Why Schnorr signature is hailed as the biggest technological update after Bitcoin Segwit

Summary:

On October 15th, codes of 3 proposals (BIP340-342) led by Bitcoin core developer Pieter Wuille were officially merged into the main branch of Bitcoin code [1]. The three proposals included Schnorr, Taproot and Tapscript. The community evaluated this change as the biggest change in Bitcoin since Segregated Witness.

The main goal of Schnorr signature is to replace the current ECDSA signature in Bitcoin. Compared with ECDSA currently adopted by the Bitcoin blockchain, Schnorr has some advantages as follows:

(1) Schnorr signature is highly secure, which can be proved in math, and is not malleable;

(2) The signature can provide privacy protection for multiple signatures;

(3) The linear feature of the signature can be used as the basis of Taproot and other technologies to enhance the privacy of transactions;

(4) The signature length is shorter, and multiple signatures can be aggregated, which can save storage space and realize expansion;

(5) Signatures can be verified in batches, which can improve verification efficiency;

However, it also has some shortcomings as follows:

(1) Users need multiple rounds of interaction before use;

(2) Some additional bandwidth and computing resources will be consumed;

(3) The randomness requirement for random numbers is very high.

As an update that may replace the ECDSA (elliptical encryption algorithm) signature mechanism, Schnorr signature is one of the most important milestones in the development of the underlying technology of Bitcoin. The addition of the Schnorr signature code means that this technology has basically taken shape in Bitcoin, and what we need to is to wait for the community to decide the activation time of the soft fork, but the exactly time has not yet been determined.

Authors:

【Huobi Research Institute】Yuan Yuming, Ma Tianyuan, Zhao Wenqi, Chen Le

Contact the Authors:

Huobi Research Institute: HuobiResearch@huobi.com

Content

1. Background

The Schnorr signature was originally created by the German cryptographer and mathematician Claus-Peter Schnorr (Figure 1), and the technology is also named after him. Based on a specific discrete logarithm problem, Schnorr has long been known for its security and simplicity. But Schnorr registered a patent for this signature. Therefore, good as the technology is, it can not be widely used in many applications for a long time.

Figure 1 German cryptographer and mathematician Claus-Peter Schnorr

The patent signed by Schnorr did not expire until 2008. In the mean time, the industry did not have a widely accepted specific implementation plan. So Satoshi Nakamoto, who released the Bitcoin white paper in the same year, did not choose the Schnorr signature technology, but the more mature technology, ECDSA signature scheme, at that time. With the expiration of this Schnorr patent, this technology gradually landed. Driven by core developers of the Bitcoin community such as Pieter Wuille, the community began to seriously consider applying Schnorr signatures to replace the current ECDSA signatures in a way of soft fork upgrade.

In July 2018, Bitcoin Core developer Pieter Wuille proposed to upgrade Schnorr's BIP, and then Blockstream and the open source community also participated in related development work. Before officially adopted by Bitcoin, the technology of Schnorr had been deployed in advance through a hard fork in Bitcoin's forked chain, BCH. In May 2019, BCH upgraded the signature scheme to Schnorr signature. The reason why it has been activated earlier is its upgrade way is hard fork rather than soft fork. But Bitcoin cannot adopt a hard fork scheme, which requires a more sophisticated soft fork scheme.

Later, Pieter Wuille further proposed the Taproot/Schnorr soft fork upgrade proposal, which was officially released in January this year(the BIP 340-342 mentioned in this article). This time, Schnorr's upgrade proposal has been officially merged into the code base. The three proposals merged into the Bitcoin master branch are BIP 340: Schnorr Signatures for secp256k1[2], BIP 341:

Taproot: SegWit version 1 spending rules[3], and BIP 342: Validation of Taproot Scripts[4].

Among them, the first proposal is the main proposal of Schnorr signature, and Taproot is an abstract syntax tree upgrade of Merkel tree. Together with the Schnorr signature, it will allow Bitcoin to execute more smart contract scripts in a private manner; the last proposal is a supplement to the other two proposals, mainly upgrading the original Bitcoin script to support Schnorr signature, batch verification, signature hash, etc. However, it is worth noting that the Schnorr algorithm is still not standardized by the industry. The Schnorr used in the BIP 340 proposal is still tailor-made based on Bitcoin.

