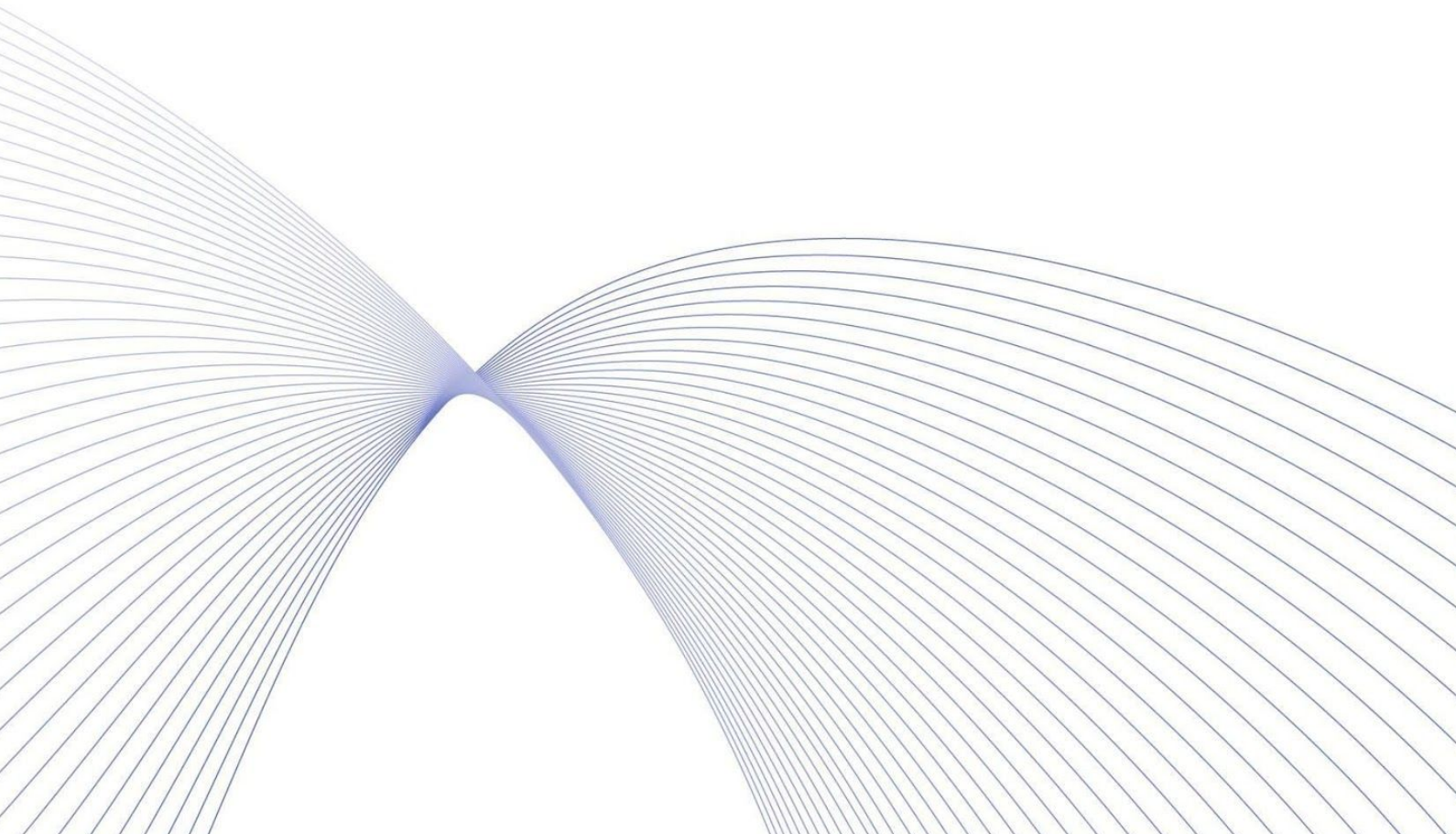
ICORATING

January 24, 2019

Private blockchains overview



While major public blockchains like Bitcoin, Litecoin or Ethereum are well-known to public, the private ones are not so famous. We will try to review the main private blockchains in the article, as well as highlight the key similarities and differences.

