Abstract.

Built on the Ethereum distributed ledger, the Blockchain Board of Derivatives (BBOD) is designed to be the open-source, decentralized trading platform, which allows trading cryptocurrency smart derivatives contracts (futures and options) with high liquidity and unprecedented security. BBOD is designed to benefit the community therefore, most of BBD tokens, that BBOD collects from fees will be burned.

The BBOD platform introduces multiple state-of-the-art and long-awaited features in the space of decentralized derivatives trading platforms including (i) a frequent batch auction market mechanism with market maker, (ii) enhanced liquidity pools across a wide range of assets, (iii) instant price discovery for digital tokens and (iv) on-chain encryption of sensitive transaction data (price, volume).

To enhance liquidity, we propose a hybrid market of frequent batch auctions with an autonomous market maker. The proposed design provides users with high liquidity, reduced spreads, protection from "flash crashes" and overall improved traders' welfare.

BBOD's system is secure against all known quantum algorithms by applying elliptic curves post-quantum cryptography to encrypt, on-chain, all sensitive transaction data like price and volume.

The BBOD platform makes it possible to either protect cryptocurrency investments against crashes or speculate on price changes using a wide range of digital tokens (eg. Ethereum, Qtum, GNT).

The platform’s roadmap lays out its future path to develop a turnkey solution in the form of one venue for cryptocurrency owners to trade derivatives, convert and list new tokens on the market.
Table of Contents

I. Team .......................................................................................................................... 2

II. Introduction .............................................................................................................. 4
   - General flaws in centralized cryptocurrency derivatives trading platform
   - Challenges in decentralized trading platforms design

III. BBOD System Design ............................................................................................. 8
   - Users and Agents on the BBOD platform
   - Overview of Market design
   - Frequent Batch Auctions and liquidity creation
   - Autonomous Market Maker and liquidity creation
   - Interaction between market models
   - Encryption of transactions data with elliptic curves post-quantum cryptography
   - The importance of Reserve Contributors
   - Safety of the Central Reserve
   - Central Reserve AI Manager
   - Listing Service – a turnkey solution for price discovery of new digital tokens

IV. Token specification, crowdfunding and legal classification ................................... 17
   - Crowdfunding
   - Token design
   - Legal classification

V. Platform core features ............................................................................................ 20
   - Security of Assets
   - Security of Transactions
   - High Liquidity
   - Efficient Price Discovery
   - On-chain Settlement
   - Comparison to existing cryptocurrency derivatives trading platform

VI. Applications ............................................................................................................ 21
   - Protect against price fluctuations
   - List your tokens on the BBOD Trading platform
   - Convert your tokens

VII. Roadmap and products offering ........................................................................... 23

VIII. LEGAL DISCLAIMER ............................................................................................ 25

IX. Appendix 1. Options 101 ...................................................................................... 30

X. Appendix 2. Options pricing model used in BBOD platform .................................. 33
Team

The most distinguished feature of the team is a unique combination of scientific background, industrial and entrepreneurial experience. BBOD’s international and highly experienced team consists of scientists, programmers and coders with professional experience acquired in IBM, Hewlett Packard, CERN and Max-Planck Institute, Bunge.

Our offices are located in Dublin, Geneva and additionally the technology office is situated in Gdansk next to the National Quantum Information Centre, with which we are about to sign long term collaboration agreement. Steps have been taken to establish an office at UCDNexus in the vicinity of the University College Dublin. We are also in close contact with the University of Cambridge and have taken steps to commence collaboration with the Faculty of Mathematics at the University of Cambridge.

*Full team bios (with links to LinkedIn and Google Scholars) are available at [http://www.bbod.io](http://www.bbod.io).*

---

**Piotr Arendarski, Ph.D**
Co-founder

Piotr is an expert in market microstructure theory, one of the leader of Quantitative Finance Research Group, at University of Warsaw. He is an Assistant Professor in Finance at Poznan University of Economics where has educated +4000 students who later have worked for Goldman Sachs, Citi, EY, KPMG. Piotr is a Project Manager and manages day-to-day business operations at BBOD. He is a founder of Quant Technology, a fintech startup. Piotr holds Ph.D degree in Economics.

---

**Krzysztof Urbanowicz, Ph.D**
Co-founder

Krzysztof is highly experienced coder and mathematician with +20 years of professional and scientific experience in Max Planck Institute, Bunge and Trinity College Dublin. He is a great passionate about Informationism, the theory described in book: Informationism from Philosophy to Quantitative Trading. Krzysztof guards the quantitative accuracy of algorithms at BBOD platform. He is a founder of Quant Technology, a fintech startup. Krzysztof holds Ph.D degree in Econophysics.

---

**Tomasz Jackowski, Ph.D**
Head of Software Development

Tomasz has +20 years executive experience acquired in Morgan Stanley and Societe Generale in New York in investment banking division. He has more than two decades of industrial experience in trading platform development and architecture (he created Sogena’s trading platform before 08 crisis). Tomasz holds Ph.D degree in Computer Science from Columbia University.

---

**Marcin Pawlowski, Ph.D**
Head of Quantum Cryptography

Marcin is an industrial expert and scientific authority in Quantum Cryptography. He is a leading member of National Quantum Information Centre in Gdansk, with more than 50 publication on Quantum cryptography and experience in large scale projects at Max Planck Institute and University of Bristol. Marcin watches over security at the BBOD Platform. Marcin holds Ph.D degree in Quantum Information.
Hubert worked in the online services and telecommunications sectors. His main focus is public relations and online-marketing. He has a master’s degree in media & communications from Middlesex University and his responsibility is to implement BBOD’s marketing and PR. Hubert is a voracious reader with a deep interest in socio-economics.

Andrew is one of the world’s leading software designers with more than a decade of industrial experience in IBM, CERN (Geneva), Hewlett Packard. He has worked as developer/designer and later as an Application Architect and Team Leader for P&G, ING, Deutsche Bank. He has specialized in architecting large scale applications and leading delivery distributed teams. He is blockchain enthusiast. Andrew holds Msc degree in Computer Science.

Pawel is a leading software developer with technical industrial experience in CERN (Geneva) and Onwelo, He has gained expertise in mobile application development (Android), as well as, full-stack development and blockchain based trading platforms.

Mateusz’s main focus is Financial Markets and Blockchain technology law. He was a Business & Legal Advisor at a Bitcoin Exchange. Mateusz is responsible for incorporation and legal services, such as AML/KYC procedure, monitoring the legal aspects and status of cryptocurrencies at BBOD.

Advisors

Professor Janusz Holyst, Ph.D
Head of Advisory Team

Alex is a leading expert in Machine Learning and Artificial Intelligence in Ireland with almost decade of industrial and postdoctoral experience in the areas Evolutionary Computation, and Artificial Intelligence. He will advise on theoretical framework and practical application of artificial intelligence module in BBOD Platform.

Josh is experienced derivatives trader, and has been specializing in Algorithmic & High-Frequency Trading (HFT) since 2012. He holds a MSc in Quantitative Finance from the University of Warsaw. He develops a multivariate backtesting system for statistical arbitrage as well as a limit order book (LOB) simulation system for ultra-low latency HFT, both written in multi-threaded C++ from scratch. He supervises theoretical framework and practical application of market microstructure in BBOD Platform.

Yoshiharu Sato
Algorithmic Trading Advisor

Yu-Jul Huang, Ph.D
Financial Mathematic Advisor

Yu is an Assistant Professor at University of Colorado. His research is focused on Mathematical Finance and Applied Probability. He advises on theoretical framework of order flows and market stability at BBOD Platform. He holds PhD degree in Applied and Interdisciplinary Mathematics from University of Michigan.
Introduction

Blockchain technology offers an innovative way to run decentralized applications; often called Dapps in this circumstance. Dapps, decentralized applications, in broad terms defines any script or software, that is distributed throughout the network in a decentralized manner. This is in contrast to normal apps, which are located on a particular server. As a result, dapps connect users and providers directly. Ethereum enables coders to create smart contracts - code, which is executed on the distributed ledger virtual machine.

Ethereum smart contracts are trustless and provide a secure framework for agreements between sellers and buyers. If some objective conditions are met (money paid or price reached some level), the contract is automatically executed. Therefore, Ethereum smart contracts are well designed to function as cryptocurrency derivative contracts.

The derivatives market plays important roles in the economy, by providing tools for protecting against price fluctuations and for speculating on prices and thus enhancing market efficiency. Nowadays, both fiat and crypto derivatives contracts are settled off-chain (eg. CBOT, Deribit, CryptoFacilities). The derivatives industry is highly intermediated, and blockchain computation provides an opportunity for cost reductions and increased efficiencies. The lack of existence of full-on-chain trading platform derives mainly from inability to guarantee on-chain encryption of transaction (miners front-running problem, spoofing), insufficient market depth (large transaction may have high impact on average execution price) and insufficient liquidity in general to offer liquidity pools across a wide range of asset.

