



# DarkPayCoin

Darkpaper v1 - 2018



# DarkPay Introduction

Crypto-currencies were initially created in order to fulfill three purposes:

Privacy, decentralization and real world usage.

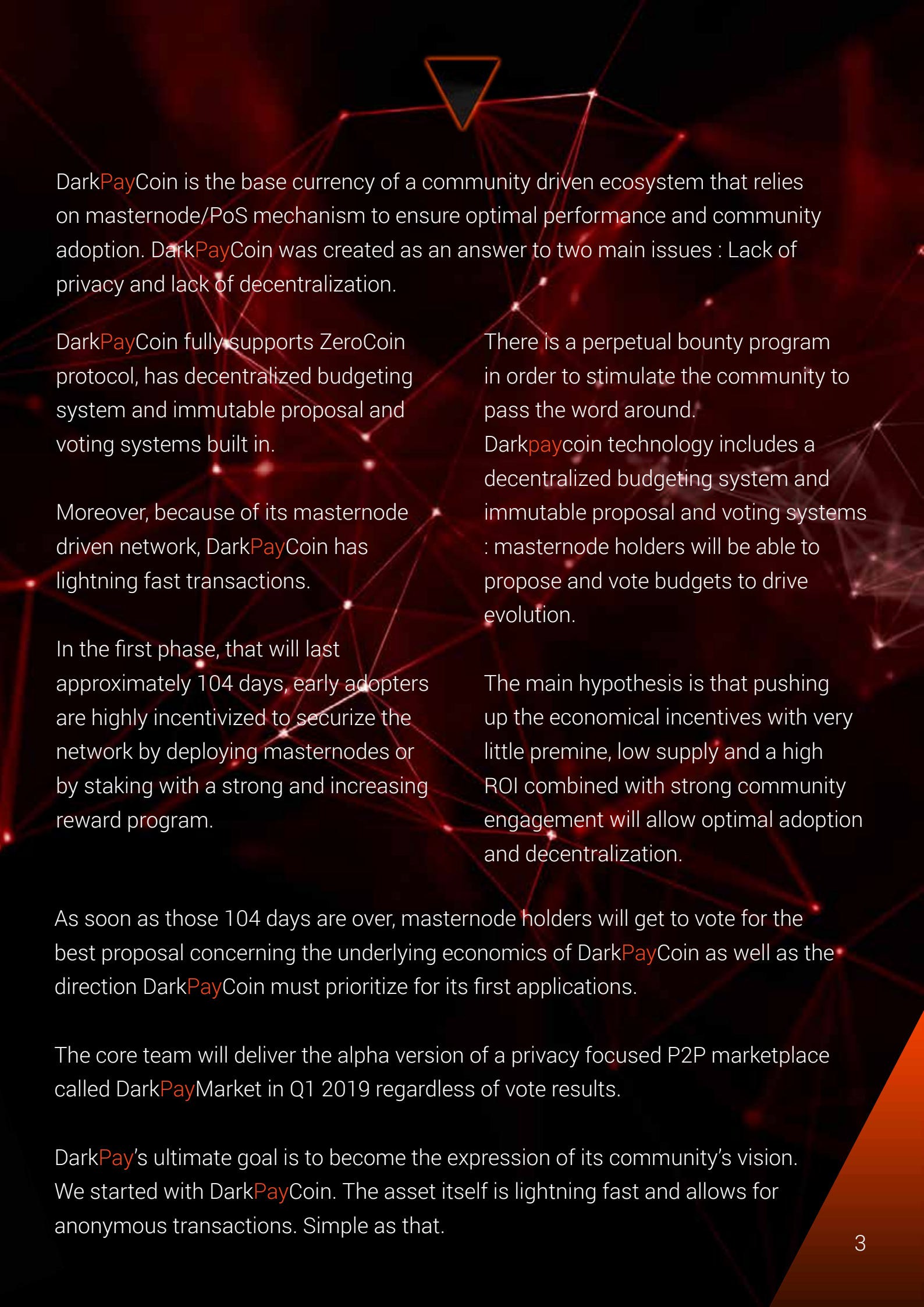
As they became more mainstream over the past few years the highly speculation driven market allowed for incredibly overvalued projects to sell empty promises for billions of dollars.