As its name suggests, private blockchains are the complete opposite of public blockchains. In public blockchains anyone can participate because it is open to everyone and anyone can read, write and audit information within the blockchain, however, that is not the case with private blockchains, unless one has permission to do so. In private blockchains the owner is usually a single entity, that is why it is not, in its true sense, decentralized. It is more of a distributed data ledger with embedded cryptographic protection in it. However, that is not a drawback but another concept. Private blockchain is supposed to be faster and cheaper than its public analogue, because the system does not need to spend high amounts of energy, time and money to reach consensus here. But from another point of view, it is relatively less secure and non-transparent as opposed to public blockchains.

So the main differences between public and private blockchains can be summarized as follows:

PUBLIC BLOCKCHAIN	PRIVATE BLOCKCHAIN
Almost anyone can run a full node.	Only predetermined entities may run a node or even the entity behind the blockchain runs nodes itself.
Anyone can read/access data within the blockchain.	Not anyone can read/access data or some of the data is hidden
The code is usually open-source.	The code is usually private.

Although the differences above are a good way to identify which blockchain is better suited for a specific use case, there are similarities between both types which can make it confusing to make the right choice:

- Both types of blockchain are somewhat decentralized and represent P2P distributed ledger.
- Both types contain a replica of the blockchain on each full node which gets updated with consensus.
- Both types of blockchain provide immutability, however, this may be not equal, because immutability is highly dependent on the underlying blockchain architecture.
- Both types of blockchain can be used by both enterprises and the public, however, we note that enterprises are more likely to use private ones.

A list of private blockchains under review and their main metrics is provided below:

NAME	PARENT TECHNOLOGY	CONSENSUS	TRANSACTION STATS	NOTABLE BLOCKCHAIN METRICS	TRANSACTION VOLUMES IN THE LAST MONTH	NODE METRICS
ZCash	Bitcoin	PoW	2.5 minutes per block	The total amount of addresses is circa 3 million. 13.5% of transactions are private.	80,725 transparent ts amounting to 37,343,582 ZEC and 16,039 private ts amounting to 552,333 ZEC.	4,810 unique nodes for all time, 414 for the last month. Almost 50% of blocks mined relate to single mining pool.
Monero	Bytecoin	PoW	2 minutes per block	N/A	111,621 ts and 6 ts in block in average	The top-3 mining pools accumulate almost 72% of network hash rate
Dash	Bitcoin	PoW	2.5 minutes per block	The top-100 addresses contain 14.9% of all coins	On average, 349 ts hourly, each ts is circa 15.1 DASH.	4,886 active master nodes and 166 are inactive.
PIVX	Dash	PoS	1 minute per block	Total amount of addresses is 88,681, 34,945 of which were active last month 30% of coins are locked Top-20 addresses contain over 30% of all coins (Top-1 is 5.8%).	On average, 6,200 ts daily	1,744 master nodes
Verge	Bitcoin	PoW	0.5 minutes per block	The top-25 addresses contain 51% of all coins, top-100 contain 95.8%	N/A	N/A
Bitcoin private	Bitcoin/ZClassic	PoW	2.5 minutes per block	The top-1 address in ZClassic possesses 48,56% of all coins, top-25 – almost 73%. Since Bitcoin Private is a fork of ZClassic, we believe that the proportion is somewhat similar.	The majority of blocks contain 1 or 2 transactions	13 sponsored mining pools, 32 mining pools were confirmed by the BTCp team and 55 pools were unconfirmed.

Grin	N/A	PoW	1 minute per block	There is an alert that completing 2 chains forked at one block means that one of those will be forbidden and part of the transactions will be excluded.	687 blocks so far (the network launched on January 15th).	N/A

ZCash

The ZCash blockchain is built based on the Bitcoin blockchain, with zk-SNARK technology embedded, which allows private transactions and hides private address balances. There are two types of addresses in ZCash blockchain – private (starting with "z") and public (starting with "t"), therefore there are four types of transactions available. "Mixed", private-to-public transactions are hidden only from the private side. Private addresses may also send encrypted messages within private transactions. The owner of private addresses may also reveal information regarding his transactions to regulators and auditors, however the addresses of counterparties can not be revealed.

Despite the fact that private transactions on the ZCash blockchain represent 20% of transactions in terms of amount, in terms of volume they make up only 1.5%.

Most nodes of ZCash come from Germany (79 nodes), France (70 nodes), US (68 nodes) and China (39 nodes).