2. Schnorr signature and BIP proposal

2.1 What exactly is a Schnorr signature?

Schnorr is essentially a cryptographic signature technology. We can simply understand that in the Bitcoin system, Schnorr will be an alternative upgrade to ECDSA.

The full name of ECDSA is Elliptic Curve Digital Signature Algorithm. Its role in Bitcoin is not unfamiliar to us. We use ECDSA technology for every signature in the Bitcoin network. For example, if Alice wants to send a transaction, the miner must confirm that only Alice has the private key and the right to dispose of the asset. Therefore, Alice needs to use ECDSA to generate a unique signature that cannot be modified to prove that Alice has the private key and confirm the specific amount of the transaction. When Schnorr is officially activated, this work will be taken over by Schnorr. This process is shown in Figure 2.

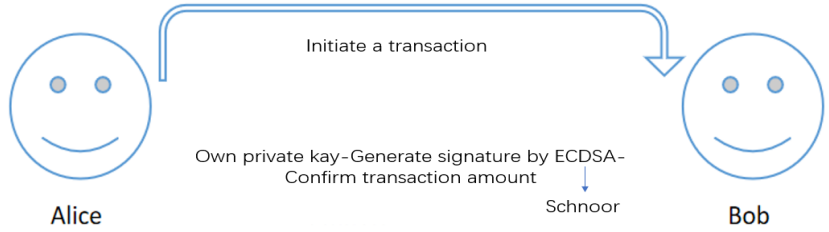

Figure 2 ECDSA/Schnorr algorithm in a transaction

2.2 Why do we need to change the signature scheme?

In the past 10 years, ECDSA has performed well, and seems to be able to perform the key task

of generating signatures. However, there is a problem that has been lingering over ECDSA. At present, the industry has not been able to give a rigorous mathematical and cryptographic argumentation process to prove that ECDSA is mathematically safe. However, Schnorr can. Under certain conditions, the Schnorr signature technology is proved to be mathematically safe [5-6]. For cryptocurrencies that rely heavily on security such as Bitcoin, technologies that can prove security are certainly more reassuring than cannot.

At the same time, for Bitcoin, what is more important is that the Schnorr signature has a "linear" feature, which allows the public keys of multiple users to be aggregated into one public key through linear calculation, and the corresponding aggregated signature can be generated.

Why is the "linear" characteristic so important to the current Bitcoin? ECDSA itself does not support. So multi-signature in Bitcoin is now processed through P2SH scripts, but P2SH-like scripts will expose the existence of multi-signature transactions to the network, which can be used to infer all participants. Schnorr technology can aggregate multi-signatures into one, helping to enhance the privacy of transactions, save the space cost by multi-signature in the unlocking script, save valuable on-chain space, and realize expansion. On the whole, if widely popularized, this technology may be able to bring about 5% to 20% improvement in Bitcoin performance.

In addition, since several signatures are aggregated into one, only one single time of verification process is required when verifying all these signatures, which will reduce the cost of calculation. The technical details of this part will be described in the next chapter.

The great significance of Schnorr signature to Bitcoin also relies on its cornerstone role for technologies such as Taproot which is the content of the second proposal BIP341. Taproot is derived from MAST (Merkelized Abstract Syntax Tree), which can express complex scripts in the form of Merkel trees. We know that one of the important characteristics of the Merkel tree is that it can quickly verify the existence of a node value without revealing the true data of irrelevant branches, and it is widely used to store transactions and states data in the blockchain. Based on this feature, Taproot can complete the running of the script without revealing the irrelevant branches. In contrast, P2SH needs to reveal all the script content.

Combined with Schnorr signature technology, Taproot can even make a transaction with complex scripts (including Lightning Network transactions, multi-signature transactions, multi-

judgment branch transactions, etc.) look like an ordinary P2PKH transaction. It supports complex scripts, protects script privacy, does not expose the signer, and makes a transaction with complex judgment conditions look as simple as an ordinary transaction, which cannot be distinguished from the form, which is the effect of the combination of Taproot and Schnorr.

2.3 In what form will Schnorr proceed?

Similar to many previous BIPs, this time Schnorr scheme will be conducted in a way of soft fork.