In today's market we trade centralized assets for speculative purposes on over-centralized platforms that require the user to go through a KYC. On the other hand, as our global economy is showing signs of collapse Crypto-currencies have proven to be valuable assets in real life, as in Venezuela or Zimbabwe where people suffered from centralized money issuance.

It's not a bold statement to say that the initial drive of this technology is irrelevant in today's market.

This is the reason why we decided, first as a small team, and now as an already strong community to create our ecosystem, but first, let's take a look back at our project's inception.





DarkPayCoin is the base currency of a community driven ecosystem that relies on masternode/PoS mechanism to ensure optimal performance and community adoption. DarkPayCoin was created as an answer to two main issues : Lack of privacy and lack of decentralization.

DarkPayCoin fully supports ZeroCoin protocol, has decentralized budgeting system and immutable proposal and voting systems built in.

Moreover, because of its masternode driven network, DarkPayCoin has lightning fast transactions.

In the first phase, that will last approximately 104 days, early adopters are highly incentivized to securize the network by deploying masternodes or by staking with a strong and increasing reward program.

There is a perpetual bounty program in order to stimulate the community to pass the word around.

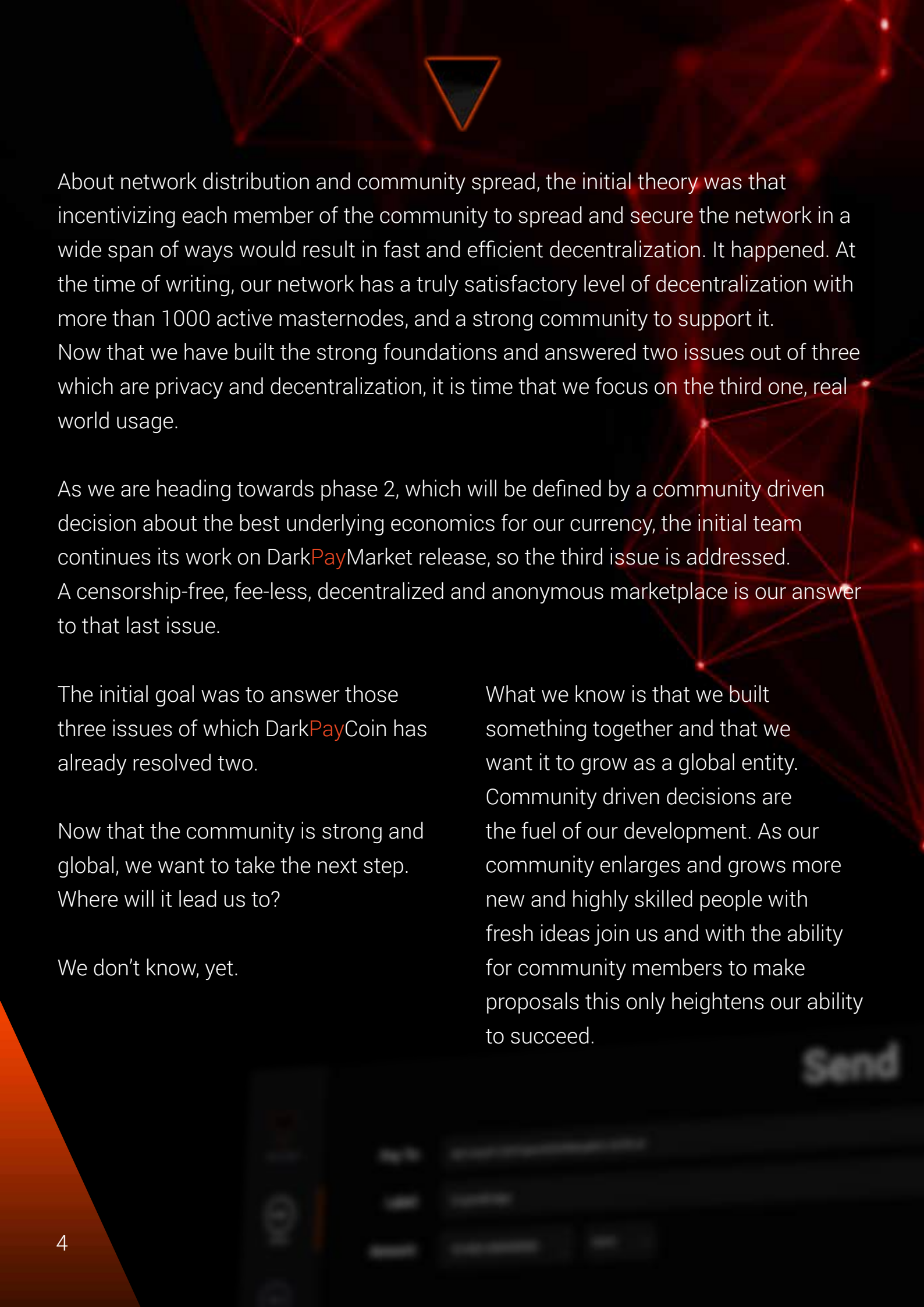
Darkpaycoin technology includes a decentralized budgeting system and immutable proposal and voting systems : masternode holders will be able to propose and vote budgets to drive evolution.

