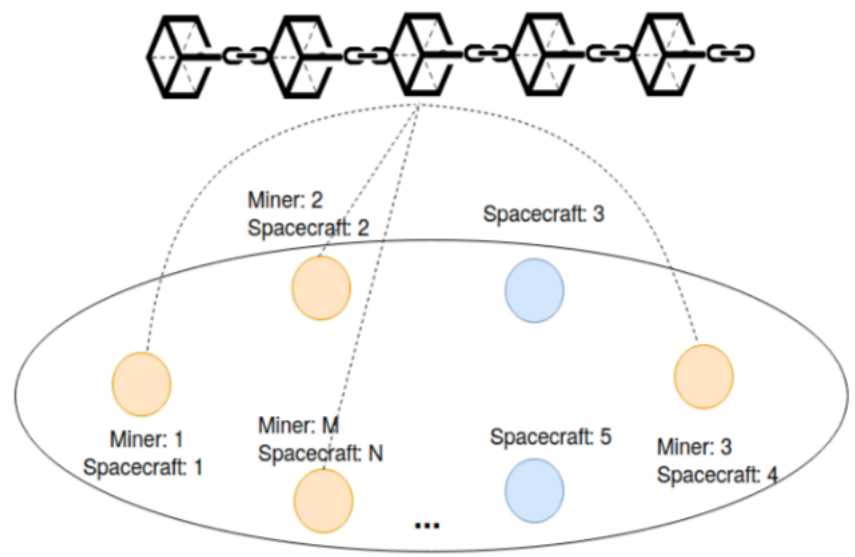


A Secure and Collision-resistant Spectrum Auction Framework

We first generate the encryption key in a distributed manner. In particular, we let each bidder b_i choose a random key $rk_i \in G_q$ and broadcasts $y_i = g^{rk_i} \bmod p$ to all the miners on the blockchain.

Each bidder b_i can calculate the public encryption key as $y = \Pi_{i=1}^{N} y_i$, and encrypts its own bid tuple $s_i = < v_i, sn_i >$ as $Enc(v_i) = < g^{r_i}, g^{v_i} y^{r_i} >$ and $Enc(sn_i) = < g^{r_i}, g^{sn_i} y^{r_i} >$.

r_i is a random number generated by the bidder b_i.



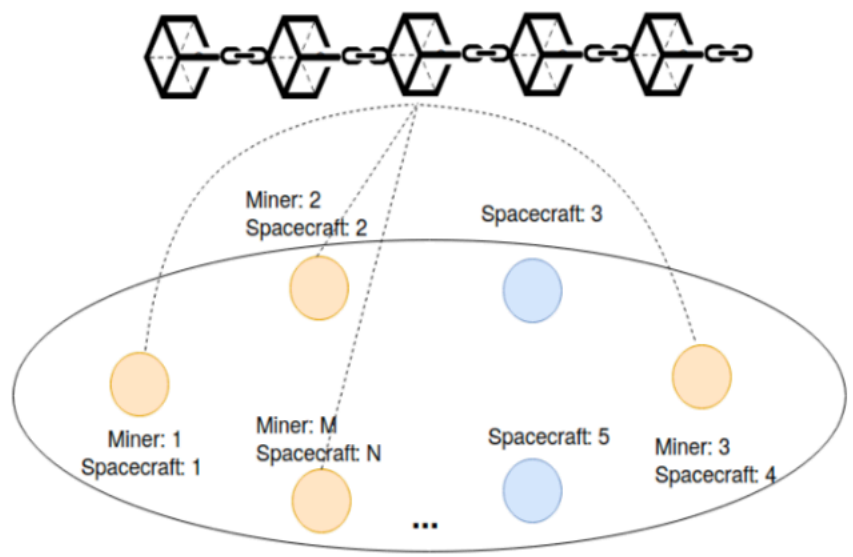
A Secure and Collision-resistant Spectrum Auction Framework

The seller's smart contract holds the codes that require the winning miner to encrypt the marginal cost for each channel, i.e., $p - C$, as $Enc(p - C) = < g^{r_C}, g^{p-C} y^{r_C} >$ where r_C is a random number generated by the winning miner.

