Capricoin+

A Look Into The Future

展望未来

白皮书 v0.1

内容

1. 综述
2. 动机
3. 摘要
4. 多重隐私性
5. 隔离见证
6. 量子电阻
7. PPoS & 静态收益
8. 托管服务
9. 去中心化投票
10. 数据储存网络（DSN）
11. 共识机制兼容的可延展性
12. 通讯安全性（SMSG）
13. 隐私智能合约
14. 社区监管
15. 去中心化的隐私市场

Capricoin+

1. 综述
2. 动机
3. 摘要
4. 多重隐私性
5. 隔离见证
6. 量子电阻
7. PPoS & 静态收益
8. 托管服务
9. 去中心化投票
10. 数据储存网络（DSN）
11. 共识机制兼容的可延展性
12. 通讯安全性（SMSG）
13. 隐私智能合约
14. 社区监管
15. 去中心化的隐私市场

Since Bitcoin, which was the first implementation of the idea of a peer to peer electronic cash system proposed by Satoshi Nakamoto back in 2008, the field of crypto currencies and blockchain based systems has exploded producing thousands of different projects, technologies and research papers. Today one can find such projects ranging from distributed computing to Enterprise solutions and applied to all fields from medicine to automotive industries.

However, the basic need for people to store their money and transact in a secure way without relying on a centralized authority is still the main use case and the most important, which is one of the reasons why Bitcoin is still the top cryptocurrency and is as influential today as it was almost ten years ago.

In Bitcoin, as in most crypto currencies since, your balance is represented by a series of transactions which can be traced back to the very beginning of a blockchain. In order to trust the system we need to make sure that each transaction in a chain is valid, and to do so without relying on a centralized entity, which is the main purpose of Bitcoin nodes and miners. All participants in the system must agree, or using more professional terms “reach consensus” on an official version of the transaction history and be able to do so without trusting each other or anyone else. The ability of the system to do so is the true strength of the Bitcoin idea.

1. Summary
2. **Motivation**
3. Abstract
4. Multi-State Privacy
5. Native Segregated Witness
6. Quantum-Resistance
7. PPoS & Passive Income
8. Cold Staking
9. Decentralized Voting
10. Data Storage Networks (DSN)
11. Extensibility Protocol-Agnosticism
12. Secure Messaging (SMSG)
13. Privacy Smart-Contracts
14. Community Governance
15. Decentralized Privacy Marketplace

Capricoin+

Motivation

Initially, transactions in the Bitcoin network were believed to be anonymous. By generating random private and public key pairs, and using the public part to form an address that could be used to receive and control transactions, many Bitcoin users assumed that nothing in that process could link to their real identity. They turned out to be wrong.

Using blockchain analysis, research has shown that there are always data leaks. These can come from exchanges, merchants, OTC deals or even by collecting and clustering the blockchain data. It is then possible to deanonymize users, and since all data, including transaction amounts, is open and permanently stored in a public ledger, once users identity is known all their transactions past and future as well as their balance, become directly linked to them as a person. This situation is far from ideal. Both individuals and organizations would prefer that their transactions and balance remain confidential and could only be seen only by parties specifically authorized by them to do so. This would require limiting the visibility of transaction details and keeping as little information as possible about the transactions in the public record to prevent future analysis and a potential disclosure.

1. Summary
2. Motivation
3. **Abstract**
4. Multi-State Privacy
5. Native Segregated Witness
6. Quantum-Resistance
7. PPoS & Passive Income
8. Cold Staking
9. Decentralized Voting
10. Data Storage Networks (DSN)
11. Extensibility Protocol-Agnosticism
12. Secure Messaging (SMSG)
13. Privacy Smart-Contracts
14. Community Governance
15. Decentralized Privacy Marketplace

Abstract

This document offers an overview of the Capricoin+ platform. With an aim to give a wide picture about the eco-system we are trying to build.

Capricoin+ is a scalable privacy coin, based on a Particl fork which is based on the latest Bitcoin source with the addition of advanced features, this means it comes with a huge list of scaling and security improvements over the old Capricoin.

1. Summary
2. Motivation
3. Abstract
4. **Multi-State Privacy**
5. Native Segregated Witness
6. Quantum-Resistance
7. PPoS & Passive Income
8. Cold Staking
9. Decentralized Voting
10. Data Storage Networks (DSN)
11. Extensibility Protocol-Agnosticism
12. Secure Messaging (SMSG)
13. Privacy Smart-Contracts
14. Community Governance
15. Decentralized Privacy Marketplace

Multi-State Privacy

Privacy (being one of the very important features of this coin) is accomplished by implementing different privacy levels each with its own complexity and privacy degree, each come at a different costs as well.