The main hypothesis is that pushing up the economical incentives with very little premine, low supply and a high ROI combined with strong community engagement will allow optimal adoption and decentralization.

As soon as those 104 days are over, masternode holders will get to vote for the best proposal concerning the underlying economics of DarkPayCoin as well as the direction DarkPayCoin must prioritize for its first applications.

The core team will deliver the alpha version of a privacy focused P2P marketplace called DarkPayMarket in Q1 2019 regardless of vote results.

DarkPay's ultimate goal is to become the expression of its community's vision. We started with DarkPayCoin. The asset itself is lightning fast and allows for anonymous transactions. Simple as that.



About network distribution and community spread, the initial theory was that incentivizing each member of the community to spread and secure the network in a wide span of ways would result in fast and efficient decentralization. It happened. At the time of writing, our network has a truly satisfactory level of decentralization with more than 1000 active masternodes, and a strong community to support it. Now that we have built the strong foundations and answered two issues out of three which are privacy and decentralization, it is time that we focus on the third one, real world usage.

As we are heading towards phase 2, which will be defined by a community driven decision about the best underlying economics for our currency, the initial team continues its work on DarkPayMarket release, so the third issue is addressed. A censorship-free, fee-less, decentralized and anonymous marketplace is our answer to that last issue.

The initial goal was to answer those three issues of which DarkPayCoin has already resolved two.

Now that the community is strong and global, we want to take the next step. Where will it lead us to?

We don't know, yet.

What we know is that we built something together and that we want it to grow as a global entity. Community driven decisions are the fuel of our development. As our community enlarges and grows more new and highly skilled people with fresh ideas join us and with the ability for community members to make proposals this only heightens our ability to succeed.

Send



# Current Technology

## PROOF OF STAKE

Proof of Stake is a proposed alternative to Proof of Work. Like proof of work, proof of stake attempts to provide consensus and double-spend prevention. With Proof of Work, the probability of mining a block depends on the work done by the miner (e.g. CPU/GPU cycles spent checking hashes). With Proof of Stake, the resource that's compared is the amount of Bitcoin a miner holds - someone holding 1% of the Bitcoin can mine 1% of the "Proof of Stake blocks".

Some argue that methods based on Proof of Work alone might lead to a low network security in a cryptocurrency with block incentives that decline over time (like bitcoin) due to Tragedy of the Commons, and Proof of Stake is one way of changing the miner's incentives in favor of higher network security.

## MOTIVATION FOR PROOF OF STAKE

A proof-of-stake system might provide increased protection from malicious attacks on the network. Additional protection comes from two sources:  
Executing an attack would be much more expensive.

Reduced incentives for attack. The attacker would need to own a near majority of all Bitcoin. Therefore, the attacker would suffer severely from his own attack.

When block rewards are produced through txn fees, a proof of stake system would result in lower equilibrium txn fees. Lower long-run fees would increase the competitiveness of Bitcoin relative to alternative payments systems. Intuitively reduced fees are due to vast reductions in the scale of wastage of resources.





## THE MONOPOLY PROBLEM

If a single entity (hereafter a monopolist) took control of the majority of txn verification resources, he could use these resources to impose conditions on the rest of the network.

Potentially, the monopolist could choose to do this in malicious ways, such as double spending or denying service. If the monopolist chose a malicious strategy and maintained his control for a long period, confidence in bitcoin would be undermined

and bitcoin purchasing power would collapse. Alternatively, the monopolist could choose to act benevolently.