The BBOD trading platform will be the world’s first open-source, decentralized cryptocurrency derivatives trading platform, that that is designed to benefit community and therefore all fees earned by the platform return to token holders’ wallet through buy back program - All BBD tokens that BBOD collects from fees, after paying exchange operator, will be burned – i.e. destroyed and taken out of circulation. BBOD platform guarantees liquidity at any time and provides unparalleled security for assets and transactions.

Below, we outline most important challenges in space of cryptocurrency exchanges along with our solutions.
General flaws in centralized cryptocurrency derivatives trading platform

Lack of security

Centralized trading platforms and third-party wallets store your private keys on your behalf. This is a giant risk since in the event that anything goes wrong with their servers, or if they make a decision to close business, then your assets are gone forever (because there is no authority that cover the losses). One solution is to hold cryptoassets in “cold storage” by keeping coins safe in an offline manner. However, cryptocurrency trading platforms frequently find themselves being victims of hackers, no matter what security system they use. The latest example was one of the world’s largest bitcoin exchanges, Bitfinex on 2 August 2017, that lost $65 million to a hack.

BBOD’s trading platform is decentralized, therefore Users’ funds remain under their control in decentralized smart contracts on secure Ethereum distributed ledger (blockchain).

Lack of market depth

The growing supply of digital assets and underdeveloped financial infrastructure has negative impact on general level of liquidity in cryptocurrency market. Liquidity is described as having the availability of a product or market to a sizeable audience or more specifically how conveniently and cheaply you can buy or sell an asset. The problem arises when substantial amount of cryptocurrency needs to be hedged or converted. Therefore, large orders would have negative market impact on subsequent change in price and in consequence the price taken by user. Lack of market depth is responsible also for flash-crashes, for example Ether price crashed from $319 to 10 cents 21 June 2017 for couple of seconds.

The BBOD trading platform provides a unique market design to enhance market depth and liquidity by introducing a hybrid structure consisting of two market models: Frequent Batch Auctions and the Autonomous Market Maker. Additionally, liquidity will be instantly supported by Reserve Contributors who supply capital to the Central Reserve.

Limited number of instruments

Variety in the amount of financial instruments, that a trader has at his disposal is the key to a diversified portfolio. This is especially true in today's volatile markets, where sentiments change from minute to minute and flash crashes occur on a regular basis. There are currently several widely known centralized cryptocurrency exchanges offering derivatives. The offer is usually limited to Bitcoin, Ethereum and Ripple futures contracts, and options on Bitcoins.
The BBOD trading platform provides a full range of derivative instruments (Ethereum, ERC20 tokens and cross-chain trades in the future). Due to its unique market design, virtually any token may be traded or exchanged on the trading platform. BBOD also provides listing service for users who want to place their token on the trading platform. No matter, whether the token is traded on any other exchange, or not. There will be no restrictions and no waiting list for token issuers who want to make the market for their tokens.

Challenges in decentralized trading platforms design

Exposure to arbitrage and miner front - running

The most popular cryptocurrencies reward miners for contributing to the efficiency of the network. Whoever chooses to pay more gas for his or her transaction, gets his request processed faster. It is alike to connection speeds on NYSE and CBOT. Namely, that whoever has the faster connection has his orders processed faster by the exchange. For the blockchain this means: whoever pays more gas is faster. Arbitrage is usually a socially-accepted form of promoting marketing efficiency and liquidity. In terms of the internal mechanisms of distributed ledger technology, however, there is a frequently abused loophole. A cryptocurrency owner sends an order, then decides to cancel that order. There is a time delay between these two processes, that can be exploited by savvy miners.

BBOD stops this abusive process by using double-blind encryption on the price and volume of each transaction on its entire trading platform.

Slow cancelation and slow order processing

This applies to both placing orders and cancelling them, extremely important functions if you want to protect your investment and time your purchase and sales orders.

Since the transactions are, in first order, settled between BBOD's Central Reserve and the client, after, which BBOD settles the transaction between the Ethereum Main Network and itself; in return, a fee on the transaction and cancellation is levied.

Encryption and protection from abuses (eg. high gas costs for competing transactions)

To prevent abuses from parties that monitor the exchange, BBOD's system uses double-blind encryption for all transactions in order ensure that neither any of the users nor the system itself has
access to their details. As a result, BBOD insulates anyone from front-running, including itself. It also prevents pursuit for faster order execution that consumes high gas\(^1\) costs.

This is achieved by applying zero knowledge encryption protocols to identify the users and their transactions. These protocols use the fact that computing some functions \(f\) is trivial while their inverses \(f^{-1}\) can be even NP-complete. One party (usually called prover) can claim that it holds a value \(x\) without revealing it by communicating \(y = f(x)\). Since finding \(x = f^{-1}(y)\) is not feasible the other party (verifier) cannot compute \(y\) but, when \(x\) is later revealed, it can check if prover’s claim was true. In our case BBOD plays the role of the prover. For speed and reliability, we use non-interactive zero-knowledge protocols which reduce communication required.

Another challenge in this area comes from the rapid development of crypto-analysis. Methods of encryption that are currently considered secure can soon become compromised. To cope with this BBOD is built with crypto agility (the ability to easily shift between different methods of encryption).

\(^1\) Gas is a transaction fee in Ethereum network
BBOD System Design

The main idea behind the design of the system was to create healthy market structure with maximum security and high liquidity.

BBOD trading platform offers a trading venue with access to a highly liquid cryptocurrency derivatives execution venue (margin trading) and cryptocurrency conversion (token physical conversion).

Our markets (products):

- Crypto ERC-20 Futures
- Crypto ERC-20 Options (European, vanilla)
- Crypto ERC-20 Spot token conversion
- Cross-chain trading and conversion (future development)

Our Service:

- Trading
  - Frequent batch auctions (FBA)\(^2\)
  - Autonomous market maker (AMM)\(^3\)
- Listing service
- Reserve Contributors service

Future developments assume introducing cross-chain trading, see the Roadmap for details. Both market models are equipped with mechanisms, that support high liquidity. Please refer to the details below.

Users and Agents on the BBOD platform\(^4\)

There are three types of the trading platform users on the Blockchain Board of Derivatives:

*Traders* are individual clients who participate on the trading platform and generate volume by executing trades.

---

\(^2\) Here and after, words: Frequent batch auctions, FBA and the auction will be used interchangeably

\(^3\) Here and after, words: Autonomous market maker, AMM and quotes driven market will be used interchangeably

\(^4\) Here and after, words: BBOD Platform and BBOD will be used interchangeably
**Reserve Contributors** provide liquidity in form of capital to the Central Reserve to increase liquidity for active users. By serving trade requests from Traders, reserve contributors earn profit from the spread by quoting offer and bid price.

**Issuers** request for listing service to Trading Platform Operator. They feed the platform with supply of new tokens. If the minimum requirements are met, the Operator allow to list new tokens at the Platform.

Additionally, there are four types of *agents* on the Blockchain Board of Derivatives:

- **Central Reserve.** An on-chain module, that is part and parcel of the platform, as it holds assets and participates in the market by providing liquidity. Central Reserve is divided into cells for respective digital tokens.

- **Clearinghouse (Smart contract).** An on-chain module, that facilitates transactions among counter parties by providing clearing and settlement services. This is the main contract which serves as the main entrance to the system for Users.

- **Central Reserve AI Manager.** An off-chain agent, our proprietary AI is closely connected to Central Reserve and processes information needed to distribute liquidity provided by Central Reserve, manage risk exposure, volumes and open positions of the Central Reserve. This module is responsible for keeping the system stable.

- **Trading Platform Operator.** An off-chain agent, the operator administrates the platform by issuing and removing instruments, feeding rates, listing new tokens.

**Overview of Market design**

The BBOD Trading Platform offers two market models: Frequent Batch Auctions (discrete time model) and the Autonomous Market Maker (continuous-time model) for trading derivatives and converting tokens. The main idea behind the creation of such novel market design was to enhance market liquidity and maximize trader welfare. Frequent Batch Auctions provide a fair mechanism of price discovery and prevent high-frequency trading arms races. On the other hand, there is a portion of scholars including Hass & Zoican (2016) who found that a batch auction market could potentially hurt liquidity. Therefore, we propose another layer to the market design: our Autonomous Market Maker to increase liquidity, as it guarantees liquidity at some predefined level. The capital for making the market (offering bid and ask) is provided by initial contribution to Central Reserve (from initial token sale) and continuously leveraged by Reserve Contributors in exchange for BBD utility tokens (more details in section “Token model”).
Frequent Batch Auctions and liquidity creation

We apply Frequent Batch Auctions\(^5\) in line with mechanics provided by Budish, Peter Cramton & John Shim (2015). The underlying idea of an auction in financial markets can be simplified in the following way: the market identifies an equilibrium price, that matches supply and demand, thus reducing the proportion of unfilled buy-and-sell orders. Please note, the counter party of a User is either another User or the Central Reserve.