The full name of BIP is Bitcoin Improvement Proposals. Generally speaking, it includes updates to the underlying blockchain technology of Bitcoin, introduction of new features, and information supplements. Since Satoshi Nakamoto released the first version of the Bitcoin blockchain client in 2009, most technical updates have been added to Bitcoin technology in the form of BIP. At present, the Bitcoin community has adopted more than 100 BIP proposals, such as Segregated Witness (BIP 144), P2SH multi-signature structure (BIP 49) and Mnemonic (BIP 39).

The difference between a hard fork and a soft fork may not be unfamiliar to many people. In a hard fork, when the community has strong disagreements on certain features and technologies, the main chain will be divided into two, with the old and new clients incompatible with each other, such as BTC and BCH, BCH and BSV, etc. And in a soft fork, such as Segwit upgrade. Although the community may have opposite ideas, the chain can still remains only one, and the old and new clients can be compatible to a certain extent.

Hard forks may sometimes bring strong turbulence in the community. Therefore, the Bitcoin community have a long-term reservation about active hard fork upgrades and avoid hard fork upgrades as much as possible. This Bitcoin Schnorr upgrade will be completed through a soft fork, which is an important feature that it is likely to be successfully activated by the community.

Replacing the ECDSA signature seems to be a very big change. Why can Schnorr be able to complete it through a soft fork? This starts with Schnorr technology itself.

The security of Schnorr is based on such an assumption: that a particular discrete logarithm problem is very difficult to solve, and its security can be proved by mathematical means. In other words, as long as this assumption is true, the intractability of Schnorr signature will be equal to that of the discrete logarithm problem.

At the same time, the elliptic curve also has a problem very similar to the discrete logarithm. The security of the elliptic curve digital signature algorithm (ECDSA) in Bitcoin in the past is also based on the intractability of the elliptic curve discrete logarithm problem (ECDLP).

Therefore, the Schnorr signature still uses the elliptic curve inherited from the original Bitcoin and adopts a new calculation method, in order to be compatible with the version that does not want to upgrade to the greatest extent, and realize the soft fork upgrade.

On the other hand, Schnorr has made very little changes to the Segwit client, and the current penetration rate of the Segwit client exceeds 90%. According to statistics from luke.dashjr, as of October 2020, more than 90% of Bitcoin network nodes have updated their clients to version 0.16 or higher, which is the upgraded version of Segwit. Segwit isolates the signature information from the transaction information and attaches it to the end as a separate structure. Because the signature information only plays a role of verification and does not affect the key parameters of the transaction: such as the transfer address and quantity. Schnorr signatures mainly affect signature information. For clients that have upgraded Segwit features, Schnorr signatures only involve signature verification information attached to the end with a separate structure, which has little impact.

In summary, Schnorr signatures can be added to the underlying technology of Bitcoin in the form of a soft fork upgrade, without hard forks or bringing divisions to the community. Clients that reject Schnorr signature can still join the network normally and complete operations such as packaging like before. As a form of upgrading, soft forks are more difficult to implement and often require sophisticated designs to bypass certain rules, but they are more compatible and will not lead to consensus splits. In one word, it is a gradual-approach and gentle-update method.

Due to the gentle upgrade characteristics of the soft fork, the smaller drawbacks of Schnorr, and the favorable condition driven by core developers, it has a higher possibility of activation.

3. Analysis of Schnorr signature technical details

Next, let us analyze the technical details of Schnorr signature。

3.1 High security

The security of Schnorr signature has been proved mathematically, whereas ECDSA has not

yet been proven. Although ECDSA has not had any safety issues for many years, it is like a volcano that has been silent for many years without erupting, which you don't know if it will erupt. But an algorithm that is mathematically proven must be more trustworthy than an algorithm that may have "hidden troubles".

Based on the mathematical proofs of scholars such as David Pointcheval and Yannick Seurin [5-6], we know that in the random prediction model, it is very difficult to assume the discrete logarithm of the elliptic curve. The only way to break through the Schnorr signature is to solve the discrete logarithm problem.

So in some ways, Schnorr signatures are more secure and trustworthy.

In addition, Schnorr signatures are not malleable, which can be fully demonstrated in comparison with ECDSA, which is a malleable signature algorithm. Specifically, based on the signature generated by ECDSA, an attacker can generate a new signature that is equally valid for a given message without knowing the private key. Bitcoin also specifically proposed BIP 146 to deal with this problem. However, Schnorr signatures are naturally non-extensible and can directly bypass this security problem.