Confidential Transactions(1): This type of transaction (blind transaction) uses the Confidential Transaction (CT by Gregory Maxwell) privacy protocol, this will keep the transferring amounts visible only to the transaction participants (and those they designate), while still guaranteeing the transaction's cryptographic integrity while costing a bit more than the standard transactions in fees.

RingCT(2): This type of transaction (Anon transactions) uses the RingCT privacy protocol (Described Shen Noether) to hide both transferring amounts and participants' blockchain identity by combining ring signatures and CT protocols. It is one of the highest levels of trustless privacy protocol the crypto industry has to offer and was made famous by Monero, and this cost the most in fees.

Capricoin+

1- Confidential Transactions by Greg Maxwell

2- RingCT paper Shen Noether Monero Reasearch lab

1. Summary
2. Motivation
3. Abstract
4. Multi-State Privacy
5. **Native Segregated Witness**
6. Quantum-Resistance
7. PPoS & Passive Income
8. Cold Staking
9. Decentralized Voting
10. Data Storage Networks (DSN)
11. Extensibility Protocol-Agnosticism
12. Secure Messaging (SMSG)
13. Privacy Smart-Contracts
14. Community Governance
15. Decentralized Privacy Marketplace

Native Segregated Witness

The Capricoin+ platform has deployed a native implementation of Segwit. This has the added benefit of making all transactions (including private ones) go through Segwit by default, resulting in better scalability and cheaper transaction fees. Unlike forked Segwit implementations, 100% of Capricoin+ addresses are compatible with Segregated Witness.

Segwit grants additional features to the Capricoin+ platform such as transaction malleability vulnerability protection and block capacity increase, but its most notable feature is that it renders Capricoin+'s blockchain compatible with the Lightning Network

1. Summary
2. Motivation
3. Abstract
4. Multi-State Privacy
5. Native Segregated Witness
6. **Quantum-Resistance**
7. PPoS & Passive Income
8. Cold Staking
9. Decentralized Voting
10. Data Storage Networks (DSN)
11. Extensibility Protocol-Agnosticism
12. Secure Messaging (SMSG)
13. Privacy Smart-Contracts
14. Community Governance
15. Decentralized Privacy Marketplace

Quantum-Resistance

Current Proof-of-Stake implementations have a vulnerability not present in Proof-of-Work whereby they reveal the public key of staking addresses when they find and sign blocks. The most dangerous attack by quantum computers is against public key cryptography. On traditional computers, it takes on the order of 2128 basic quantum operations to get Bitcoin private keys associated with Bitcoin public keys. This number is so massively large that any attack using traditional computers is completely impractical. However, it is known for sure that it would take a sufficiently large quantum computer on the order of only 1283 basic quantum operations to be able to break a Bitcoin key using Shor's algorithm. This might take some time, especially since the first quantum computers are likely to be extremely slow, but it is still very practical. It could be estimated that it is maybe 2 to 5 years until quantum computers become an issue, but any project that plans on staying relevant on a long period of time should tackle these vulnerabilities way before they become problematic.

It is worth mentioning that public keys are NOT public addresses. To reverse a private key from a public address, it would require more energy than what is available in the universe, therefore a quantum hacker cannot just go pick public addresses with large amounts and reverse those.
When a Capricoin+ block is staked from a cold staking node, the private key of the address on the staking node (which contains no coin) is broadcasted to the network instead of the private key of the address which contains the staking funds. Because cold staking nodes are able to sign staked blocks on behalf of any wallet, hot or cold, cold stakers can effectively remain anonymous and shielded from theoretical quantum computer attacks.

1. Summary
2. Motivation
3. Abstract
4. Multi-State Privacy
5. Native Segregated Witness
6. Quantum-Resistance
7. **PPoS & Passive Income**
8. Cold Staking
9. Decentralized Voting
10. Data Storage Networks (DSN)
11. Extensibility Protocol-Agnosticism
12. Secure Messaging (SMSG)
13. Privacy Smart-Contracts
14. Community Governance
15. Decentralized Privacy Marketplace

PPoS & Passive Income

Particl proof of stake is built and improved upon the popular PoS3 protocol on top of which were added several security and utility features.

PPoS can serve as a great passive income tool. It rewards stakers a minmum rate of 2%. This staking reward rate is true if 100% of the total supply is put up for staking, but gets higher as less coins are being staked. For example, if 50% of the total network is being put up for staking, the staking reward rate would be of 4%.

