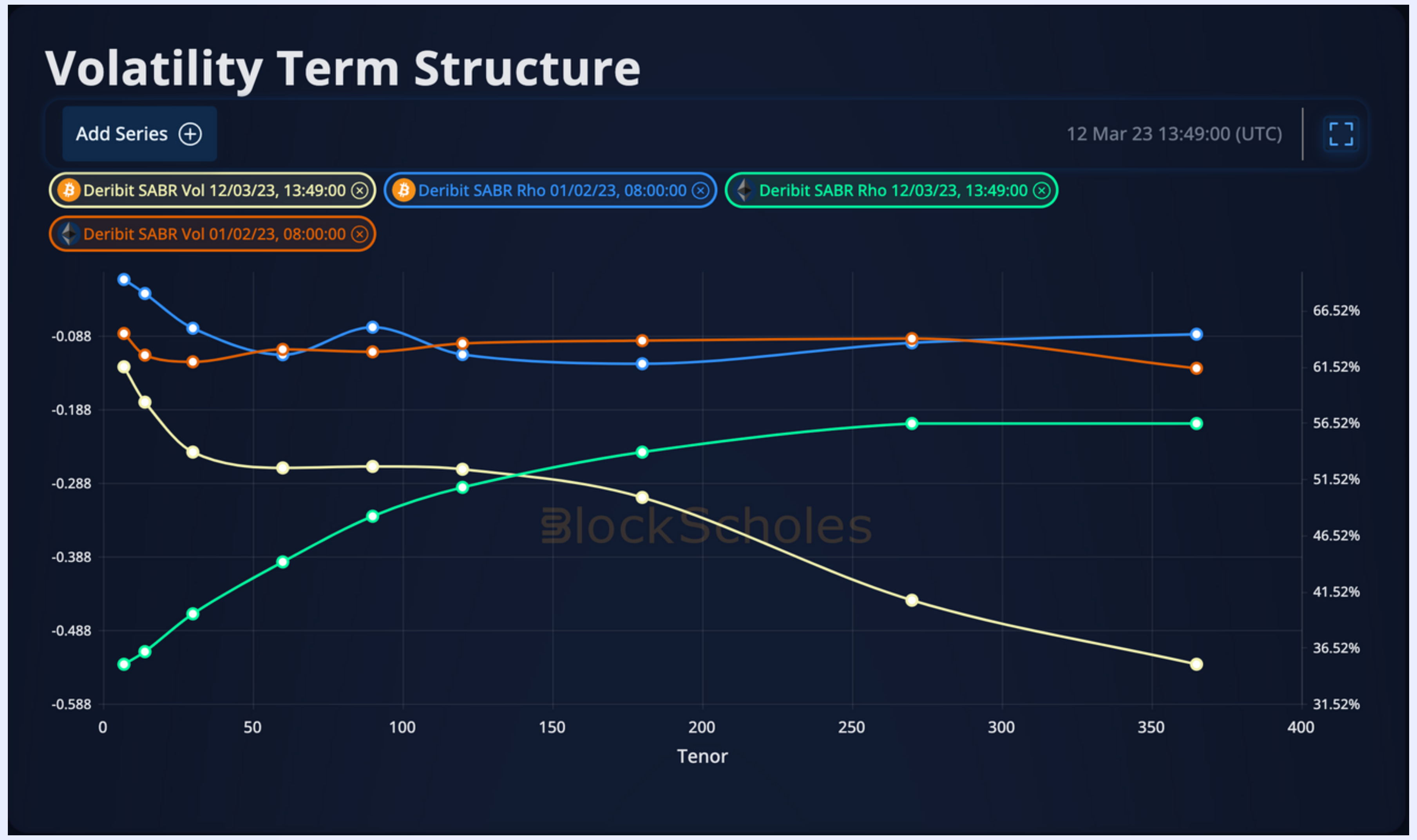
BlockScholes

INTERACTIVE ANALYSIS



INDEPENDENT RESEARCH

Previous Articles

DERIVATIVES INSIGHTS | MARKET COMMENTARIES | **THEMATIC REPORTS**

*Our **Thematic Reports** explore a variety of topics in the blockchain ecosystem; diving into the depths of DeFi protocols, analysing the effects of different actors in the ecosystem and much more. Our reports shed light onto complex and often misunderstood concepts and provide readers with valuable and coherent insights.*

UTXO vs Account-Based Models
10th Mar 2023

On-chain Options: Lyra
24th Feb 2023

Ethereums Shanghai-Capella Upgrade
10th Feb 2023

Ethereum's Gas Mechanics
3rd Feb 23

Crypto 2023
Yearly Review - 31st Dec 22

Big Keychain, Small Blockchain
Blockchain - 28th Nov 22

Maximal Extractable Value
DeFi - 27th Nov 22

The Merge
DeFi - 20th Sep 22

Decentralised Exchanges Review
DeFi - 24th Jun 22

ENVIRONMENT & OPPORTUNITY

- In 2022, the price of digital assets dropped significantly
- 2 options: (a) HODL and hope for the best or (b) exit your investment
- The problem: shortage of mature financial products for institutional investors and miners
  Derivatives are financial instruments that provide insurance against adverse price moves