The diagram below illustrates the interaction between agents in FBA design for one token.

The BBOD Platform regularly gathers buy and sell orders in batches, in order to facilitate efficient price discovery and match buy/sell orders. Frequent Batch Auctions is a process where Users and Central Reserve feed the auction with buy and sell orders, their preferred limit prices and volumes. After all bids and asks are sent, the equilibrium price is calculated at which the orders are executed simultaneously. Thus, concluding the auction. In case some orders are left unmatched, either due to insufficient volume or a mismatch in corresponding prices, the order may either be cancelled or are carried over to the next batch. In general, batch auctions can be illiquid because of frequently recurring unmatched orders. BBOD provides the trading platform and its participants with an intelligent mechanism to support our client's need for liquidity. Central Reserve provides “on-demand” liquidity, eg. when there is imbalance between volume of buy and sell orders. Instant stream of capital is supplied by Reserve Contributors. The whole process is managed and guarded by a proprietary Central Reserve AI Manager to streamline the batch auctions' effectiveness.

\(^5\) Here and after, words: FBA, Auction and Frequent Batch Auctions will be used interchangeably
BBOD’s Trading platform provides the client with a strong self-reinforcing encryption mechanism, functioning on-chain, to protect their individual transaction data (volume and price), thus preventing front-running and predatory arbitrage.

The market benefits from potentially greater market depth and a streamlined price discovery mechanism for less liquid tokens, which as a result should contribute to lower liquidity costs. On the other hand, users do not know the price until the auction is finalized.

**Autonomous Market Maker and liquidity creation**

This market is a continuous-time trading model where the counter party of a User is always the Central Reserve, and provides guaranteed level of instant liquidity (Quote Driven Market). The level of liquidity depends mostly on amount of capital and net exposure of Central Reserve. The reason we call it the market maker is, because the User takes the price, and Central Reserve makes the price. The AMM makes a profit by adding a spread, or markup to their quote. AMM model sets itself apart from the batch auction in, that the User does not need to wait for an auction to finish. The User chooses a bid or ask price, volume and the transaction is executed immediately at the selected price. In contrast, to the auction, the Central Reserve provides instant, guaranteed liquidity for the market. The client benefits from the absence of transaction fees and instant liquidity and known price taken by the User.

The diagram below illustrates the interaction between agents in AMM market for one token.

![Diagram of Autonomous Market Maker]

In a regular market maker model there is, however, a limit to the amount of liquidity any market maker can provide. As a result, there is always a cap on the volume of the transaction dictated by the size of its reserve (capital) and the net exposure to the financial instrument it holds.

---

6 Net exposure is a measure of the extent to which a fund’s trading book is exposed to market fluctuations
BBOD is built to fix this limitation through Reserve Contributor. Our autonomous market maker model is designed with instant, guaranteed liquidity in mind for both sides of trade and low spreads. The Reserve Contributor provides capital to the Central Reserve, thus increasing volume of transactions, in exchange for BBD utility tokens (more details in section “Token specification and legal classification”).

AMMs quotes of Options and Futures are initially provided to Users by our propriety algorithm. (See Appendix 2 to see details on our option valuation model) which stands for initial valuation in case there is insufficient liquidity at the auction to discover a price. The quotes provided by algorithm will adapt to quotes found at the FBA. Therefore, any discrepancy in price between both markets should be vanished.

### Interaction between market models

Both markets act as independent venues for derivatives trading and converting tokens. The diagram below illustrates how the liquidity is distributed between markets.

![Diagram showing interaction between market models](image)

From the User’s perspective, both markets operate independently, for example, an ETH (Ether) futures contract is traded on both markets, therefore there may be a price discrepancy between the prices on each market. On the other hand, the platform is designed to prevent arbitrage between the two markets by pegging the quotes found at the AMM to the quotes found at the FBA.

However, from the perspective of the whole system, both markets are closely connected through Central Reserve, which may *hedge their net exposure* at either market. The main goal of the system is to provide...
maximum liquidity and keep net exposure of Central Reserve close to zero. This complex problem is managed by Central Reserve AI Manager.

The final outcome for traders is illustrated at the diagram below. Please note, this is diagram present only intuitive structure of trader window, it is not an illustration of future graphical and structural representation of final version of the platform.

First, user select the type of market (Auction or Market Maker) the appropriate window is activated and select respective options. User may set limit price to take part in auction and wait if his order is filled or take the price offered by market maker.

Encryption of transactions data with elliptic curves post-quantum cryptography

BBOD's system uses double-blind encryption for all transactions in order ensure that neither any of the users nor the system itself has access to their details. Following the U.S. National Institute of Standards and Technology (NIST) guidelines on future cryptography (report no. NISTIR 8105, see http://dx.doi.org/10.6028/NIST.IR.8105) our system is designed for crypto agility. This means the ability to easily shift from one method of encryption to another in response to the development of new attacks. The default encryption uses RSA algorithm for its ease of implementation and speed. In RSA
blinding involves computing the blinding operation \( E(x) = (xr)^e \mod N \), where \( r \) is a random integer between 1 and \( N \) and relatively prime to \( N \) (i.e. \( \gcd(r, N) = 1 \)), \( x \) is the plaintext, \( e \) is the public RSA exponent and \( N \) is the RSA modulus. As usual, the decryption function \( f(z) = zd \mod N \) is applied thus giving \( f(E(x)) = (xr)^{ed} \mod N = xr \mod N \). Finally, it is unblinded using the function \( D(z) = zr - 1 \). Multiplying \( xr \mod N \) by \( r - 1 \mod N \) yields \( x \), as desired. When decrypting in this manner, an adversary who is able to measure time taken by this operation would not be able to make use of this information (by applying timing attacks RSA is known to be vulnerable to) as it does not know the constant \( r \) and, hence has no knowledge of the real input fed to the RSA primitives.

Since NIST guidelines are a consequence of the rapid development of quantum computing (which will probably only accelerate in the future since European Union pledged to invest 1 billion EUR in “quantum revolution”) BBOD has a version with elliptic curves post-quantum cryptography, which is secure against all known quantum algorithms. Since standard elliptic curves techniques are even more vulnerable to quantum attacks than RSA [QIC 3 (No. 4) (2003) pp.317-344] the security of BBOD is based on Supersingular Isogeny Diffie–Hellman key exchange (SIDH). This method works with the set of supersingular elliptic curves \( E \) over \( Fp^2 \), where the number of points on any such curve will be \((p \pm 1)^2\). An isogeny of an elliptic curve \( E \) is a rational map from \( E \) to another elliptic curve \( E' \) such that the number of points on both curves is the same. For supersingular elliptic curves, isogenies are equivalently defined by points inside their kernel. The SIDH method works with a prime of the form \( p = (wA)^{eA}(wB)^{eB}(f) \pm 1 \) where \( wA \) and \( wB \) are small primes and an elliptic curve \( E \) defined by the equation: \( y^2 = x^3 + ax + b \). SIDH builds an isogeny map from a single elliptic curve point which is taken as the generator for the isogeny's kernel. This point is chosen to be a random linear combination to two fixed points chosen to be in the kernel of the isogeny. The security of SIDH is closely related to the problem of finding the isogeny mapping between two supersingular elliptic curves with the same number of points. The security of SIDH is \( O\left(p^{\frac{1}{2}}\right) \) for classical computers and \( O\left(p^{\frac{1}{6}}\right) \) for quantum computers [Jao D., De Feo L. (2011) Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. In: Yang BY. (eds) Post-Quantum Cryptography. PQCrypto 2011. Lecture Notes in Computer Science, vol 7071. Springer, Berlin, Heidelberg]. This suggests that SIDH with a 768-bit prime \( p \) will have a 128-bit security level. BBOD can swiftly switch between these two variants if the need arises.

The importance of Reserve Contributors

BBOD's trading platform is designed to attract Reserve Contributors, who hold cryptocurrencies idly in their wallets, to participate in providing capital to the Central Reserve in exchange for BBD utility tokens. They maintain the reserve, determines exchange rates and feeds the rates to the BBOD platform. By
serving trade requests from users, reserves earn profit from the spread by sending bid and ask prices to the platform. Therefore on average they should earn a spread. The Central Reserve AI Manager collects all quotes from Reserve Contributors and provide the narrower spread to Traders. The more capital contributed, the more liquidity the Central Reserve can offer to Traders. Reserve Contributor Is a liquidity provider (market maker).