The smart contract also requires the winning miner to generate a set of sampling parameters $\{ \alpha^1, \alpha^2, \alpha^3, ..., \alpha^{l'} \}$, where at least one of them satisfies $\alpha^l < v_1^{'}$ for $1 \leq l \leq l^{'}$.

$v_1^{'}$ is the highest valuation among all bidders and $\alpha \in (1, +\infty)$ is the price sampling parameter.

The winning bidder encrypts each of them by the public key y, i.e., $Enc(\alpha^l) =< g^{r_\alpha}, g^{\alpha^l} y^{r_\alpha} >$.

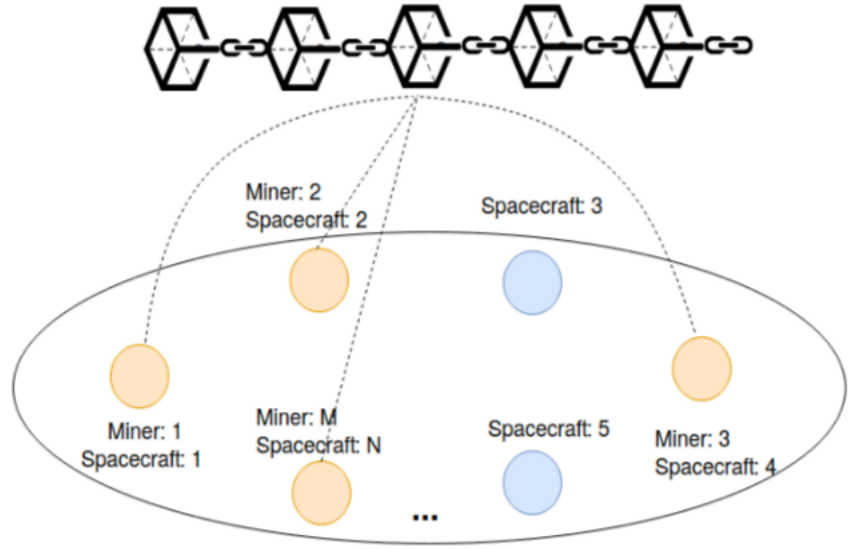


A Secure and Collision-resistant Spectrum Auction Framework

In the clearing price determination phase, the auctioneer needs to choose a candidate clearing price φ.

It first sorts the bidders' valuations $v_i's$ in a non-ascending order given that they are encrypted, for example $Enc(v_1), Enc(v_2), ..., Enc(v_N)$, which can be achieved from the outcome in study [20] that can compare two encrypted values.

It first sorts the bidders' valuations $v_i's$ in a non-ascending order given that they are encrypted, for example $Enc(v_1), Enc(v_2), ..., Enc(v_N)$, which can be achieved from the outcome in study [20] that can compare two encrypted values.



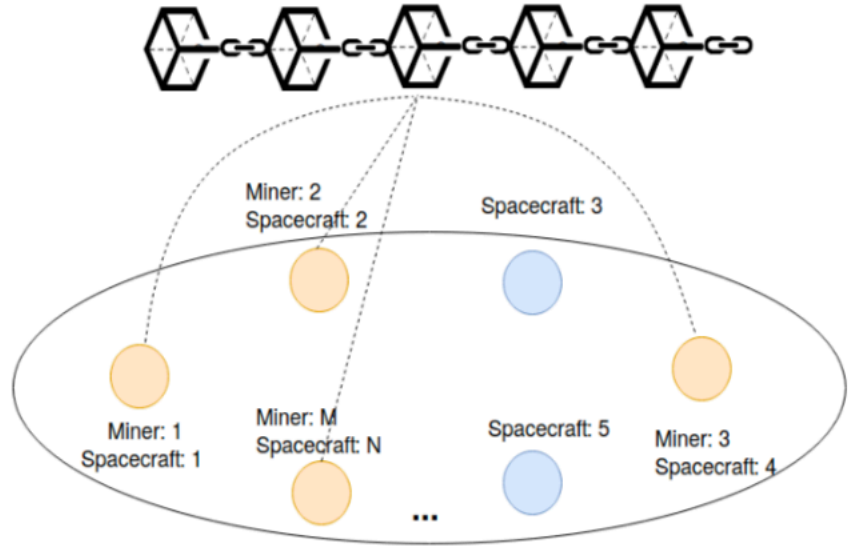
A Secure and Collision-resistant Spectrum Auction Framework