The Capricoin+ platform also redirects any fee generated from it directly to stakers, including but not limited to currency transactions, extended messaging, privacy balance transfers and others, meaning staking becomes more profitable as the platform gets more traffic.

1. Summary
2. Motivation
3. Abstract
4. Multi-State Privacy
5. Native Segregated Witness
6. Quantum-Resistance
7. PPoS & Passive Income
8. **Cold Staking**
9. Decentralized Voting
10. Data Storage Networks (DSN)
11. Extensibility Protocol-Agnosticism
12. Secure Messaging (SMSG)
13. Privacy Smart-Contracts
14. Community Governance
15. Decentralized Privacy Marketplace

Cold Staking

Cold staking is enabled by smart-contract functionality and lets users securely delegate staking powers to "staking nodes" and "staking pools" which contain no coin. The purpose of these "staking nodes" is to provide a dedicated resource connected to the Capricoin+ blockchain and stake on behalf of another wallet without being able to spend its coins.

Cold staking nodes are intended to be used in combination with cold, hardware and multisig addresses, making it possible to stake "offline" coins with no risk of being hacked or exposing your public key to the network. Staking nodes can be set up on any device, secure or not, such as public/cloud servers, virtual machines or DSDs.

1. Summary
2. Motivation
3. Abstract
4. Multi-State Privacy
5. Native Segregated Witness
6. Quantum-Resistance
7. PPoS & Passive Income
8. Cold Staking
9. **Decentralized Voting**
10. Data Storage Networks (DSN)
11. Extensibility Protocol-Agnosticism
12. Secure Messaging (SMSG)
13. Privacy Smart-Contracts
14. Community Governance
15. Decentralized Privacy Marketplace

Decentralized Voting

Integrated into PPoS is a blockchain voting system that can be used by any Capricoin+ users to poll others or vote. This tool allows the platform's community to provably reach consensus and better coordinate itself.

Polls run for a desired number of blocks and each staked block is a voting ticket, meaning the more blocks a staker finds, the more of his votes are registered. A staker can vote for any number of polls and they will all receive one vote for the selected option once the staker finds a block.

Embedding voting into PPoS means people who do not have any stake in the platform can't vote, leaving the decisional power entirely up to the community of users.

1. Summary
2. Motivation
3. Abstract
4. Multi-State Privacy
5. Native Segregated Witness
6. Quantum-Resistance
7. PPoS & Passive Income
8. Cold Staking
9. Decentralized Voting
10. **Data Storage Networks (DSN)**
11. Extensibility Protocol-Agnosticism
12. Secure Messaging (SMSG)
13. Privacy Smart-Contracts
14. Community Governance
15. Decentralized Privacy Marketplace

Data Storage Networks

Data Storage Networks are used on Capricoin+ to store any data (i.e. marketplace-related data such as images) off-chain. This allows the platform to scale well regardless of the amount of data it uses.

DSN is a generic term that describes a specific set of software with the purpose of storing and retrieving data on the internet. The usage of the term DSN is simply a layer of abstraction as it is not required to know how a specific DSN works internally as long as it can store blobs of data and later retrieve them using a comparable cryptographic identifier. Popular DSN include BitMessage, IPFS, SMSG, HTTPs, TOR, and etc.

A small hash of the hosted content is created and stored on the Capricoin+ blockchain when it is used to store data on a DSN. To verify the integrity of data when it is retrieved back from the DSN, its hash is recomputed and compared with the one stored on the Capricoin+ blockchain. The data is considered trusted if the hashes match, and rejected by the platform if they don't.

1. Summary
2. Motivation
3. Abstract
4. Multi-State Privacy
5. Native Segregated Witness
6. Quantum-Resistance
7. PPoS & Passive Income
8. Cold Staking
9. Decentralized Voting
10. Data Storage Networks (DSN)
11. **Extensibility Protocol-Agnosticism**
12. Secure Messaging (SMSG)
13. Privacy Smart-Contracts
14. Community Governance
15. Decentralized Privacy Marketplace

Extensibility Protocol-Agnosticism

Technology moves at an exponential rate, and the very few protocols that survive the test of time are all designed with extensibility in mind. A protocol looking to be relevant on a long enough timeline should be both robust and flexible enough that it easily allows any developer to securely expand it. The development of data storage networks (DHTs, BitTorrent, IPFS) and blockchain solutions is still young, there aren't any clear "winners" that meet all criteria nor may there ever be, thus the protocol must accommodate for it.

Capricoin+'s way to deal with this reality is with the protocol agnosticism built at its core. The platform is indeed designed to be able to interact and exchange data with any DSN rather than using the same hard-coded DSN everytime regardless of context or user preference.