**Safety of the Central Reserve**

The heart of the trading platform is the Central Reserve; its safety, therefore, is a major concern. Funds held by this unit are used to provide liquidity and settle transactions. The Central Reserve is divided into cells, each cell represents different token deposited by Users. BBOD Trading platform employs a special unit, the Central Reserve AI Manager. Its purpose is to gather all data related to transactions including incoming orders, the amount of funds in the Central Reserve and the net exposure of Central Reserve and distribute liquidity to provide the tightest spreads and highest rate of fulfilled order at auction. The data is processed by an artificial intelligence algorithm to provide safety measures to Central Reserve in terms of how much liquidity should be supplied to both markets with objective function to keep balance between sell and buy positions, while still provide Users with high liquidity.

**Central Reserve AI Manager**

The safety of Central Reserve is guarded by Central Reserve AI Manager who manages the resource in the Central Reserve. Below we propose theoretical and initial AI structure.

The basic asset acquisition problem arises in applications where we decide to set the position of asset at time $t$ to be used during time interval $t + 1$. A variation of the basic setting of the position at the market is the time delay between making a decision and finalizing it on the market in a future unknown state (unknown demand and supply).

We model the problem using:

- $x^p_t$ is value of position that we decide to managed in time $t$
- $x^s_t$ is value of position realized just at time $t + 1$
- $x_t = (x^p_t, x^s_t)$ is the state of the parameters that we can manipulate in order to manage the risk of AMM
- $p^p_t$ is market price of instrument in time $t$ when we making decision.
- $p^s_t$ is the market price of instrument in time $t + 1$ when position is executed.
- $R_t$ represents of our resources to manage the position $x^p_t$ at time $t$
- $D_t$ represents of demand/supply of the instrument on the market at time $t + 1$
The state of the system is described by $S_t = (R_t, D_t, p_t)$. We represent the evolution of our state variable using $S_{t+1} = S^M(S_t, x_t)$.

The one period reward function is given by $C_t(S_t, x_t) = p_t^s \cdot x_t^s - p_t^p \cdot x_t^p$.

We can find optimal decisions by solving Bellman’s equation

$$V_t(S_t) = \max_{x_t}\left(C_t(S_t, x_t) + \gamma \int (V_{t+1}(S^M_{t+1}(S_t, x_t))) \cdot PDF_t(S_t) dS_t\right)$$

Where $PDF_t(S_t)$ is the probability distribution function of state $S_t$.

We will solve the Bellman’s equation using Reinforcement Learning. In particular we will employ Q-learning with Neural Network value-function approximator.

**Listing Service – a turnkey solution for price discovery of new digital tokens**

Aside from trading service, BBOD offers a listing service. Issuers or holders of any ERC20 tokens will find an automated way to introduce their tokens into our derivative market and/or conversion market. Any issuer or holder of ERC-20 compatible tokens may submit a request for listing after satisfying our requirements, that are related to minimum supply of tokens. Issuers may ask to list their tokens at the auction, even if the token is not traded at other exchanges. Issuers may also ask market making support or be simultaneously Reserve Contributors and providing quotes to the market. Both, derivatives and conversion markets are available. *Listing service is free.*
Token specification, crowdfunding and legal classification

Crowdfunding

The crowdfunding of BBOD and the corresponding token creation process are organized around smart contracts running on Ethereum. Participants willing to support development of the BBOD platform can do so by sending ether to the designated address. By doing so they create BBD Tokens (BBD) at the rate of 1 000 BBD per 1 ETH.

The parameters of crowdfunding are published at www.bbod.io

Crowdfunding process leads to creation of BBD, a backbone token for the BBOD platform.

BBD implementation follows widely adopted token implementation standards with two additional functionalities core to the crowdfunding process and future upgrades, namely, token creation and token migration.

It is important to note that BBOD team plans to issue a separate migration contract to transfer tokens to the new contract. BBD upgrade will be reacquired to satisfy all functionality of the platform presented in this document. Therefore, please note, the main purpose of this token issue is to support development of the BBOD platform to the level described in the Roadmap.

The upgrade will need action from token holders and cannot be imposed by BBOD team members.

Token design

BBD tokens are utility tokens and are used to pay for a trade execution fees at BBOD trading platform.

Benefits for BBD token owners

1. Most of transaction fees collected in BBD will be burned

   Most BBD tokens that BBOD collects from fees, after paying Exchange Operator and Partners, will be burned and taken out of circulation, ceasing to exist, forever.

2. Discounted trading

   The more BBD tokens are held, the lower trade execution fee. The discount is linearly related to respective BBD ownership percentage.

3. Listing Services
Listing is Free. No initial fees and no annual fees are charged. The requirement is to supply a minimum number of tokens to be listed, to a specified cell in Central Reserve.

**The Trading Service: Frequent Batch Auctions.** Trading fees in the auction market are paid with BBD. When users use the platform to trade, they will be charged a trade execution fee as a percentage of the trade size. The fee is converted into BBD tokens. For example, a User buys 1 ETH Future contract at price $300, the commission is 0.01%\(^7\) of nominal value, if 1 ETH = 0.9 BBD, the trade execution fees equal 0.01 ETH ( $0.03 ), therefore User pays 0.009 BBD ( $0.027 ). The fee percentage is set by BBOD and will differ depending on product (futures, options, token conversion) and its liquidity. If there are not enough BBD tokens to cover the fees, a User will be prompt to buy BBD tokens through the platform. For tokens that are used, a trade execution fee is burned (permanent destruction of BBD tokens), therefore the total supply will decrease. BBOD intends to set a trade execution fee to be the lowest comparing to existing and future competitors.

**The Trading Service: Autonomous Market Maker.** There is no execution fee. BBOD intends to set the lowest possible trade execution fee, in comparison to existing and future competitors.

**BBD token purchase.** If users do not already hold BBD tokens to use a service, they can buy BBD tokens directly on the platform.

There will be no additional issue of new tokens to the public. Therefore, the value of the token should be closely related to the demand for the platform’s service.

**Once the MinCap is reached, BBD tokens may be converted to Ether** directly at our simple decentralized exchange using ethereum wallet or Mist. Additionally, BBD tokens will be listed on exchanges shortly after MinCap is reached.

We offer extra bonus for token buyers who purchase significant amount of BBD tokens in a single transaction. The bonus of additional 5%, 10%, 15% or 20% BBD tokens is guaranteed by smart contract. The details of the Token Issue along with structure of Token Issue and Use of Funds may be found on our website.

*Please note, the services and benefits outlined above will be developed on the BBOD platform over time specified period and not all will be available in the initial release of the platform. See the Roadmap for more details.*

---

\(^7\) This commission rate serves only as example, the actual execution fees will be set before the Release 1.0.
**Legal classification**

**BBD tokens are utility tokens** whose entire value derives from the services provided the BBOD platform in exchange for holding or consumption of the token.

The BBD token is not an investment in any way, shape, or form. Possessing the token does not grant the owner a share of any profits outside of any made through his own endeavors in the stated roles above. Passively holding the token has no expectation of profit or value.

BBD tokens are not supposed to be used for speculation and hold no promise to intellectual or other property or cash flows. They offer no right to involvement in the company, and do not entitle to make any decision over company assets or strategy. There is no guarantee of value or claim on income associated with BBD tokens other than, that derived from platform’s utility. **BBD tokens are not securities.**

More information you will find in chapter “Legal Disclaimer”.

Platform core features

Security of Assets
Users' funds stay under their control in decentralized smart contracts on the Ethereum distributed ledger and are managed via smart contract. We never hold users’ funds. We do not hold a private key to the account where Users deposited tokens.

Security of Transactions
Our systems are designed with discretion in mind, for this reason we double-blind encrypt on-chain each transaction’s volume and price to eliminate possibility of front-running and other form of high-frequency trading arms race.

High Liquidity
The BBOD provides two independent sources of liquidity, Frequent Batch Auctions and Autonomous Market Maker model. In addition, Reserve Contributors act as an autonomous liquidity support mechanism to provide instant funds to the Central Reserve. The more capital contributed, the more liquidity the Central Reserve can offer to Users.

Efficient Price Discovery
Issuers of new and existing digital assets should feel right at home on BBOD, as we provide a venue for them to list their digital tokens. As a result, newly issued tokens, that may not yet be tradable on any exchange have a tailor-made and easy-to-use tool at their disposal to accurately value their cryptocurrency. This precisely is executed on our frequent batch auctions.

On-chain Settlement
All transactions are settled on-chain meaning, that the profit or loss from a transaction is calculated by the smart contract on the distributed ledger, away from centralized servers. This provides yet another layer to ensure tamper-proof transactions.

Comparison to existing cryptocurrency derivatives trading platform
We compare the BBOD Platform to existing systems in the table below.
Applications

Protect against price fluctuations

The Blockchain Board of Derivatives is designed to offer each crypto investor the tools to protect their investment using cryptocurrency futures and options. Almost any investment conversation includes phrases, such as enter the market early, do not enter the market too late, buy the dip, buy low and sell high. While some can be correct, you never truly know when it is too late. Especially if you are new to investing! You may have heard of hedge funds making and losing huge sums of money, but what do they use to protect their investments? The answer, a lot of the time, is derivatives. It is the first step to truly protecting an investment.