A benevolent monopolist would exclude all other txn verifiers from fee collection and currency generation, but would not try to exploit currency holders in any way. In order to maintain a good reputation, he would refrain from double spends and maintain service provision. In this case, confidence in Bitcoin could be maintained under monopoly since all

of its basic functionality would not be affected.

Both benevolent and malevolent monopoly are potentially profitable, so there are reasons to suspect that an entrepreneurial miner might attempt to become a monopolist at some point.

Due to the Tragedy of the Commons effect, attempts at monopoly become increasingly likely over time.





## HOW PROOF OF STAKE ADDRESSES MONOPOLY PROBLEMS

Monopoly is still possible under proof-of-stake. However, proof-of-stake would be more secure against malicious attacks for two reasons.

Firstly, proof-of-stake makes establishing a verification monopoly more difficult. At the time of writing, an entrepreneur could achieve monopoly over proof-of-work by investing at most 10 million USD in computing hardware. The actual investment necessary might be less than this because other miners will exit as difficulty increases, but it is difficult to predict exactly how much exit will occur. If price remained constant in the face of extremely large purchases (unlikely), such an entrepreneur would need to invest at least 20 million USD to obtain monopoly under proof-of-stake.

Since such a large purchase would dramatically increase bitcoin price, the entrepreneur would likely need to invest several times this amount. Thus, even now proof-of-stake monopoly would be several-fold more costly to achieve than proof-of-work monopoly.

Over time the comparison of monopoly costs will become more and more dramatic. The ratio of bitcoin's mining rewards to market value is programmed to decline exponentially.





As this happens, proof-of-work monopoly will become easier and easier to obtain, whereas obtaining proof-of-stake monopoly will become progressively more difficult as more of the total money supply is released into circulation.

Secondly, and perhaps more importantly, a proof-of-stake monopolist is more likely to behave benevolently exactly because of his stake in Bitcoin. In a benevolent monopoly, the currency txn continue as usual, but the monopolist earns all txn fees and coin generations. Other txn verifiers are shut out of the system, however. Since mining is not source of demand for bitcoin, bitcoin might retain most of its value in the event of a benevolent attack. Earnings from a benevolent attack are similar regardless of whether the attack occurs under proof-of-stake or proof-of-work. In a malicious attack, the attacker has some outside opportunity which allows profit from bitcoin's destruction (simple double-spends are not a plausible motivation; ownership of a competing payment platform is).

At the same time, the attacker faces costs related to losses on bitcoin-specific investments which are necessary for the attack. It can be assumed that a malicious attack causes the purchasing power of bitcoin to fall to zero. Under such an attack, the proof-of-stake monopolist will lose his entire investment.

By contrast, a malicious proof-of-work monopolist will be able to recover much of their hardware investment through resale.

Recall also, that the necessary proof-of-work investment is much smaller than the proof-of-stake investment. Thus, the costs of a malicious attack are several-fold lower under proof-of-work. The low costs associated with malicious attack make a malicious attack more likely to occur.





## Why Proof of Stake Would Likely Decrease Long-run Txn Fees Considerably

In a competitive market equilibrium, the total volume of txn fees must be equal to opportunity cost of all resources used to verify txns. Under proof-of-work mining, opportunity cost can be calculated as the total sum spent on mining electricity, mining equipment depreciation, mining labor, and a market rate of return on mining capital. Electricity costs, returns on mining equipment, and equipment depreciation costs are likely to dominate here. If these costs are not substantial, then it will be exceptionally easy to monopolize the mining network. The fees necessary to prevent monopolization will be onerous, possibly in excess of the 3% fee currently charged for credit card purchases.

Under pure proof-of-stake, opportunity cost can be calculated as the total sum spent on mining labor and the market interest rate for risk-free bitcoin lending (hardware-related costs will be negligible). Since bitcoins are designed to appreciate over time due to hard-coded supply limitations, interest rates on risk-free bitcoin-denominated loans are likely to be negligible. Therefore, the total volume of txn fees under pure proof-of-stake will just need to be just sufficient to compensate labor involved in maintaining bandwidth and storage space. The associated txn fees will be exceptionally low.

Despite these exceptionally low fees, a proof-of-stake network will be many times more costly to exploit than the proof-of-work network. Approximately, a proof-of-work network can be exploited using expenditure equal to about one years worth of currency generation and txn fees.

By contrast, exploitation of a proof-of-stake network requires purchase of a majority or near majority of all extant coins.