ONE SOLUTION: ON-CHAIN DERIVATIVES

On-chain Financial Options for Digital Assets

Alfonso D. D. M. Rius[1] and Eamonn Gashier[2]

[1] Department of Computer Science, Imperial College London
a.delgado17@imperial.ac.uk
[2] Digital Finance Research
egashier@icloud.com

Abstract. In this paper, we introduce a framework to create financial options for digital assets that use smart contracts to take custody over assets and settle transactions. We commence our analysis by defining the benefits that derivatives can bring to market participants and deconstructing the range of financial products that are currently available. We argue that both centralised and decentralised products are subject to economic frictions and risks that cannot satisfy the needs of sophisticated investors or large tokenholders. To address this challenge, we outline how smart contracts on Ethereum can be used to create call and put options by following a set of economic and technical principles designed to minimise frictions. We also evaluate the trade-offs between different oracle and arbitration systems that allow financial data to be fed and disputes to be resolved. We hope that our work will help to drive further research in relation to on-chain financial products within business and academia.

Keywords: Financial Cryptography, Blockchain, Smart Contracts, Options, Derivatives

1 Introduction

A series of critical breakthroughs have been made in the field of distributed computing over the past decade. In 2009, the Bitcoin network [1] pioneered the use of the blockchain data structure as a means of maintaining data integrity in a distributed peer-to-peer network. This data structure takes the form of an auditable ledger that records the network's shared data into a series of interlinking blocks. In the absence of a central record-keeper, the task of validating and updating the ledger entries is shared amongst the nodes in the network. The nodes propagate information, store data and update the network's ledger by applying transactions. Bitcoin also implements cryptographic techniques (such as digital signatures) and incentive systems to allow the nodes to detect and reject malicious alterations to the shared data.

The launch of the Ethereum network [2] in 2015 constitutes an important milestone in the development of distributed ledger technology (DLT). Ethereum is a general purpose platform that facilitates the process of creating DLT-based applications. Ethereum also popularised the concept of a "smart contract" to refer to deterministic programs with internal state. However, the concept can be traced back to the work on Nick Szabo (e.g. [3,4]) in the 1990s, who defined a smart contract as a "computerized transaction protocol that executes the terms of a contract". To date, the most promising use cases for smart contracts involve issuing and transferring financial instruments (such as derivatives) in a fast and secure manner.[3] In this way, the combination of DLT and smart contracts is opening new avenues in the field of financial cryptography that are ripe for academic and commercial exploration.

Within the realm of financial instruments, it is derivatives that we wish to explore in this paper. A derivative is a contract between two or more parties that derives its value from a reference entity (the *underlying*). In general, this underlying may be an asset (e.g. Apple stock), an index (e.g. S&P 500) or an interest rate (e.g. LIBOR). As a result of this relationship, the price of a derivative is affected by fluctuations in the price of the underlying. Derivative contracts are settled at a future date by requiring the parties to fulfill any outstanding payment obligations. *Exchange traded derivatives* (ETDs) are traded on regulated exchanges under standardised terms that facilitate

[3] Eskandari et al. [5] observe that papers on Ethereum and Solidity tutorials often use derivatives as a paradigmatic use case.

Academic paper introducing a design for on-chain derivatives with no counterparty risk or jump risk

Smart contracts provide efficient custody of digital assets and fast settlement of payouts

Adapting financial engineering techniques to the new medium, removing components that are problematic (e.g. margining)

Mathematical guarantees ensure there is a fair payout under every state of the world

Eliminating Counterparty Risk

- In contrast to conventional markets, a counterparty's identity will not be known. This prevents the assessment of that counterparty's risk of default
- Derivatives that rely on margining are problematic, as a counterparty may fail to meet a margin call and walk away with no liabilities, leaving the other party with a shortfall
- We solve this problem through full collaterisation. By requiring the option's notional to be escrowed, there is no need to rely on margining systems
- Parties can transact pseudonymously and trade out of their positions without fear

FINANCIAL ENGINEERING

Eliminating Jump Risk

- Full collaterisation solves another challenge associated with volatile assets: if the price of a digital asset jumps (or falls) rapidly, a party will be closed out of their trade
- Our design ensures that (1) if an ETF is approved and the price moons; or (2) a regulatory announcement is made and the price drops to 0, there will never be a shortfall of payouts

TECHNICAL DESIGN

We have made the process of creating new derivatives simple and intuitive

- The buyer and seller each make only one transaction
- Payouts are automatically distributed on expiry – no need to monitor

An oracle mutually agreed by the parties will feed the price on expiry

- The price fed can be in any fiat currency (or even another digital currency)
- An arbitration mechanism can be put in place to resolve disputes (e.g. Augur model)