We use $v^2_{1'} \geq v^2_{2'} \geq ... \geq v^2_{N'}$ to stand for the sorted bidders' valuation.

Then, the auctioneer compares its price samplings with the highest valuation $v_1^{'}$ until it finds one that can satisfy $\varphi = \alpha^l \leq v_1^{'}$.

The auctioneer calculate the revenue yielded by φ, i.e., $R = \Sigma_{\{i|v_i>p\}}(p-C)sn_i$ as aforementioned, which can be realized by employing the homomorphic encryption scheme.

Furthermore, the auctioneer computes the revenue for all the $\alpha_l \leq v_1^{'}$, and the highest one and its φ^* value respectively, which is set to be the clearing price p.

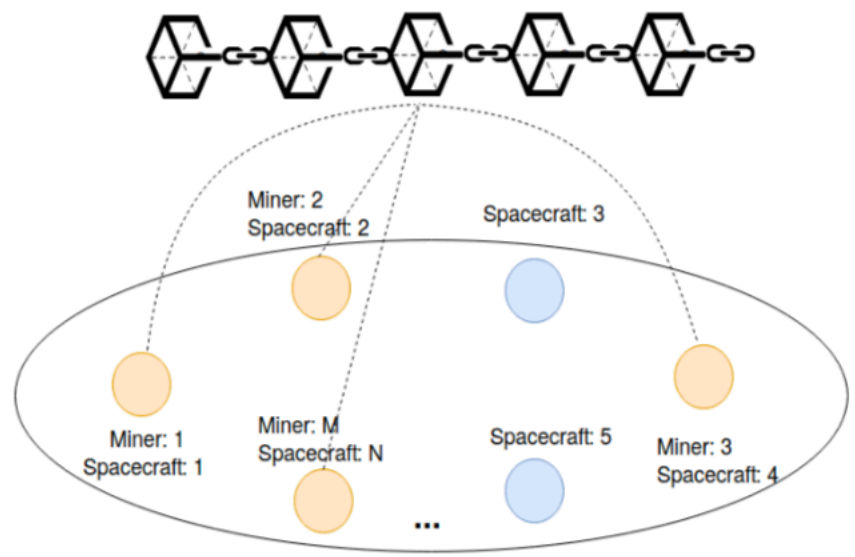


A Secure and Collision-resistant Spectrum Auction Framework

Finally, the auctioneer encrypts the bidders' addresses, bids s_i, as well as the clearing price p with the public encryption key y, respectively, and writes the ciphertexts into a new block.

Particularly, the ciphertext of p is $< g^{r_p}, g^p y^{r_p} >$, where r_p is a random number chosen by the auctioneer.