Monero

Monero is technically a Bytecoin fork which utilizes the CryptoNote protocol for one of the layers, Ring Signatures for transaction signing, Ring CT for transaction hiding and Stealth Addresses for the purpose of hiding the users' addresses. Upon creation of an address, a user receives three keys – 1 for review incoming ts and balance, 1 for sending and 1 public key. 3rd parties ken review addresses and transaction only having the review key.

The Monero team is currently developing Kovri Project which will route and ecrypt transactions using I2P nodes. This will help to hide transactors' IP addresses and provide further protection from external monitoring. In addition to the above, Monero is ASIC-resistant proof of work.

DASH

DASH is built based on Bitcoin blockchain and it has 2 different types of nodes (on the contrary to is "parent") – usual nodes and masternodes, which have the ability to privately sending and quick-sending of transactions (around 1 second). DASH uses CoinJoin protocol and utilizes I2P technology for privacy purposes.

32% of all master nodes are located in the US, 21% in the Netherlands, 13% in Lithuania, 9,1% in Germany and 4.3% in Russia.

PIVX

PIVX is based on DASH tech, so the key main features of DASH are the same, however, PIVX utilizes the PoS protocol of Zerocoin for consensus whereas DASH is PoW. The network speed of PIVX is circa 170 TPS. In addition to the above, PIVX team is globally decentralized with no central ruling company. The project is maintained by the community. The project is also claiming itself to be energy-efficient with an estimate of 1 wind turbine to fully power the network.

Verge

Verge is based on the Bitcoin blockchain with multiple layers for privacy. One of the layers is Tor for hiding IP addresses and the other is I2P, similar to Dash for privacy purposes, as well. Verge has a built-in Wraith protocol which allows choice between private and public network somewhat similar to ZCash. Verge uses a PoW protocol, however, there are 5 different mining algorithms, each of which takes 30 seconds to execute, which provides protection from 51% of attacks. The verge team also claims to support atomic swaps between blockchains that support BIP65.

There is only one block explore for Verge which contains minimum data.

Bitcoin Private

BTCp is a fork-merge of ZClassic and Bitcoin, which allows for 4 different types of transactions. BTCp utilizes ZCash's zk-SNARK tech to hide transactions. BTCp utilizes a PoW protocol similar to the one of Bitcoin Gold, therefore, having same block time. The team is currently developing the Dandelion protocol, which will improve the security of transactions.

The total supply of BTCp should have been the sum of the total BTC supply at BTCp launch date plus the total supply of ZClassic at the same date plus 62,500 BTCp under Volutary Mining Contribution Program. However, the actual amount of BTCp upon launch was higher that it should have been.

Grin (MimbleWimble)

MimbleWimble is a blockchain format and protocol which provides scalability, fungibility and privacy. Grin is an open source project which implements MimbleWimble blockchain and provides blockchain environment. Grin has privacy by default and also allows for the partial disclosure of information if need be. The Grin blockchain scale in relation to number of users and minimally in relation to the number of transactions, because of the check that each new transaction does not have any new coins, previous blocks can be removed without concern. Based on that, the Grin blockchain takes much less disk space in comparison with competitors. The blockchain itself is simply designed and easy-to-audit and maintain. The Grin blockchain utilized time-proven Elliptic Curves which have been used for decades. The Grin blockchain is developed by the community, utilized ASIC-resistant algorithm (Cuckoo Cycle) while encouraging miner decentralization. It also supports sidechains and Quantum-resistant.

Conclusion

As can be seen from above, each of the private blockchains which we have reviewed has its own features, mainly related to the privacy of the data and has its own strong and weak sides. However, we would like to note that even though blockchain technology itself is still in its early stage and the whole market is tiny when compared to other markets, private blockchain share is even tinier – even on well-known blockchains focusing on privacy (like ZCash) still have relatively low volumes of transactions when compared to their public rivals. Regardless of that, we believe that private blockchains definitely have their customers and market, therefore their development is not in vain. It is also worth noting that private blockchains implement technical solutions which have proven their relative effectiveness in privacy protection like Tor, I2P, etc. However, there is no such thing as absolute privacy and 100% anonymity, and the attacks against privacy are getting better. One should use common sense, prudence and in-depth cautiousness to keep their privacy safe.