1. Summary
2. Motivation
3. Abstract
4. Multi-State Privacy
5. Native Segregated Witness
6. Quantum-Resistance
7. PPoS & Passive Income
8. Cold Staking
9. Decentralized Voting
10. Data Storage Networks (DSN)
11. Extensibility Protocol-Agnosticism
12. **Secure Messaging (SMSG)**
13. Privacy Smart-Contracts
14. Community Governance
15. Decentralized Privacy Marketplace

Capricoin+

Secure Messaging

Secure Messaging (SMSG) is Capricoin's very own DSN, it is a decentralized P2P message mixnet where all nodes store a copy of everyone's end-to-end encrypted messages and data for a duration of 48 hours (which can be increased for a fee). It is the default and most private DSN available for use on the platform. The reference implementation is developed in C++ and incorporated into the Capricoin+'s daemon, allowing it to operate over the same peer to peer network as the Capricoin+ blockchain.

All nodes continuously attempt to decrypt every incoming message, but can only succeed if the node is able to recalculate the HMAC hash accompanying said message. If the hash check fails, then it can not be decrypted by the node, which means the message was either fraudulent, tampered with or meant for another node. SMSG messages and data are stripped from almost any metadata, therefore it is impossible for anyone to extract information such as IP addresses, sender or receiver. The only metadata accompanying data on SMSG are the hash, the encryption payload and a temporary public key.

1. Summary
2. Motivation
3. Abstract
4. Multi-State Privacy
5. Native Segregated Witness
6. Quantum-Resistance
7. PPoS & Passive Income
8. Cold Staking
9. Decentralized Voting
10. Data Storage Networks (DSN)
11. Extensibility Protocol-Agnosticism
12. Secure Messaging (SMSG)
13. **Privacy Smart-Contracts**
14. Community Governance
15. Decentralized Privacy Marketplace

Capricoin+

Privacy Smart-Contracts

While not turing-complete, Capricoin+ is still able to deploy secure and complex smart-contracts. Good examples include the planned Capricoin+ marketplace (coming in Q3 2020), the MAD escrow mechanism and cold staking. Any developer can deploy their own Dapp on Capricoin+ and use the CT and RingCT privacy protocols to make contracts that natively respect users' rights to privacy.

1. Summary
2. Motivation
3. Abstract
4. Multi-State Privacy
5. Native Segregated Witness
6. Quantum-Resistance
7. PPoS & Passive Income
8. Cold Staking
9. Decentralized Voting
10. Data Storage Networks (DSN)
11. Extensibility Protocol-Agnosticism
12. Secure Messaging (SMSG)
13. Privacy Smart-Contracts
14. **Community Governance**
15. Decentralized Privacy Marketplace

Community Governance

Keeping decentralization in mind, Particl is governed by its community of stakers rather than the team or a third-party. Since the coming marketplace is going to be fully anonymous, it is not unlikely that undesirable items and services would be listed for sale so their must be a way to moderate the marketplace in order to preserve its legitimacy and for it to not be an enabler of immoral or illegal businesses and activities. Having a third-party be nominated as moderator introduces a whole lot of issues such as legal liability, centralization of power and lack of scalability.

1. Summary
2. Motivation
3. Abstract
4. Multi-State Privacy
5. Native Segregated Witness
6. Quantum-Resistance
7. PPoS & Passive Income
8. Cold Staking
9. Decentralized Voting
10. Data Storage Networks (DSN)
11. Extensibility Protocol-Agnosticism
12. Secure Messaging (SMSG)
13. Privacy Smart-Contracts
14. Community Governance
15. **Decentralized Marketplace**

Decentralized Marketplace

Capricoin+'s decentralized marketplace is going to be a highly scalable and secure solution for e-commerce. Built with privacy at its core, it will use several platform-wide features to deliver the full suite of tools required to shop and sell products and services online.

The marketplace will be built with privacy at its core, meaning that all transactions between buyers and vendors are fungible (untraceable and private). To achieve this feat, many privacy solutions are deployed such as CT escrow smart-contract, IP obfuscation, encrypted messaging and metadata leak protection.

Decentralized Escrow: As buyers and vendors do not know and trust each other, there is no protection against one of the party never honoring their end of the trade unless a mechanism is put in place. One common solution marketplaces and payment processors implement on their platforms is the use of a mutually-trusted third party (usually the platform provider itself) as "escrow agent". However, not only does this represents a scalability and privacy problem but it also does not offer any protection against collusion between the escrow agent and one of the party. Capricoin+, being a fully decentralized solution, solves this problem without the need for a third party by using what is called MAD escrow smart-contracts. This type of escrow does not require any fee to be paid.