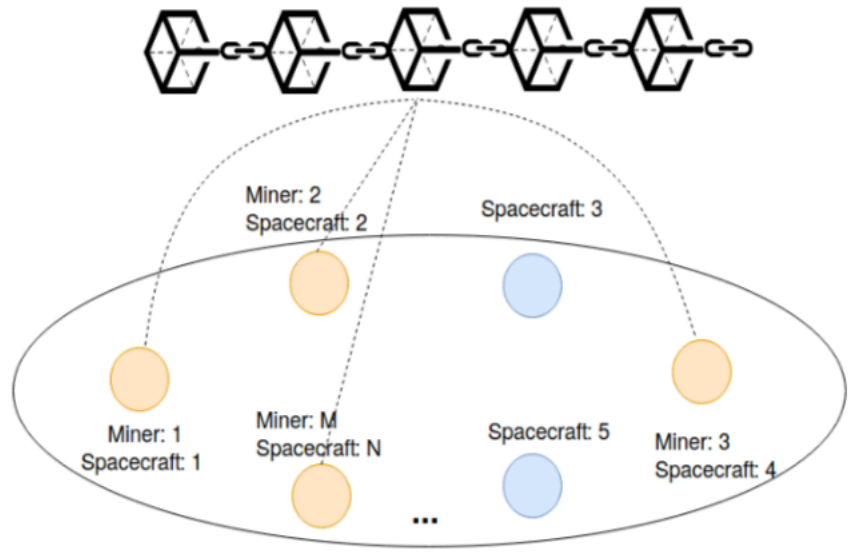
Each bidder broadcasts $(g^{r_p})^{rk_i}$ to all the bidders, and then each of them can decrypt the message by $g^p y^{r_p} / \Pi_i^N (g^{r_i})^{rk_i} = g^p$.



A Secure and Collision-resistant Spectrum Auction Framework

Given that there are only l' possible clearing prices as defined by the price sampling parameters, g^{α^l} $(1 \leq l \leq l')$ can be computed in advance.

Hence, each bidder can find out the clearing price by itself by comparing g^p with g^{α^l}.

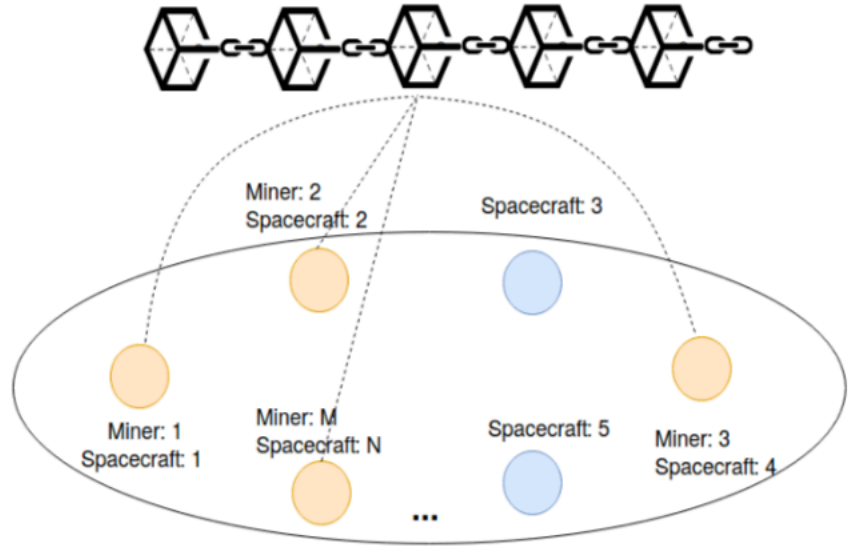


Simulation

We use PCs to simulate a heterogeneous spacecraft communication network.

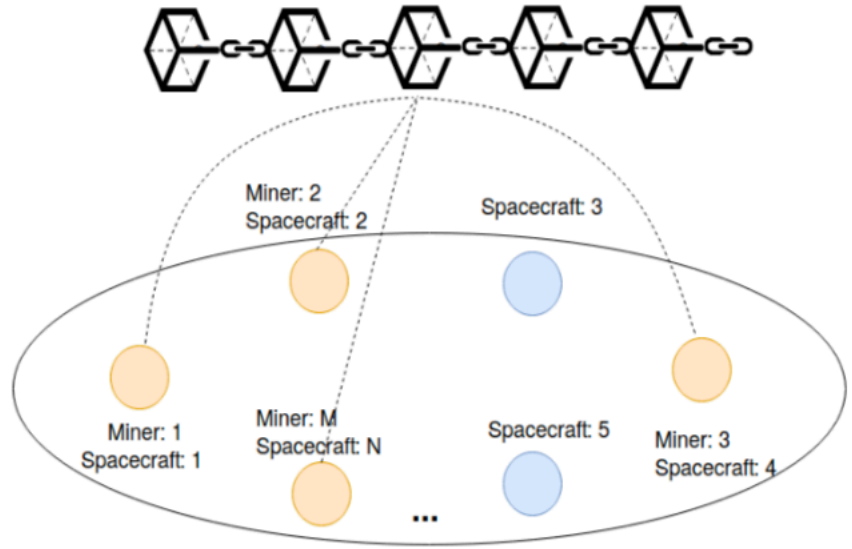
we employ 7 PCs to simulate a spacecraft network, each of which hosts 4 virtual machines representing 4 spacecrafts, thus resulting in 28 spacecrafts in total.