Our platform provides a potentially invaluable financial service to every holder of cryptocurrencies. Our futures and options contracts allow the speculator to generate value by betting on future price movements. A hedger, such as a crypto-miner, can insure himself against adverse price movements using the same financial instruments, in either direction.

For example, when a trader hopes to capitalize on an expected rise in the price of a cryptocurrency, he can consider buying a call option, selling a put option or buying a futures contract. However, when a trader hopes to capitalize on an expected fall in the price of a cryptocurrency, he can consider selling a call option, buying a put option or selling a futures contract. Combinations of these are also commonly used among options and futures traders. The Appendix should give the reader an indication of the inner workings of these financial instruments and how they work to protect what you own of cryptocurrencies.

1: a problem arises in illiquid markets when one party needs to have its position closed automatically (margin call) and the exchange needs to find a counterparty for the second party (winning side).

2: email storage

<table>
<thead>
<tr>
<th>Trading Platform</th>
<th>On-chain</th>
<th>Front-running removed</th>
<th>Guaranteed liquidity</th>
<th>Low spreads</th>
<th>Encrypted transaction data</th>
</tr>
</thead>
<tbody>
<tr>
<td>CryptoFacilities</td>
<td>No</td>
<td>No</td>
<td>Somewhat¹</td>
<td>Depends on market</td>
<td>No</td>
</tr>
<tr>
<td>Deribit</td>
<td>No</td>
<td>No</td>
<td>Somewhat¹</td>
<td>Depends on market</td>
<td>No</td>
</tr>
<tr>
<td>BBOD</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trading Platform</th>
<th>Security of assets guaranteed</th>
<th>Listing service</th>
<th>Anonymity</th>
<th>Trading fees</th>
<th>Efficient Price Discovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>CryptoFacilities</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Low</td>
<td>No</td>
</tr>
<tr>
<td>Deribit</td>
<td>No</td>
<td>No</td>
<td>Somewhat²</td>
<td>Very Low</td>
<td>No</td>
</tr>
<tr>
<td>BBOD</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Very low</td>
<td>Yes</td>
</tr>
</tbody>
</table>

¹: On-chain
²: Front-running removed

Table: Trading Platform Features

<table>
<thead>
<tr>
<th>Trading Platform</th>
<th>Security of assets guaranteed</th>
<th>Listing service</th>
<th>Anonymity</th>
<th>Trading fees</th>
<th>Efficient Price Discovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>CryptoFacilities</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Low</td>
<td>No</td>
</tr>
<tr>
<td>Deribit</td>
<td>No</td>
<td>No</td>
<td>Somewhat²</td>
<td>Very Low</td>
<td>No</td>
</tr>
<tr>
<td>BBOD</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Very low</td>
<td>Yes</td>
</tr>
</tbody>
</table>
List your tokens on the BBOD Trading platform

Our turnkey solution allows all Users to list their tokens on the auction market, either to facilitate derivatives trading or physically convert tokens. Even if the tokens are not traded on any exchange, BBOD Frequent Batch Auctions provides a perfect venue to value tokens and discover real price. **Listing is Free.** No initial fees and no annual fees are charged. The requirement is to supply a minimum number of tokens to be listed, to a specified cell in Central Reserve.

Convert your tokens

BBOD Trading platform is a venue used to physically convert tokens. The distinguished feature from existing exchanges are: Frequent Batch Auctions and instant liquidity provided by from Reserve Contributors. These features should stimulate unparalleled liquidity and market depth even for less liquid tokens.
Roadmap and products offering

**Roadmap**

**Preview version**
- Matemask connection to the platform
- ETH Futures and Options test trading
- Trading analytics

**Q3 2017**

**2017 Oct-Nov**

**TOKEN SALE**

**Base Platform V1.0**
- Decentralized Trading platform
- Encryption of transaction data
- On Blockchain Settlement
- Fully Non-Custodial Trading
- Automatic Listing service for Issuers

**Q1 2018**

**Platform V2.0**
- Selected derivatives contract may settled via physical delivery
- Reserve contributors (private Market Makers)
- Support cross-chain derivatives trading
- Encryption of transaction data using elliptic curves post-quantum cryptography, if needed.

**Q2 2018**

**Platform V3.0 : Attracting Institutional Investors**
- Simulated Trading
- Managed Accounts
- API for Automated Trading

**Q3-Q4 2018**
Product Offering (Option & Futures & Spot)

Q1 2018
- Ethereum and Major ERC-20 Tokens
- Golem
- OmniseGO
- Qtum
- KyberNetwork

Q2-Q3 2018
- All liquid ERC-20 Tokens
- Major Cryptocurrency (Bitcoin, Zcash, Dash ...)

Q3-Q4 2018
- Crypto Volatility indexes
- Exotic Crypto
  (Mining Capacity – HashRate ... )
References:

2. Yang, Post-Quantum Cryptography, 2011, PQCrypto
3. Jao & De Feo, Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies, 2011
5. Proos & Zalka, Shor's discrete logarithm quantum algorithm for elliptic curves, QIC 3 (No. 4), 2003, pp.317-344

LEGAL DISCLAIMER

Jurisdiction

We have approached the Blockchain Board of Derivatives (BBOD) token sale in a comprehensive and responsible manner. Given the uncertain status of cryptocurrency and digital tokens in various jurisdictions, we spent a significant amount of time and resources to analyze the legal status of Blockchain Board of Derivatives business model and the BBD tokens in jurisdictions where we plan to operate. The sale of BBD tokens constitutes the sale of a legal software product under Gibraltar law. This product sale is conducted by Mackenzie Management Limited, operating under Gibraltar law.

It is the responsibility of each potential purchaser of BBD tokens to determine if the purchaser can legally purchase BBD tokens in the purchasers’ jurisdiction and whether the purchaser can then resell the BBD tokens to another purchaser in any given jurisdiction.

Especially, we encourage citizens of United States, China and South Korea to check the regulations regarding participation in digital token sale.

It is difficult to predict how or whether regulatory agencies may apply existing regulation with respect to blockchain technology and its applications, including the Blockchain Board of Derivatives and BBD tokens. It is likewise difficult to predict how or whether legislatures or regulatory agencies may implement changes...
to law and regulation affecting blockchain technology and its applications, including the Blockchain Board of Derivatives and BBD tokens.

Due to mentioned above uncertain state of regulation on a global scale, we cannot guarantee the legality of Blockchain Board of Derivatives trading platform in every jurisdiction.

There is also no unified regulatory framework applicable to crowdsourced forecasting platforms. These products and services are regulated in some jurisdictions based on existing financial services regulatory frameworks, while they are left unregulated in others.

Therefore, you should carefully consider all risks involved, including, but not limited to, those listed above and, to the extent necessary, consult an appropriate lawyer, accountant, or tax professional. Do not use our services or get involved with any activities related to BBD tokens in case of not being certain about your rights that the jurisdiction of your residence or citizenship grants you.

----

**Legal status of BBD tokens**

BBD tokens are functional utility tokens designed for the Blockchain Board of Derivatives trading platform. BBD tokens are not securities. BBD tokens are sold as a digital asset, similar to downloadable software, digital music, and alike. Once you purchase BBD tokens, they cannot be refunded. We do not recommend buying BBD tokens for speculative investment purposes. You should buy BBD tokens to participate in the Blockchain Board of Derivatives trading platform.

BBD tokens do not represent or confer any ownership right, share or security (or any equivalent right) in Blockchain Board of Derivatives or any other company, any future right to receive an interest or revenue share in Blockchain Board of Derivatives or any other company, any future right to receive an interest in any intellectual property rights relating to the Blockchain Board of Derivatives or any other form of participation in or relating to Blockchain Board of Derivatives, other than a right to participate in the Blockchain Board of Derivatives trading platform.
We do not recommend purchasing BBD tokens unless you have prior experience with cryptographic tokens and blockchain-based software.

---

**Intellectual property rights**

BBOD LABS Ltd, The Black Church, St. Mary's Place, Dublin 7, Republic of Ireland is the owner or the licensee of all intellectual property rights in BBOD site, and in the material published on it (including this document). Those works are protected by copyright laws and treaties around the world. All such rights are reserved.

You must not modify this white paper or digital copies of any other materials you have printed off or downloaded in any way, and you must not use any illustrations, photographs, video or audio sequences or any graphics separately from any accompanying text.

---

**AML/KYC procedure**

AML and KYC regulations are followed in every jurisdiction that is a member of the global banking community.

BBOD is not financial institution therefore BBOD is not required to establish KYC procedure.

However, Blockchain Board of Derivatives protects itself from involvement in any activity that facilitates money laundering or other criminal activities.