Game Theory: Mutually Assured Destruction (MAD) is a doctrine of military strategy and national security policy in which a full-scale use of nuclear weapons by two or more opposing sides would cause the complete annihilation of both the attacker and the defender, thus making their use not an option.

- Particl decentralized private marketplace paper
- Open Market Protocol (OMP)

It is based on the theory of deterrence and the Nash Equilibrium, which holds that the threat of using strong weapons against the enemy prevents the enemy's use of those same weapons. The strategy is a form of Nash equilibrium in which, once armed, neither side has any incentive to initiate a conflict or to disarm. Capricoin+'s MAD escrow mechanism replaces the nuclear annihilation deterrence factor of the MAD game theory for a mutual financial loss should one party acts dishonestly.

1. Summary
2. Motivation
3. Abstract
4. Multi-State Privacy
5. Native Segregated Witness
6. Quantum-Resistance
7. PPoS & Passive Income
8. Cold Staking
9. Decentralized Voting
10. Data Storage Networks (DSN)
11. Extensibility Protocol-Agnosticism
12. Secure Messaging (SMSG)
13. Privacy Smart-Contracts
14. Community Governance
15. **Decentralized Marketplace**

How It Works: Capricoin+ uses the BIP 65 opcode to enable MAD escrow contracts by locking funds in a secure multi-signature address until all of the parties sign off on the transaction.

The seller starts by depositing an amount they want the buyer to match to symbolize a virtual handshake. This could be between 0 and 100 percent of the item's purchase price, but optimal MAD odds are achieved when the insurance deposit equals 100 percent of the item's purchase price. The buyer then deposits an amount equal to the handshake amount plus the price of the item they are buying. The escrowed funds are not released to any party until both confirm that the transaction has been completed satisfactorily. To avoid filibustering, the MAD smart-contract has a timer that runs for a pre-determined duration of time (which can be extended if both parties agree) after which funds are destroyed/burned (forever locking them for both parties with no option to unlock). This prevents both parties from willingly delaying and hindering the escrow process.

When both parties are satisfied with the outcome of the transaction, they are required to confirm the transaction as completed. When this is done, the item's escrowed funds are released to the vendor and the insurance deposit is refunded to both parties at no fee.

1. Summary
2. Motivation
3. Abstract
4. Multi-State Privacy
5. Native Segregated Witness
6. Quantum-Resistance
7. PPoS & Passive Income
8. Cold Staking
9. Decentralized Voting
10. Data Storage Networks (DSN)
11. Extensibility Protocol-Agnosticism
12. Secure Messaging (SMSG)
13. Privacy Smart-Contracts
14. Community Governance
15. **Decentralized Marketplace**

Capricoin+

Privacy: Capricoin+'s MAD escrow system renders the marketplace fully fungible as it makes all transactions untraceable by default. In fact, not only is the entire marketplace content encrypted at the DSN level, but all currency transactions are rendered untraceable through the use of the Confidential Transaction (CT). This is achieved by making the MAD escrow smart-contract only work with CT and forcing all transactions to have to go through it. This technique enhances privacy much more than if CT MAD escrow was optional, as it makes all marketplace transactions equally the same (fungible).

Another privacy-enhancing aspect of the MAD escrow mechanism is its lack of third-party acting as escrow agent. In fact, in most arbitrated escrow system, both parties need to keep their discussion in the same environment as the arbitrator., effectively exposing every detail of the deal. This is so the escrow agent can step in if any problem arises and issue a resolution based on the context. This involves a lot of trust in the arbitrator and assumes it is honest. By not requiring any third-party.

Private Listings: While public listings can be moderated out of the marketplace by the Capricoin+ community, private listings cannot. Private listings are a private form of listing that can only be accessed by users' in possession of its access key. It is not possible to find these listings on the public side of the marketplace.

Anti-Spam Listing Fee: Spam is a problem which all networks are exposed to. To mitigate this possibility on the Capricoin+ marketplace, two measures are deployed: a listing fee and a payment renewal requirement.

Marketplace Data Storage: The marketplace data is stored off-chain on DSNs. The default DSN on Capricoin+ is SMSG, and it is also the one with the best privacy specifications. Storing marketplace data off-chain allows the Capricoin+ platform scale better without bloating its blockchain or centralizing nodes with masternodes. Content uploaded on most types of DSNs produce a small hash that can be stored on the Capricoin+ blockchain. This hash must match the hash of the content once it is retrieved from the DSN at a later time. If it does not, the content is considered fraudulent and is rejected by the Particl platform.