On each PC, we select one virtual machine to be a miner, and the rest three virtual machines to be the bidders, each of which asks for one channel.



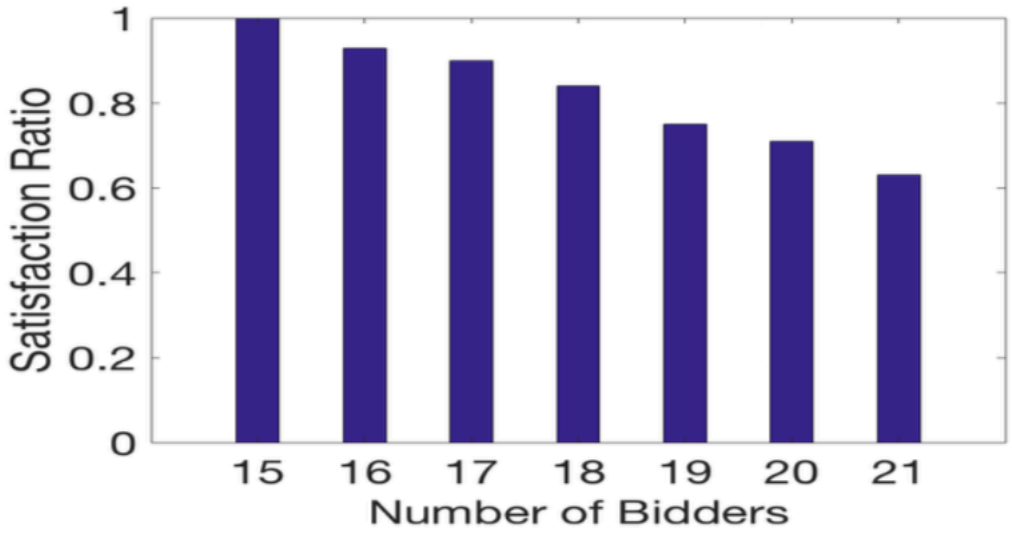
Simulation

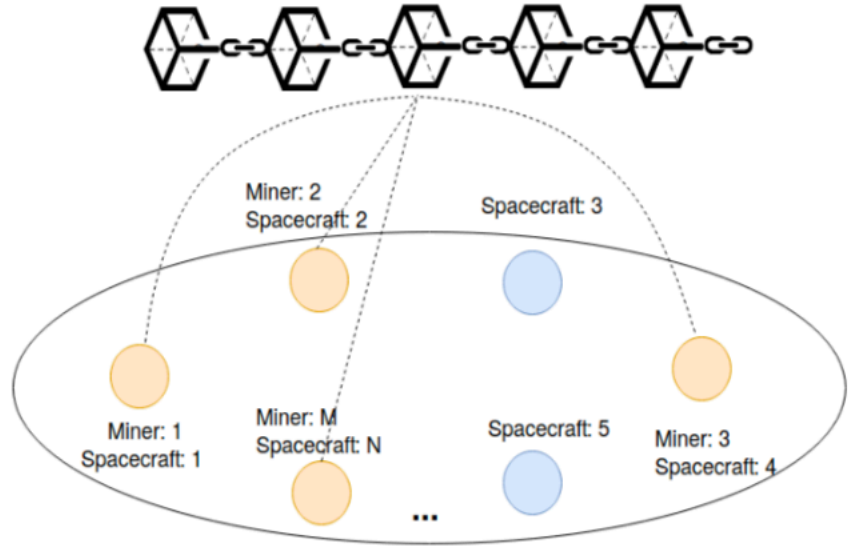
In the simulations, we test the satisfaction ratio under various numbers of available spectrum channels, which is defined as the ratio of the number of winning bidders to the total number of bidders.



