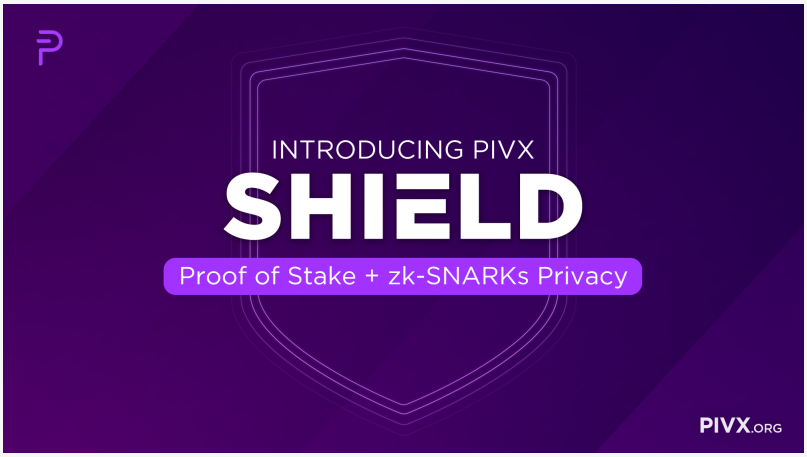
Introducing SHIELD: PIVX's Cutting Edge User Data Protection And Privacy Protocol

SHIELD is the world's first zk-SNARKs based privacy protocol on a Proof of Stake blockchain, brought to you by PIVX.



Introducing PIVX SHIELD - Privacy meets proof of stake

USA, November 10, 2020 /EINPresswire.com/ -- Since its inception in January of 2016, PIVX has continually strived for, built, and delivered superior blockchain applications that protect users' data. These User Data Protection Protocols (UDP) maintain the privacy and security of various elements in the Proof-of-Stake segment of blockchain technology. Starting with coin-join, it pivoted to a novel (and crypto-first) implementation of the Zerocoin protocol in 2018. While this integration provided robust privacy, the protocol had its limitations and ultimately had to be retired.

> PIVX is consistently implementing new code architectures and improvements. SHIELD is yet another major milestone in PIVX's rich legacy of pioneering proof of stake privacy and protecting users' data."
>
> *Furzy, Core PIVX Developer*

Today, we are excited to introduce SHIELD; a monumental leap forward in user data protection. This announcement comes as a result of PIVX's research and successful custom implementation of the highly vetted and academically proven zk-SNARK Sapling protocol, initially developed by the Electric Coin Company.

SHIELD stands for just that: A SHIELD. When using PIVX's user data protection feature, you can rest confidently that PIVX, whose logo and brand is a shield in and unto itself, is, in fact, being that SHIELD for you in the world, protecting your rights, preserving your privacy, and keeping your financial and self-identifiable information, protected.

SHIELD: PRIVACY MADE SIMPLE AND EFFICIENT

SHIELD also represents the “type” of protection that is afforded to users: No longer do you have to go through an arduous, tech-intensive process. Rather, through the simplicity of selecting a “shielded” address, you can send or receive with the confidence that your data, and financial records, are protected.

New PIVX logo

This also means you are free to spend ANY amount you like completely secured and protected. Your full balance is available for transacting privately at a moment’s notice, anytime you wish. There is no preparation time or separate balances of “private” or “public” coins.

SHIELD provides complete user data protection for your transactions; preserving the invisibility of transaction details from the sender to the receiver, the amount of the transaction, and balances.

SHIELD: SUPERIOR PERFORMANCE

SHIELD provides the end-user with a robust and fast transaction experience - it’s lightweight proofs are as small as 144 bytes, and can be generated in seconds even on a low powered computing device like a Raspberry Pi. With such efficient proofs comes actual Practical Transaction Speeds. Users can enjoy shielded transactions in almost an instant fashion: Transactions take <500ms to generate, and 1/100ths of a second to verify.

SHIELD: COMPLETE USER DATA PROTECTION AND PRIVACY WHERE AND WHEN IT MATTERS, WHENEVER YOU WANT

SHIELD hides both the sender and receiver's data, as well as the transaction value. You have full control of when, and to whom, you’d like to keep your information hidden. However, you also will always have the ability to grant permission to view transaction details on a case by case basis at any time in the future through your own viewing keys.

UNRIVALED PROTECTION

As many projects have experienced (especially when requiring large denomination pools of “private coins”), when privacy is opt-in, the adoption and use is often small, which puts the actual privacy of those who use the protocols in jeopardy as it makes it easier to identify those users and their funds. With SHIELD, anonymity through its shielded addresses is offered by default. However, the ability to operate in an unshielded manner (transparent) fully remains, allowing

ease for end-users to operate with exchanges.

PIVX to bring continuous advancements in the future

On February 29th, 2020 we announced that the privacy protocol that PIVX would implement was a zk-SNARKs based privacy protocol.

In less than 8 months, the core PIVX developers have delivered a fully customized integration of that protocol to testnet.

As of November 1st, regtest network testers of SHIELD successfully completed the first shielded-to-shielded transaction on a Proof of Stake network. This functionality (and a lot more) is scheduled to be available with the next major 5.0 core wallet release, targeted for release by end of year, which is < 2 months away.

In addition to SHIELD and the full integration of Sapling protocol with zk-SNARKs, PIVX has already begun planning out many additional future projects including:

- Trustless setup: Spartan/Halo/Supersonic (ongoing research)
- Anonymous light protocol research (mobile and desktop)
- Anonymous masternodes (collateral and IP)
- Anonymous voting (community governance)
- Anonymous staking (staking using zk-SNARKs)

For more information about SHIELD, please visit the PIVX website here

Bryan Doreian
PIVX
bryan@pivx.org