3.2 Support the aggregation of signatures to save storage space

The aggregation of signatures mainly refers to the aggregation of multiple signatures. Multi-signature is a technology in Bitcoin that controls the use of funds. For example, our common "2 of 3" multi-signature requires that at least two of the three authorized parties have signed the transaction before the funds can be used.

Figure 4 "2 of 3" multi-signature——

at least 2 of the authorized 3 parties signed and confirmed

For example, the picture above is a "2 of 3" multi-signature input script. You can see that there are 2 ECDSA signatures in the red box. With these 2 signatures, the funds can be used legally. However, ECDSA's multi-signature does not aggregate any of the signatures, just simply puts each signature in the input script, and the public keys of the two signers also need to be placed in the input script separately. If there is a "9 of 10" multi-signature, you need to store 9 signatures and 9 public keys in the block, which consume a lot of storage space.

While Schnorr signatures can solve this problem. The Schnorr signature aggregates a sum of m signatures from any "m of n" multi-signature into one signature through a technology called Key Aggregation, and the public keys of m signers can also be aggregated into 1 public key. No matter how big the number m is, only one signature and one public key need to be filled in the input script, which can greatly reduce the space occupied by the multi-signature in the block. The saving of space occupied by multi-signature pairs is shown in Figure 5.

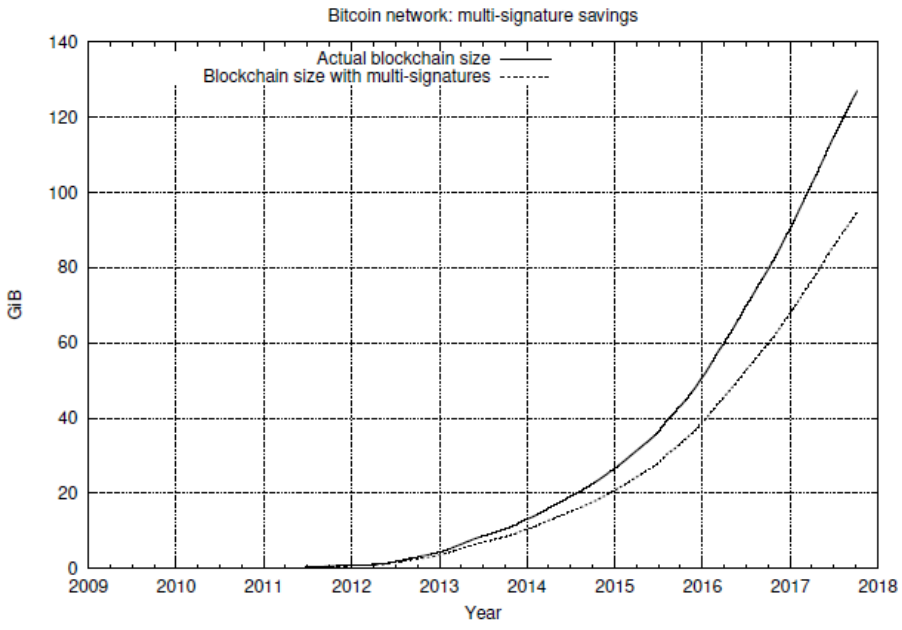

Fig. 3. Size of the Bitcoin blockchain with and without multi-signatures.

Figure 5 Schnorr signature reduces the space occupied by Key Aggregation

The picture above is a simulation calculation made by Pieter Wuille on Bitcoin historical data. After replacing all the multi-signatures in Bitcoin historical data with Schnorr's aggregated

signatures, the storage space of Bitcoin blocks can be significantly reduced.

The above mentioned is only one of Schnorr aggregated signatures, that is, "aggregate multiple signatures in a single UTXO input". In fact, Schnorr signatures have a more powerful function, which can "aggregate multiple signatures from multiple UTXO inputs", so that there is only one Schnorr signature for the entire UTXO. However, the preconditions for this kind of aggregation are harsher and more complicated to implement.

3.3 Shorter signature length, which can save storage space

According to the scheme proposed by Pieter Wuille, the Schnorr signature algorithm used in Bitcoin has a public key length of 32 bytes and a signature length of 64 bytes. The ECDSA signature algorithm currently used by Bitcoin has a public key length of 33 bytes, and a signature can reach up to 72 bytes (see Figure 3). The bitcoin block space is limited so saving a little space is of great significance.