Simulation

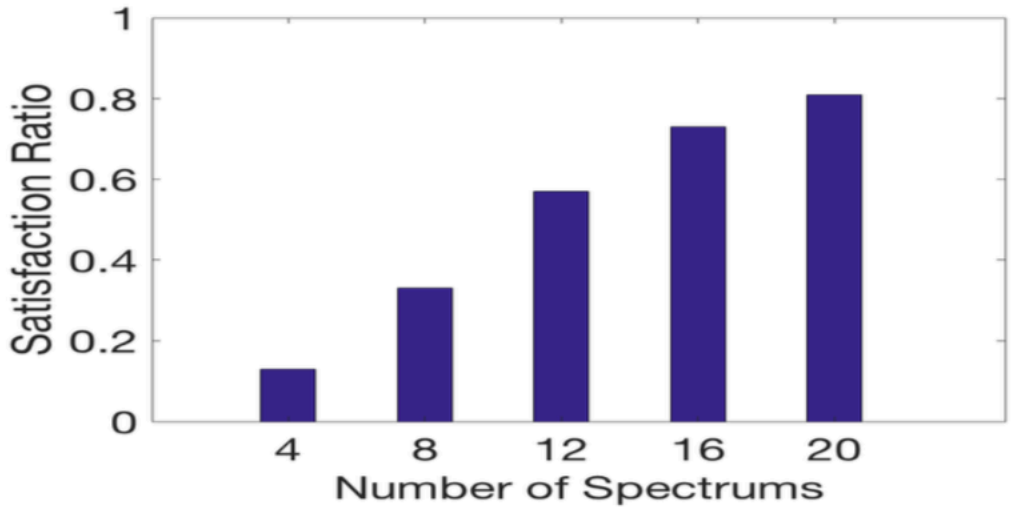
First, we have 14 available channels in the network. We increase the number of bidders number in turn from 15 to 21.

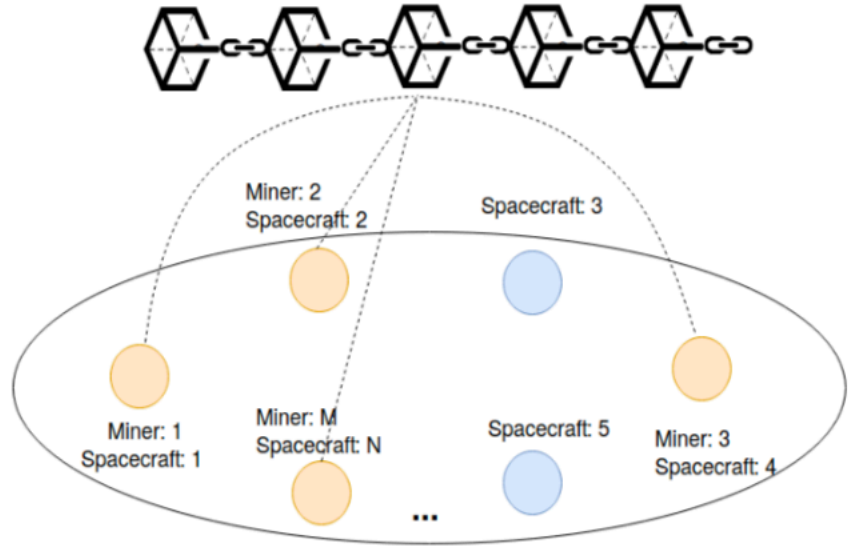




Simulation

Then, we keep the other settings as above, but increase the number of available channels from 4 to 20 (4, 8, 12, 16, 20).





Thank You!