BBOD reserves the right to verify and maintains records of the identity and address of its customers in the future.
To the extent BBOD may not prevent certain of its users from using BBD tokens in violation of law, it may subject the company to civil or criminal liability and the utility, liquidity, and trading price of BBD tokens will be adversely affected or BBD tokens may cease to be traded.

---

**General terms and conditions**

This document does not constitute an offer to sell, an invitation to induce an offer, or a solicitation of an offer to acquire securities. This document is provided for informational purposes only and does not constitute investment advice. The information set in this document may not be exhaustive. While we make every effort to ensure that any material in this white paper is accurate and up to date, such material in no way constitutes the provision of professional advice. Blockchain Board of Derivatives does not guarantee, and accepts no legal liability whatsoever arising from or connected to, the accuracy, reliability, or completeness of any material contained in this white paper.

This document may contain 'forward looking statements' - that is, statements related to future, not past, events. in this context, forward-looking statements often address our expected future business and financial performance, the performance, and accuracy of the Blockchain Board of Derivatives trading platform, and often contain words such as 'expect', 'plan', 'see', 'will', 'would'. Such forward looking statements by their nature address matters that are, to different degrees, uncertain. We cannot guarantee that any forward looking statements, backtests or experiments made by us or expected results of operation of the Blockchain Board of Derivatives trading platform will correlate with the actual future facts or results.

For the convenience of our users, the Blockchain Board of Derivatives white paper, website and other related documents are available in a number of languages. In the event there is any conflict between the English language version and a foreign language version, the English language version shall govern. It is also possible that some foreign language version does not contain all information contained in this white paper.

Any dispute or claim arising out of or in connection with BBD tokens shall be governed by the Gibraltar law.
Any dispute arising out of or in connection with BBD tokens will be exclusively dealt with the Courts of Gibraltar.

We may revise these document at any time by amending this page. You are expected to check this page from time to time to take notice of any changes we made, as they are binding on you.

Last Updated 21.09.2017 version 1.2

If you have any concerns about this white paper, please contact: chris@bbod.io. Please note that Blockchain Board of Derivatives does not provide any opinion or any advice to purchase, sell, or otherwise transact with BBD tokens or any other legal or tax advice.
Appendix 1. Options 101

Options

Options are exactly, what they describe themselves to be: the right to buy or sell, if you choose, something at an agreed time in the future, for an agreed price. And you can either buy an option from someone who sells options, or you can sell options for someone who buys them.

Now, options have their own terminology, so it will be beneficial for you to understand it.

Buy Call or Put Options?

To purchase a call option means to own the right to buy a cryptocurrency at a specified price on an agreed date, if you choose. If you buy a call option you expect the price of the cryptocurrency will rise in the foreseeable future or/and volatility of underlying asset will rise.

A put option is the right to sell or take a short position in a cryptocurrency, if you choose, on or before an agreed date. If you buy put option you expect the price of the cryptocurrency to fall in the foreseeable future or/and volatility will increase.

What is the underlying asset?

What makes a derivative a derivative is, that it derives its value from something valuable. This is known as an underlying asset. As such, all options offered on the Blockchain Board of Derivatives have a cryptocurrency as their underlying.

Expiration date

The expiration date is the date when the option expire, stop existing. Any time after the expiration date the option cannot be exercised. All options on the Blockchain Board of Derivatives are European-style and can be exercised on the expiration date, only. If you want to close the option position before expiration you need to execute the trade in opposite direction.

Exercise Price

The exercise price, alternatively known as the strike price, is the price at which the underlying cryptocurrency will be delivered to the counterparty, should the holder of an option choose to exercise the right to buy or sell.
Selling/Writing Options

To write an option means to be in a short option position, to sell. In other words, you are the seller of an option, be it call or put. As such the other side of the trade is always long, a buyer. When writing an option for someone else to buy, you do so with the hope of making money from the option premium, which the buyer has to pay in order to be long. However, once you sell an option, you have to be prepared, that the other side will choose to exercise it, meaning you are obliged to act in accordance with the contract. Please refer to the following pay-out diagrams. Long calls and long puts are bought, whereas short calls and short puts are sold.

![Pay-out diagrams](image)

Option Price components

The way we value our options is a complex process, but we can give you some basic ideas about how to value any option by yourself so you can decide, which investment is better for you. The price you pay to buy any option is known as the option premium. The option premium can be separated into two components: intrinsic value and time value. The following are the formulas for calculating the intrinsic values of call and put options respectively:

Call option intrinsic value = Spot Price - Exercise Price
Put option intrinsic value = Exercise Price - Spot Price

Time value, also known as extrinsic value, is the additional amount of premium, that a trader is willing to pay for the option. Time value decreases by default the closer the option is to its expiration date, this is known as time decay.

Option Premium = Intrinsic Value + Time Value

**Futures Contracts**

A futures contract is an agreement between a buyer and a seller to exchange currency for goods (or another currency) at a future date at agreed price at the time of transaction. All futures contracts on the Blockchain Board of Derivatives are labeled as futures CFD contracts, or futures-contracts-for-difference, therefore when a User closes a position, it is settled on the basis of the difference between the prices of the futures contract at the time of buying and selling. This proves to be a much simpler transaction for our clients. Our trading platform settles all futures transactions in cryptocurrencies but futures developments assume to introduce physically settled futures and options.
Appendix 2. Options pricing model used in BBOD platform

The Theory of Objective Values

Objective value (ObV) is a value which can be added. Consequently, it follows that you can make any arithmetic on it as subtraction, multiplication, division, etc. In the space of the Objective Values one can compare between different types of the substance or events etc. The added value is commutative, that is, switching places with respect to the operation of addition does not change the result. Therefore, the ObV theory is so important not only in theory, but also in practice.

Objective Value Theory in finance\(^8\)

Consider an asset, characterized by a price, \( p(t) \). The return is defined as \( x(t) = \ln(p(t+1)/p(t)) \) and, in what follows, we assume that returns are independently distributed. The objective function, \( w(x) \) is related to the stationary probability distribution for returns, \( P(x) \), viz:

\[
P(x) = e^{-\beta w(x)}/N
\]

\(N\) is a normalization factor. For independently distributed returns, this form may be obtained as the result of maximizing the ‘free energy’\(^9\) functional:

\[
F = \int dx P(x)[\ln P(x) - \beta w(x) - \lambda]
\]

Equally, we could minimize the objective functional, \( W \), subject to constraints on the Boltzmann-Gibbs entropy\(^10\) (entropy in statistical physics for microcanonical ensemble) and normalization of the distribution function:

\[
W = \int dx P(x)[w(x) - k \ln P(x) - \lambda']
\]

---


Such a form for the probability distribution is also the outcome of a model that assumes returns are governed by a generalized Markovian stochastic process\textsuperscript{11} of the form:

\[ x(t + 1) - x(t) = f(x) + g(x)\varepsilon(t) + \eta(t) \] (4)

The Gaussian processes, \( \varepsilon \) and \( \eta \) satisfy:

\[
\langle \varepsilon(t)\varepsilon(t') \rangle = a\delta(t - t') \\
\langle \eta(t)\eta(t') \rangle = \beta\delta(t - t') \\
\langle \varepsilon(t)\eta(t') \rangle = 0; \langle \varepsilon(t) \rangle = \langle \eta(t) \rangle = 0
\]

(5)

For the moment, we can leave the form of the functions \( f \) and \( g \) unspecified except to say they depend only on \( x(t) \). \( a \) and \( b \) are constants.

The solution to this stochastic process has been deduced elsewhere\textsuperscript{12}. Adopting the Ito convention, the distribution function associated with the process is given by the Fokker Planck\textsuperscript{13} equation:

\[
\frac{\partial P(x,t)}{\partial t} = \frac{\partial^2}{\partial x^2} \left( \beta + ag^2(x) \right) P(x,t) - \frac{\partial}{\partial x} \left( f(x) P(x,t) \right)
\] (6)

The stationary solution is:

\[
P(x) = e^{ \int dx \frac{f(x)}{\beta + ag^2(x)}} \frac{f(x)}{N(\beta + ag^2(x))}
\]

Comparing with it can be seen that:

\[
\beta w(x) = \ln[\beta + ag^2(x)] - \int dx \frac{f(x)}{[\beta + ag^2(x)]}
\]

---


\textsuperscript{13} http://en.wikipedia.org/wiki/Fokker%E2%80%93Planck_equation
\[
\int dx \frac{2ag(x)g'(x) - f(x)}{\beta + ag^2(x)}
\]

(7)

A number of different cases are evident. If we define \( P(x) \) up to a normalization factor these may be expressed in the table

<table>
<thead>
<tr>
<th>( f(x) )</th>
<th>( g(x) )</th>
<th>( w(x) )</th>
<th>( P(x) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{sgn}(x) )</td>
<td>1</td>
<td>(</td>
<td>x</td>
</tr>
<tr>
<td>( x )</td>
<td>1</td>
<td>( x^2 )</td>
<td>( e^{-\beta x^2} )</td>
</tr>
<tr>
<td>( \lambda g(x)g'(x) )</td>
<td>( g(x) )</td>
<td>( \ln[\beta + ag^2(x)]^{1-\frac{\lambda}{2a}} )</td>
<td>( \frac{1}{[\beta + ag^2(x)]^{1-\frac{\lambda}{2a}}} )</td>
</tr>
<tr>
<td>( \lambda x )</td>
<td>(</td>
<td>x</td>
<td>)</td>
</tr>
</tbody>
</table>

If we further let \( \nu = \frac{1}{\alpha^2} \), \( \beta = 1 \), \( \lambda = \frac{1}{\nu} - 1 \) and choose \( g(x) = |x| \), the distribution in the third row reduces to the t-Student distribution as shown in row 4. In developing our methodology below we shall focus on the use of this distribution. Choosing other forms for the functions \( f \) and \( g \) yields other distributions that exhibit power laws. For example, the choices \( f = -\nu x|\nu|^{\nu-1} \) and \( g = x|x|^{(\nu-1)} \) leads to \( q \) exponentials.

