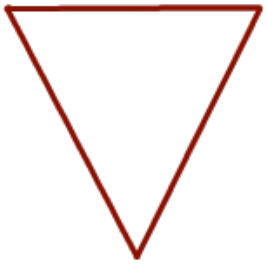

DARK

Lightpaper

DARK project aims to provide a secure and anonymous payment system and marketplace app, so you can buy, sell and exchange stuff privately.

Table of contents

ⓘ INFO: work in progress – this document may be updated at any time

1. Introduction

In 2019, retail e-commerce sales worldwide amounted to 3.53 trillion US dollars and e-retail revenues are projected to grow to 6.54 trillion US dollars in 2022. Online shopping is one of the most popular online activities worldwide.

This market has strong centralized entities dominance : when we want to buy or sell something online, we have to register in third-party systems and accept their -sometimes opaque- terms of use.

Worse, our user information is collected, parsed, used, and sold to other third parties. It is stored in many places and used without we really have control or a detailed view on how it is used and who stores it.

This is not a fair system. Fortunately, block-chain technology may offer new ways to do online commerce while preserving user privacy.

2. Project overview

Born during summer in 2018, Dark was created as a proof-of-stake blockchain project wishing to answer those two issues : lack of privacy and lack of decentralization in e-commerce.

This first step was the seed of Dark community DAO basis, developers and moderators positions were claimed, and community voted early chain metrics.

Project got listed in STEX, in CryptoBridge (RIP), Bisq and other smaller exchanges.

Since then, community kept working and funding its servers and developments : cold staking pool, explorer, OpenBazaar implementation tests, parachain proof of concept, Flutter mobile app, …

In 2019, former Shadowcash project people came in and showed what had been initiated about escrow system and user interface.

Developers forked ShadowCash, then its rebrand Particl, and community voted more long-term metrics and a much lower supply.

First experiments with SDC/Part inheritance were positive from a tech point of view, but not from a user experience and adoption point of view :

- heavy client to download for wallet operations
- no IPFS storage
- several minutes block time + needed confirmations are too long to wait
- BTC tech basis is great, but not suited for decentralized e-commerce
- heavy and hard to upgrade (and sometimes closed source) middlewares

Substrate, interoperability and open source : the way to go

Substrate offers everything a modern blockchain project needs : speed, interoperability, security, and great development frameworks.
Dark community is convinced Polkadot and Substrate framework are next-gen tech and it will initiate the next innovation cycle in crypto world.

Developers then started working on a parachain proof of concept (named 'Dystopia') in 2020 for Polkadot Rococo testnet.

As opposed to usual behavior (self-centered techs and projects) we see people in Polkadot community cooperate, innovate and share great resources and material.
We aim to become active part and contributors of this promising ecosystem.

Several projects made great work on blockchain interoperability, privacy layers, decentralization, and it opens new and different channels to spread while protecting our users privacy. One of the best early Polkadot projects, *Subsocial,* had released high quality open source pallets we could mod and use as a basis for e-commerce purpose.

3. Features

Dark “Dystopia” proof of concept, built with Substrate framework, is made of 3 layers :

- Dark Dot runtime/node
- Dark Api middlewares/libraries
- Dark Bay front-end

This software combination will allow users to create a profile, one or several storefronts, customize them, and add products so other users may order them. It will also include a search engine, a reputation system, escrow, notifications, and IPFS content storage.
Other users will be able to explore the storefronts and their listed products and order them.

More than just e-commerce oriented software, Dark will offer governance and monetary system, covered later in this paper.

Cryptography

Dark will support the Polkadot{.js} extension, that allows easy account and key management in a web browser, as the cryptography used is the same as Polkadot / Kusama.
Dark may also use any complementary tech offered by other Substrate based projects : anonymity layer (i.e zk-Snarks), mixing services, offline vault compatibility via Parity Signer…
Dark team has pushed a pull request to pre-reserve address prefix “17”.

Substrate pallets

Whole software is based on Substrate and its community or existing open-source custom modules named “pallets”.
To make it simple, pallets are code files used to define on-chain or off-chain objects : we will name them *entities*.
Each entity can have associated data to it : we will name each associated data group *fields*.

Example : a storefront is an entity, and this entity has multiple fields : owner address, name, unique identifier, description, …

You can look in pallets code parts which define custom entities and fields in the dedicated Github repository.

Storefronts

User who may want to act as a seller will be able to create one or multiple storefronts.
Each storefront is associated with its owner account and corresponding public key, so each storefront and its content can be assigned to its owner -allowing storefront ownership, profiles and reputation system.

Each storefront is a distinct entity with its own fields, which will allow a user-friendly view of all attached data :

- name
- type
- unique identifier
- banner image
- description
- tags / categories
- external links
- associated products

Non-seller users can then explore the storefronts and their products, and subscribe to their feed so user can be informed about new listings and updates.

Products

Product is an entity with its own fields :

- name
- image
- description
- price
- stock
- tags / categories
- shipping cost

User who is a storefront owner can create products in it so they appear in the storefront listings.
Regular users can then read product details and order them if they want.

Offchain worker

Offchain worker is a set of utilities which first use is to bring fiat price info so users can list and buy products in their native currency *(only USD available in alpha release)*.
It may also be used to gather info from Dark ERC20 smart contract, native chain or any useful external API available. *(please read Monetary section below)*.