# Zero coin Protocol Overview

The zerocoin extension to bitcoin would have functioned like a money laundering pool, temporarily pooling bitcoins together in exchange for a temporary currency called zerocoins. While the laundering pool is an established concept already utilized by several currency laundering services, zerocoin would have implemented this at the protocol level, eliminating any reliance on trusted third parties. It anonymizes the exchanges to and from the pool using cryptographic principles, and as a proposed extension to the bitcoin protocol, it would have recorded the transactions within bitcoin's existing blockchain.

The anonymity afforded by zerocoin is the result of cryptographic operations involved with separate zerocoin mint and spend transactions. To mint a zerocoin, a person generates a random serial number  $S$ , and encrypts (that is commits) this into a coin  $C$  by use of second random number  $r$ . In practice,  $C$  is a Pedersen Commitment. The coin  $C$  is added to a cryptographic accumulator by miners, and at the same time, the amount of bitcoin equal in value to the denomination of the zerocoin is added to a zerocoin escrow pool.

To redeem the zDKPC into DKPC (preferably to a new public address) the owner of the coin needs to prove two things by way of a zero-knowledge proof. (A zero-knowledge proof is a method by which one party can prove to another that a given statement is true, without conveying any additional information apart from the fact that the statement is indeed true.)





The first is that they know a coin  $C$  that belongs to the set of all other minted zDKPC ( $C_1, C_2, \dots, C_n$ ), without revealing which coin it is. In practice, this is done quickly by use of a one-way accumulator that does not reveal the members of the set.

The second is that the person knows a number  $r$ , that along with the serial number  $S$  corresponds to a zDKPC. The proof and serial number  $S$  are posted as a zDKPC spend transaction, where miners verify the proof and that the serial number  $S$  has not been spent previously. After verification, the transaction is posted to the blockchain, and the amount of DKPC equal to the zDKPC denomination is transferred from the zDKPC escrow pool.

Anonymity in the transaction is assured because the minted coin  $C$  is not linked to the serial number  $S$  used to redeem the coin.

The accumulator used for the zero-knowledge proof would have to be re-computed every time a spend transaction is verified, and although this can be done incrementally if the accumulator checkpoint is carried on from earlier blocks to the new block,

it would still add some overhead to the verification-process. Additionally, both the accumulator checkpoint and all the zDKPC serial numbers would have to be added to every DKPC block, thus increasing the size (although not substantially).



# Tor Integration

Tor, derived from an acronym for the original software project name The Onion Router is an IP obfuscation service which enables anonymous communication across a layered circuit based network.

Tor directs internet traffic through a free worldwide volunteer overlay network consisting of more than seven thousand relays to conceal a users location and usage from anyone conducting network surveillance or traffic analysis. The layers of encrypted address information used to anonymize data packets sent through Tor are reminiscent of an onion, hence the name. That way, a data packet's path through the Tor network cannot be fully traced.

Tor's use is intended to protect the personal privacy of users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored. Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested like the layers of an onion. Tor encrypts the data, including the next node destination IP, multiple times and sends it through a virtual circuit comprising successive, randomly elected Tor relays.

Each relay decrypts only enough of the data packet wrapper to know

which relay the data came from, and which relay to send it to next. The relay then rewraps the package in a new wrapper and sends it on.

The Final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing, or even knowing, the source IP address.

Because the routing of communication is partly concealed at every hop in the Tor circuit, this method eliminates any single point at which the communicating peers can be determined through network surveillance that relies upon knowing its source and destination.





# DarkPayMarket

DarkPayMarket is a P2P decentralized and anonymous marketplace that is based on OpenBazaar, an open source project developing a protocol for e-commerce transactions in a fully decentralized marketplace.

DarkPayMarket is built on several existing technologies. Transactions between all parties are built as Ricardian contracts, and each step of a trade is cryptographically signed. This ensures authenticity of the data, prevents tampering with contracts, and allows for arbitration if a dispute arises. Escrow is achieved using multisignatures. These 'moderated transactions' are 2-of-3 multisignature, with the buyer, seller, and a trusted third-party each having a key. Payments are performed using DarkPayCoin. The networking of DarkPayMarket relies heavily on the InterPlanetary File System to ensure distribution of data, and fully supports Tor integration.

# Contract Schema

## RICARDIAN CONTRACT