**Objective Value (ObV) Option pricing model for power-law distribution**

The standard model of Stock prices is

\[
S(t) = S(0)e^{\gamma(t)}
\]

where
\[ y(t) = \ln \left( \frac{S(t)}{S(0)} \right) \]

it follows

\[ dy = \mu dt + \sigma d\omega, \quad (8) \]

where \( \mu \) is mean rate of return and \( \sigma^2 \) is the variance. Here \( \omega \) is the noise term, which follows Wiener process and satisfies

\[ E[d\omega(t)d\omega(t')] = dt dt' \delta(t - t'), \quad (9) \]

where the notion \( E \) is the expected value. In the case the probability distribution of \( y \) is Normal distribution with variance \( \sigma^2 \) and mean \( \mu \). Follow the Ito Lemma the distribution of \( S \) is Log-normal with variance \( \sigma^2 \) and mean \( \mu - \frac{\sigma^2}{2} \). The Black and Scholes\(^1\) model uses the Ito Lemma in order to calculate the transformation from Gaussian (Normal) to Log-Normal distribution of respectively \( y \) and \( S \). There appears the noise induced drift coefficient \( -\frac{\sigma^2}{2} \), which decreases the mean. The Black and Scholes, in further calculations, integrate the value of future price \( S \) with respect of Log-Normal distribution with given above parameters. After replacing the \( S \) with \( y \), the integration reads

\[ C_{BS} = S(0)e^{-rt} \int_{y_s}^{\infty} \frac{(e^{y} - e^{y_s})}{\sqrt{2\pi} \sigma^2 t} \exp \left( -\frac{(y - \mu + \frac{\sigma^2 t}{2})^2}{2 \sigma^2 t} \right) dy \quad (10) \]

\( S(0) \) - present price of the asset,

\( e^{y_s} = K \) - strike of the option, \( t \) – time to maturity of the option.

In the Black and Scholes (BS) model they consider further the problem of portfolio with short position of one call option and long position of one asset. Such a portfolio is riskless so should give on the end the risk-free interest rate \( r \). This construction gives us the fair price of the call option, it means, that the drift coefficient \( \mu = 0 \) and the asset price in the future should be discount with risk free interest rate to present time. Following this we get the famous BS formula

\[ C_{BS} = S(0) P_{G} \left( \frac{y-}{\sigma \sqrt{t}} \right) - Ke^{-rt} P_{G} \left( \frac{y+}{\sigma \sqrt{t}} \right), \]  

where

\[ y_{\pm} = \ln \left( \frac{K}{S(0)} \right) - rt \pm \frac{\sigma^2 t}{2}. \]

In order to introduce the other form of noise element with power-law distribution, we have to modify the Eq.(11) to the form

\[ dy = \mu dt + \sigma d\Omega \]  

We assume, that \( \Omega \) possess the t-Student distribution with, for now, arbitrary power-law \( \alpha \). The t-Student distribution represents the Gauss distribution in the limit \( \alpha \to \infty \). Further we will use this property in order to find the transformation from Gaussian distribution to t-Student with arbitrary power-law \( \alpha \), so we would like to find such a scaling \( Z(\Omega) \), that

\[ d\Omega = Z(\Omega)d\omega \]  

We assume \( \Omega \) from t-Student distribution \( P_{\alpha}(y) \), which is reasonable assumption found in the literature, then repeating the calculations of BS model we obtain, that variance \( \sigma^2 \) is replaced by \( \sigma^2 Z(\Omega)^2 \) and noise induced drift coefficient as follows \(- \frac{\sigma^2}{2} Z(\Omega)^2 \). The value of call option is similar to Eq.(10) with Gauss replaced by t-Student:

\[ C_{St} = S(0)e^{-rt} \int_{z>y_s} (e^z - e^{y_s}) P_{\alpha}(z) dz \]

The \( z \) variable will be found after substitution from \( y \) and will be shown after.

The t-Student distribution which we use has the form

\[ P_{\alpha}(y) = \frac{\Gamma((\alpha+1)/2)}{\sqrt{\alpha \pi} \Gamma(\alpha/2)} \frac{\alpha+1}{1+\left(\frac{y^2}{\alpha}\right)} \]
\[ \Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt \]  

(15)

We have now the equation for option price, but the problem lays on the form of scaling coefficient \( Z(\Omega) \). Lisa Borland\(^{15}\) assume ad-hoc, that the scaling coefficient has the form

\[ Z(\Omega) = P_{tsallis}^{(1-q)/2} \]  

(16)

This form can be replaced having t-Student number degree of freedom \( \alpha \) from Tsallis q-distribution\(^{16}\) assuming, that the power-law should be the same

\[ q = \frac{2}{\alpha+1} + 1 \]  

(17)

and Eq.(16) in the form with t-Student

\[ Z(\Omega) = P_{\alpha}^{\frac{1}{\alpha+1}} \]  

(18)

The Eq.(18) is the assumption of L. Borland which gives Tsalis q-distribution of \( \Omega \). We do not want to assume this form but calculate it analytically from Objective Value Theory. The ObV theory gives the form of transformation of data between t-Student distribution of arbitrary \( \alpha \). On the beginning we will found the transformation between arbitrary t-Student distributions and further we put for one power-law in limit to infinity, which will give the transformation to Gauss distribution. The transformation form comes from normalization of objective functions as follows

\[ w(y) = \frac{w(x)}{\langle w(x) \rangle \langle w(y) \rangle} \]  

(19)

Where \( y \) takes the probability distribution \( P_{\alpha}(y) \) and \( x - P_{\beta}(x) \). The objective function for t-Student is given in table above and it reads

---

\(^{15}\) L. Borland, Option Pricing Formulas Based on a Non-Gaussian Stock Price Model, PRL 89(9), 098701(4), (2002).

\(^{16}\) D. Prato and C. Tsallis “Nonextensive foundation of Lévy distributions”, Phys. Rev. E 60, 2398 – Published 1 August 1999
\[ w(y) = \frac{\alpha + 1}{2} \ln \left( 1 + \frac{y^2}{\alpha} \right) \]

\[ w(x) = \frac{\beta + 1}{2} \ln \left( 1 + \frac{x^2}{\beta} \right) \] (20)

When \( x \) is from normalized Gauss distribution (\( \beta \to \infty \)) and \( y \) - t-Student. We have

\[ \langle w(y) \rangle = \int_{-\infty}^{\infty} \frac{\alpha + 1}{2} \ln \left( 1 + \frac{y^2}{\alpha} \right) P_{\alpha}(y) \, dy \]

\[ \langle w(x) \rangle = 0.5 \] (21)

After solving the integral for \( y \) we have circa \( \langle w(y) \rangle \approx 0.579 \) for \( \alpha = 4 \).

The transformation formula using objective function for \( x \) from Gaussian distribution reads

\[ y = \left. \frac{x}{|x|} \sqrt{\alpha} \left[ \frac{\Pi(\alpha)}{\Pi(\beta)} \left( 1 + \frac{x^2}{\beta} \right) \frac{\langle w(y) \rangle_{\beta + 1}}{\langle w(x) \rangle_{\alpha + 1}} - 1 \right] \right] \] (22)

\[ \Pi(\alpha) = P_{\alpha}(y) \left( 1 + \frac{y^2}{\alpha} \right)^{\alpha + 1} = \frac{\Gamma((\alpha+1)/2)}{\sqrt{\alpha \pi} \Gamma(\alpha/2)} \] (23)

When \( \beta \to \infty \)

\[ y = \left. \frac{x}{|x|} \sqrt{\alpha} \left[ \left( \Pi(\alpha)(\sqrt{2\pi})^2 S_y \right)^{\frac{2}{\alpha + 1}} e^{S_y \frac{x^2}{2 \alpha + 1}} - 1 \right] \right] \]

\[ x = \frac{y}{|y|} \sqrt{2 \ln \left[ \Pi(\alpha)^{-\frac{1}{2}} \left( \sqrt{2\pi} \right)^{-1} \left( 1 + \frac{y^2}{\alpha} \right)^{\frac{\alpha + 1}{2 S_y}} \right]} \] (24)

where \( S_y = \frac{\langle S(y) \rangle}{\langle S(x) \rangle} \).
The transformation from $x$ to $y$ is symmetric, so the trend in unchanged.