Input	Output
PreviousOutPoint={ TxHash:1dda832890f85288fec616ef1f4113c0c86b7bf36b560ea244fd8a6ed12ada52, OutIndex:1} SignatureScript = PUSHDATA(72) [3045022100c435eb458b295381d6e1f489b8683d1b10ecad0a7691949a4ae7ffee74bd2 2ae022031e47b9ebed5b90f6d51cd05e6f53bdc59f5d6d754aff14a88a6e8659b5fdad501] PUSHDATA(33) [038cc8c907b29a58b00f8c2590303bfc93c69d773b9da204337678865ee0cafadb] ,Sequence =0xFFFFFFFF	Value=29910240 PkScript= OP_DUP OP_HASH160 PUSHDATA(20)b5407cec767317d41442aab35bad2712626e1 7ca OP_EQUALVERIFY OP_CHECKSIG
PreviousOutPoint={ TxHash:24f284aed2b9dbc19f0d435b1fe1ee3b3ddc763f28ca28bad798d22b6bea0c66, OutIndex:1} SignatureScript =NULL,Sequence =0xFFFFFFFF	Value=120000000 PkScript= OP_DUP OP_HASH160 PUSHDATA(20)be09abcbfda1f2c26899f062979ab0708731235 a OP_EQUALVERIFY OP_CHECKSIG

Figure 3 The length of ECDSA algorithm signature is up to 72 bytes

Take the UTXO with 2 inputs and 2 outputs in the picture as an example, the part selected in the red box is the ECDSA signature filled in the input, with a length of 72 bytes, followed by the 33-byte public key. Then after adopting Schnorr signature, the space occupied by the signature and public key can be reduced to 64 bytes and 32 bytes.

There is actually a variant of Schnorr signature that reduces the signature to 48 bytes, but as it does not support batch verification, Pieter Wuille does not recommend it.

3.4 Stronger privacy protection

Schnorr can be used to aggregate multiple keys into one. It allows transactions issued by

Bitcoin "multi-signature" wallets to display only the aggregated one, which makes multiple wallets more concise and private. In the past, when a user used a "multi-signature" wallet based on ECDSA signatures, it was easy to expose the multi-signature of the wallet because it had to show multiple public keys. However, if based on Schnorr signatures, multiple keys are aggregated off-chain, which can make a multi-signature transaction look the same as a normal transaction (ie, a single-signature transaction).

Again with the "2 of 3" multi-signature example above, the public keys of the two parties who provided the signature have been exposed. However, if Schnorr aggregated signature is used, the public key is also aggregated into one, so that it will not reveal which two parties participated in the multi-signature. The multi-signature after aggregation does not even look different from a normal "single-signature", which means that the outside world does not even know that this is a multi-signature. This greatly protects the privacy of multi-signature participants.

3.5 Signatures can be verified in batches to improve verification efficiency

Schnorr signatures, due to their linear feature, can naturally support batch verification. In fact, the principle is not complicated. The verification process of Schnorr signature is to judge whether the equation $s \cdot G=R+e \cdot P$ is true. We can bring $s=r+ex$, $R=r \cdot G$, $P=x \cdot G$ into the previous equation, then it becomes$(r+ex) \cdot G=r \cdot G+ex \cdot G$, according to the distributive law of multiplication , it can be easily seen that the equation holds. And batch verification, when there are n such equations of $s_1 \cdot G=R_1+e_1 \cdot P_1$, ……, $s_n \cdot G=R_n+e_n \cdot P_n$ need to be verified, we can add up all the left sides and all the right sides of them, so that we only need to verify whether the equation is true once, and in this way we can verify whether all the n signatures are valid.

In addition, when verifying n equations, the calculation of $s_1 \cdot G$, $s_2 \cdot G$, ……, $s_n \cdot G$ required n multiplications, but now it can be combined into only n-1 additions and 1 multiplication, which greatly improves the verification efficiency.

The linear feature of Schnorr signatures is natural, so even signatures from different users, different Tx, and even different blocks can be combined for batch verification. A new full node needs to do a lot of verification work when synchronizing block data. If Bitcoin uses Schnorr signatures, batch verification can significantly improve the synchronization speed of full nodes.