Orders

Order is a more complex entity with workflows. It will manage ordering of products in storefronts, and its field are :

- unique id
- order total
- buyer escrow & seller escrow *(please read "Escrow & Dual Deposit Toll" section below)*
- associated storefront & product
- creator & timestamp
- state & update operator + timestamp *(please read ""Order flow" section below)*

Escrow & Dual Deposit Toll

As wanted as much decentralized as possible, order system needs escrow that doesn't require any third party to solve disputes between buyers and sellers.

Dark will provide an automated escrow system : **"DDT" escrow - Dual Deposit Toll.**

Inspired by first SDC/PART escrow developments, for our proof-of-concept, tokens, corresponding to both buyer and seller escrow amount, are locked (*please read ""Monetary" section below)* and released as a whole or not, following the order experience and states.

It is a part of order pallet now, but may evolve as an Ink smart-contract based on this solidity one and customized for our needs.

Escrow is also designed to be variable for each product with buyer/seller escrow percentage or amount defined separately. For our proof of concept it is a fixed percentage, but it may evolve as a voted parameter value (*please read ""Governance" section below)*

Order flow

Order can be updated by buyer or seller according to its states :

New

Buyer just placed his order, and total order amount + buyer escrow amount are locked.

Accepted

Seller accepted the order and is preparing it. Next expected order state is Shipped. Seller escrow amount is locked.

Refused

Seller refused order. Buyer locked tokens are unlocked and order cancelled.

Shipped

Seller has shipped order. He can provide a proof of shipping / tracking number.

Complete

Buyer has received order and all is fine. Both escrow locked funds are released.

Refunded

Special state where the order is refunded in full after complete state.

SlashedBuyer

Buyer had bad behavior and his locked funds are held in Treasury account.

SlashedSeller

Seller had bad behavior and his locked funds are held in Treasury account.

SlashedBoth

Both buyer and seller had bad behavior and his locked funds are held in Treasury account.

Pending

Special dummy state used between operations.

Canceled

Buyer can cancel his order before seller accepted it, his funds are released.

Dispute

Special state where Governance may arbitrate a dispute between buyer and seller.

Identity

Each user may create a profile (optional), exposing the following fields :

- Nickname
- Avatar
- Description
- Social links

Identity system may be improved, implementing other tools like decentralized Id (DID) pallet.

Permissions

A permission layer allows to define basic ownership logic : only store owner can create, edit or delete products in his storefront, for example.
It is also used in order flow to define when the buyer or the seller has editor roles depending on the order state.

Permission system may also allow lending or transferring ownership of one or multiple storefronts.

Moderation

Even if the system is designed to be censorship-free, a moderation pallet may allow Dark community to remove some content or punish bad behavior. This will be part of Governance layer which will be implemented in a second step.

Privacy

Users privacy is the key point. Even if Dark will provide its own encryption layer, one solution is not enough solutions.
We are convinced the better way to protect users privacy is to be able to use any efficient privacy solution provided by other projects or partners : zero-knowledge proof, coin mixing, relay DIDs, encryption… and make our system fully compatible with them. Or alternate all of them.

Inherited features

As Dark is built with Substrate, it is intrinsically an upgradable, scalable and customizable system.
It shares same on-chain governance and blazing fast upgrade mechanisms as all Substrate-based blockchain projects.
As a Substrate based blockchain, Dark may interact with any other parachain, as a service provider and consumer, and will be able to manage other parachains tokens such as DOT, KSM, but also future stablecoins or privacy tokens.

4. Governance & Monetary system

Governance

As a community-driven project, and since its genesis, Dark holders may initiate proposals and vote on directions to follow, developments or improvements to fund with community Treasury, parameters to adjust (escrows, timelocks), awareness campaigns to fund.

Community already voted in the past :

- supply and metrics adjustments
- hard fork

Substrate governance system will really improve the proposal and voting process, and can allow different vote types : vote per weight, vote per account, or more complex custom ones.

Fees

There are two types of fees which are collected to fund Treasury account :

regular fees

really small fees for regular actions like placing an order, changing its state, editing a storefront, deleting a product…

storefront fees

in our proof-of-concept there is a fixed 500 DARK fee, but this parameter is intended to be flexible : users with high reputation may have lower fees, community may vote higher fees aiming more quality than quantity.

Staking

As community voted it in 2019, here is the yearly decreasing staking reward scheme this year and in the future :

	june 2020	june 2021	june 2022	june 2023	june 2024	june 2025	june 2027	june 2028
average yearly %	18.00%	15.00%	13.00%	5.00%	5.00%	2.50%	2.50%	2.00%

These are the parameters applied to Dark native chain and coin, and will be ported as pallets to implement same reward scheme in our parachain proof of concept.

5. Roadmap

Public testnet proof of concept (Dystopia)

Planned February 2021

Rococo testnet application

Planned March 2021

Dark ERC20 (mirrored token)

Planned April 2021

Improvements

ETA Q3 2021

Many improvements are planned and will be implemented over time :

- storefront page visual customization
- multiple image products

- product dimensions/weight/sizes
- more FIAT currencies conversion
- ERC20 bridge
- Full governance system

...and more !

Dark Dot

Polkadot and Substrate framework offer the best tech so far. Dark project will gradually move to Substrate, having as a goal to become a full live parachain and leave current native Bitcoin core based system.

6. Contacts

Website:	https://darkdot.network
Subsocial:	https://app.subsocial.network/@darkdot
Twitter:	https://twitter.com/darkdot_network
Telegram:	https://t.me/D4rkPay
Discord:	https://discord.gg/Jwnjhwh
Medium:	https://medium.com/@darkdot
Github:	https://github.com/DarkPayCoin