For the analytical solution we have to make some assumptions. Nevertheless, one can calculate exact values by computer with no assumptions in the middle. Have in mind that further solution has its own drawbacks.

We now assume first order Taylor expansion of $y$ with respect of $x$. So we get the transformation form from Wiener process $x$ to $y$ with t-Student distribution

\[
d y = \frac{1+y^2}{y} S_y \frac{\alpha}{\alpha+1} \sqrt{2 \ln \left( \frac{1}{\Pi(\alpha)^{\frac{\alpha+1}{\alpha}} \left( 1 + \frac{y^2}{2S_y} \right)^{\frac{\alpha+1}{2}}} \right)} \, dx,
\]

where \( w = 2\langle w(y) \rangle \frac{\alpha}{\alpha+1} \)

\[
d y \cong \sqrt{w} \Pi(\alpha)^{\frac{2}{\alpha+1}} P_\alpha(y)^{-\frac{2}{\alpha+1}} \, dx
\]

Now we can refer to the Eq.(14) and (18) and we see that \( Z(\Omega) = \sqrt{w} \Pi(\alpha)^{\frac{2}{\alpha+1}} P_\alpha(y)^{-\frac{2}{\alpha+1}} \), so we obtain Eq.(18) with further additional parameters.

We can return to the Eq.(30) and use Ito Lemma for logarithmic price changes $y = \ln S$

\[
d \ln S = \left( r - \frac{\sigma^2 w}{2} \Pi(\alpha)^{\frac{4}{\alpha+1}} P_\alpha(y)^{-\frac{4}{\alpha+1}} \right) dt
\]

\[
+ \sigma \sqrt{w} \Pi(\alpha)^{\frac{2}{\alpha+1}} P_\alpha(y)^{-\frac{2}{\alpha+1}} d\eta
\]

We can recall $z$ variable which we put the Eq.(16) in order to calculate it we have to integrate the Eq.(27)

\[
z = \ln S = \int d \ln S
\]

\[
= rt - \frac{\sigma^2 w}{2} \Pi(\alpha)^{\frac{4}{\alpha+1}} \int_0^1 P_\alpha(y)^{-\frac{4}{\alpha+1}} ds + \sigma y
\]

Here we introduced $r$ as a value of risk free interest so now $z$ is martingale.
The value of call option can be write following Eq.\( (16) \):

\[
C = S(0)e^{-rt} \int_{S(0)}^{\infty} S \cdot P_\alpha(S) dS - Ke^{-rt} \int_{K/S(0)}^{\infty} P_\alpha(S) dS \tag{29}
\]

We would like to replace integrates respect \( S \) to integrate respect \( y \) so we have

\[
C = S(0)e^{-rt} \int_{S_1}^{S_2} \exp \left( rt - \frac{\sigma^2 w}{2} \int_{0}^{1} \left( 1 + \frac{y(s)^2}{\alpha} \right)^2 ds + \sigma y \right) P_\alpha(y) dy - Ke^{-rt} \int_{S_1}^{S_2} P_\alpha(y) dy \tag{30}
\]

where \( S_1 \) and \( S_2 \) are calculated from inequality

\[
y \in (s_1, s_2): rt - \frac{\sigma^2 w}{2} \int_{0}^{1} \left( 1 + \frac{y(s)^2}{\alpha} \right)^2 ds + \sigma y > \ln \left( \frac{K}{S(0)} \right)
\]

In the Eq. (30) we have to integrate \( \int_{0}^{1} \left( 1 + \frac{y(s)^2}{\alpha} \right)^2 ds \), which we have to resolve. To this end we use the scaling property of variance with respect of time which reads

\[
\text{var}(t) \approx t^{\frac{\alpha-1}{\alpha-2}} \tag{31}
\]

So we have

\[
y(s) = \frac{\text{var}(s)}{\sqrt{\text{var}(t)}} y(t) \tag{32}
\]

Now we can resolve the integral as follows

\[
\int_{0}^{1} \left( 1 + \frac{y(s)^2}{\alpha} \right)^2 ds = 1 + \frac{2}{\alpha \cdot \text{var}(1)} y^2 \int_{0}^{1} \text{var}(s) ds + \frac{1}{\alpha \cdot \text{var}(1)} y^4 \int_{0}^{1} \text{var}(s)^2 ds = 1 + \frac{y^2(\alpha-2)}{2 \cdot \alpha-3} + \frac{y^4(\alpha-2)}{5 \cdot \alpha-3} \tag{33}
\]

Substitution to Eq.(30), reads
\[ C_{ObV} = S(0)\Pi(\alpha) \int_{s_1}^{s_2} \left(1 + \frac{y^2}{\alpha}\right)^{-\frac{\alpha+1}{2}} \exp\left(\sigma y - \frac{\sigma^2 w}{2} \left(1 + \frac{y^2(\alpha-2)}{2\alpha-3} + \frac{y^4(\alpha-2)}{5\alpha-3}\right)\right) dy - K\Pi(\alpha)e^{-rt} \int_{s_1}^{s_2} \left(1 + \frac{y^2}{\alpha}\right)^{-\frac{\alpha+1}{2}} dy, \]  

(34)

Where

\[ y \in (s_1, s_2): \]

\[ rt - \frac{\sigma^2 w}{2} \int_{0}^{1} \left(1 + \frac{y(s)^2}{\alpha}\right)^2 ds + \sigma y > \ln\left(\frac{K}{S(0)}\right) \]  

(35)

In the case of Call option the integration is from \( s_1 \) to \( s_2 \).

The power-law \( \alpha \), as well as, \( \sigma \) is taken from past data. \( \alpha \) is calculated by Maximum Likelihood method\(^\text{17}\) as the fit of t-Student distribution to past data and \( y = \ln\left(\frac{s_i}{s_{i-t}}\right) \), where \( t \) is time to maturity in working days.

When we are dealing with Gauss distribution, so \( \alpha \to \infty \), then we have normal Black-Scholes option pricing. You have to be aware that because we use approximation Call-Put parity may not be preserved, so you should keep this important factor using some additional parameter and optimize this by computer.

**Put option**

\[ P_{ObV} = K\Pi(\alpha)e^{-rt} \int_{s_1}^{s_2} \left(1 + \frac{y^2}{\alpha}\right)^{-\frac{\alpha+1}{2}} dy \]

\(^\text{17}\) The method is described in section Generalized gaussianity evaluation.
\[ -S(0)\Pi(\alpha) \int_{s_1}^{s_2} \left( 1 + \frac{y^2}{\alpha} \right)^{-\frac{\alpha+1}{2}} \exp \left( \sigma y - \frac{\sigma^2 w}{2} \left( 1 + \frac{y^2(\alpha-2)}{2 \cdot \alpha - 3} + \frac{y^4(\alpha-2)}{5 \cdot \alpha - 3} \right) \right) dy, \]

where

\[ y \in (s_1, s_2): \text{rt} - \frac{\sigma^2 w}{2} \int_0^1 \left( 1 + \frac{y(s)^2}{\alpha} \right)^2 ds + \sigma y < \ln \left( \frac{K}{S(0)} \right) \]

In the case of Put option the integration is from \(-\infty\) to \(s_1\) and from \(s_2\) to \(\infty\).

**Greek letter Delta**

\[ \Delta_{\text{call}} = \int_{s_1}^{s_2} A(y) \, dy - A(s_2) - A(s_1) + \frac{K}{S(0)} (B(s_2) - B(s_1)) \]  \hspace{1cm} (37)

\[ \Delta_{\text{put}} = -\int_{s_1}^{s_2} A(y) \, dy + A(s_2) - A(s_1) - \frac{K}{S(0)} (B(s_2) - B(s_1)) \]  \hspace{1cm} (38)

\[ A(y) = \Pi(\alpha) \left( 1 + \frac{y^2}{\alpha} \right)^{-\frac{\alpha+1}{2}} \exp \left( \sigma y - \frac{\sigma^2 w}{2} \left( 1 + \frac{y^2(\alpha-2)}{2 \cdot \alpha - 3} + \frac{y^4(\alpha-2)}{5 \cdot \alpha - 3} \right) \right) \]

\[ B(y) = \Pi(\alpha) e^{-rt} \left( 1 + \frac{y^2}{\alpha} \right)^{-\frac{\alpha+1}{2}} \]

For Delta Put there is a change in integration (see the option pricing for Put option Eq. 36).