3.6 Some shortcomings

All of the above are the advantages of Schnorr signatures. In fact, these benefits come at a price. Because of the characteristic of Schnorr aggregating private key signatures, it requires multiple rounds of interaction between the participants, which is more troublesome than the past ECDSA. Moreover, it has relatively high requirements for random numbers. It is necessary to ensure that random numbers are not easy to be guessed by attackers. Some traditional pseudo-random number generation methods are not necessarily suitable. At the same time, calculating these signatures and random numbers is relatively cumbersome, so it will cause a slight delay in the step of sending transactions and require the PC to consume more computing bandwidth resources. But with current technology, these problems can be solved and overcome to a certain extent.

In addition, the Schnorr signature is not anti-quantum computing with regard to the anti-quantum computing problem that the industry is more concerned about. In the future, if quantum computing makes breakthrough progress, Bitcoin may need to continue to replace or upgrade Schnorr signatures, and may even undergo a hard fork upgrade.

6. Summary

Compared with ECDSA, Schnorr signature is more secure and credible, and by the way, it also brings the expansion of the space on the Bitcoin chain, which makes the performance of Bitcoin slightly improved. At the same time, Schnorr signature can also protect the privacy of participants in multi-signature, lightning network and other transactions, and can play a greater role combined with Taproot.

The proposal was promoted by members of the Core group for a mild upgrade in the form of soft fork. At present, the probability of smooth activation in the future is very high. It is expected that Schnorr signatures can bring more fresh technical vitality to Bitcoin and the blockchain world.

References

[1]https://github.com/bitcoin/bitcoin/pull/19953

[2]BIP 340: https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki

[3]BIP 341: https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki

[4]BIP 342: https://github.com/bitcoin/bips/blob/master/bip-0342.mediawiki

[5]David Pointcheval, Security Arguments for Digital Signatures and Blind Signature

[6]Yannick Seurin, On the Exact Security of Schnorr-Type Signatures in the Random Oracle Model

About Huobi Blockchain Research Institute

Huobi Blockchain Application Research Institute (referred to as "Huobi Research Institute") was established in April 2016. Since March 2018, it has been committed to comprehensively expanding the research and exploration of various fields of blockchain. As the research object, the research goal is to accelerate the research and development of blockchain technology, promote the application of blockchain industry, and promote the ecological optimization of the blockchain industry. The main research content includes industry trends, technology paths, application innovations in the blockchain field, Model exploration, etc. Based on the principles of public welfare, rigor and innovation, Huobi Research Institute will carry out extensive and in-depth cooperation with governments, enterprises, universities and other institutions through various forms to build a research platform covering the complete industrial chain of the blockchain. Industry professionals provide a solid theoretical basis and trend judgments to promote the healthy and sustainable development of the entire blockchain industry.

Contact us:

Consulting email:	huobiresearch@huobi.com
Official website:	http://research.huobi.cn
WeChat Subrsciption:	HuobiCN
Jianshu	Huobi Blockchain Research Institute
Sina Weibo:	Huobi Blockchain Research Institute https://www.weibo.com/u/6690456123
Twitter:	@Huobi_Research https://twitter.com/Huobi_Research
Medium:	Huobi Research https://medium.com/@huobiresearch

Welcome to join the research exchange group of the Institute

Scan code to add our learning assistant

Disclaimer

1. The author of this report and his organization do not have any relationship that affects the objectivity, independence, and fairness of the report with other third parties involved in this report.

2. The information and data cited in this report are from compliance channels. The sources of the information and data are considered reliable by the author, and necessary verifications have been made for their authenticity, accuracy and completeness, but the author makes no guarantee for their authenticity , accuracy or completeness.

3. The content of the report is for reference only, and the facts and opinions in the report do not constitute business, investment and other related recommendations. The author does not assume any responsibility for the losses caused by the use of the contents of this report, unless clearly stipulated by laws and regulations. Readers should not only make business and investment decisions based on this report, nor should they lose their ability to make independent judgments based on this report.

4. The information, opinions and inferences contained in this report only reflect the judgments of the researchers on the date of finalizing this report. In the future, based on industry changes and data and information updates, there is the possibility of updates of opinions and judgments.

5. The copyright of this report is only owned by Huobi Blockchain Research Institute. If you need to quote the content of this report, please indicate the source. If you need a large amount of reference, please inform in advance (see "About Huobi Blockchain Research Institute" for contact information), and use it within the allowed scope. Under no circumstances shall this report be quoted, deleted or modified contrary to the original intent.