We have used contract factory model to create child contracts

- No need to deploy new code on-chain
- The collateral is segregated in child contracts to reduce the risk systemic risk

Commitment: no ICO or proprietary tokens

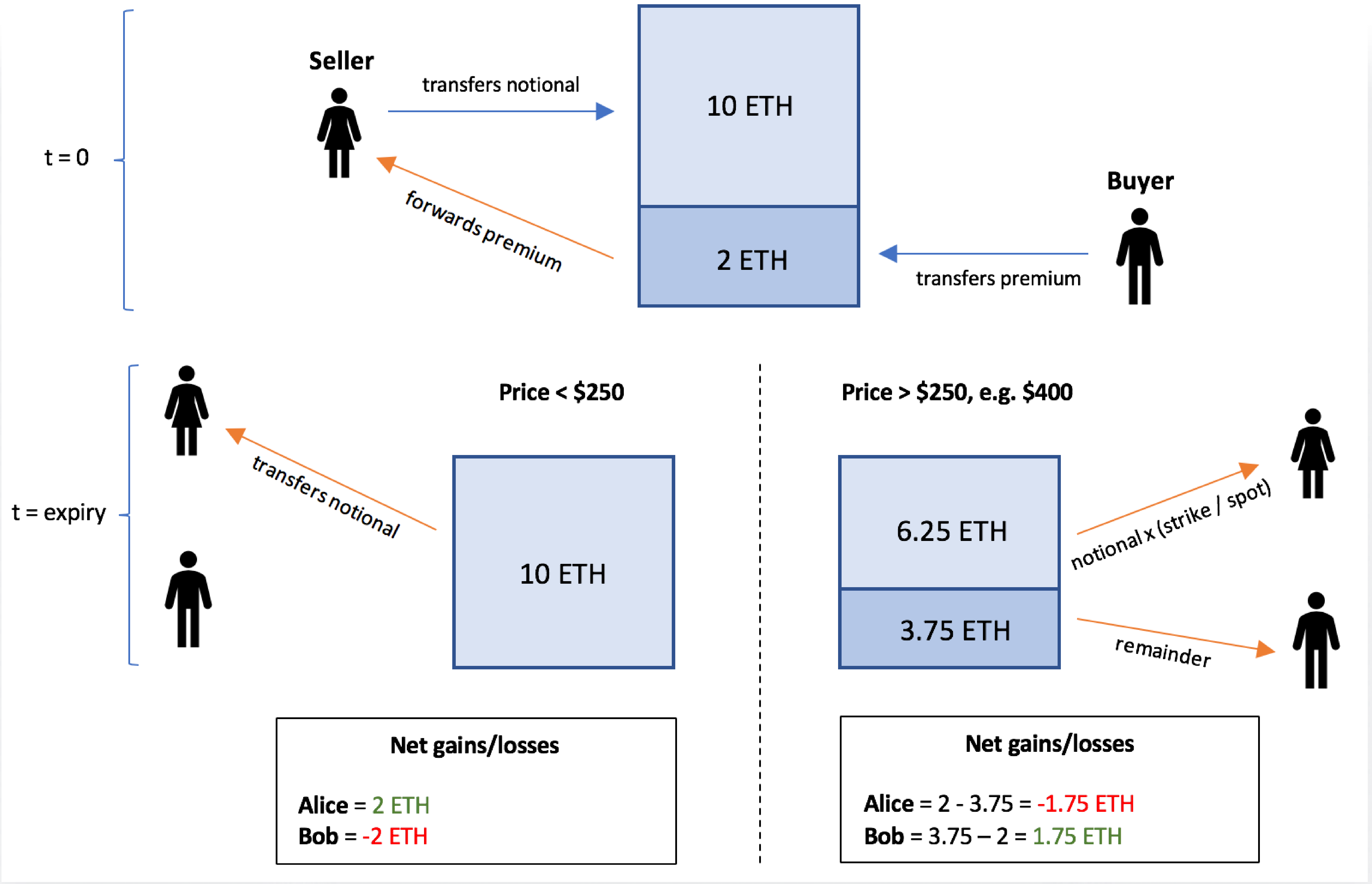
- Our derivatives rely on physical delivery and can escrow a variety of digital assets
- There is no need to hold fiat at any stage

CURRENT PLAYERS

	Highlights
opyn	• Mints tradable European Option tokens representing users position. • Implements settlement logic for Option Tokens. • Doesn’t implement market for options.
Ribbon StakeDAO	• Structured products offering - DeFi Options Vaults (DO Relies on other option minting protocols (Opyn)). • Pools users tokens and mints and sells option tokens. • Auctions for tokens held very infrequently (once a week) • High management fees (12.5% on Ribbon).
Lyra	• Uses AMM to create a European Options market. • Users pool tokens to provide liquidity • AMM Algorithmically determined Implied Volatility. • No constant and decentralised source for IV initialisation of new expiries.

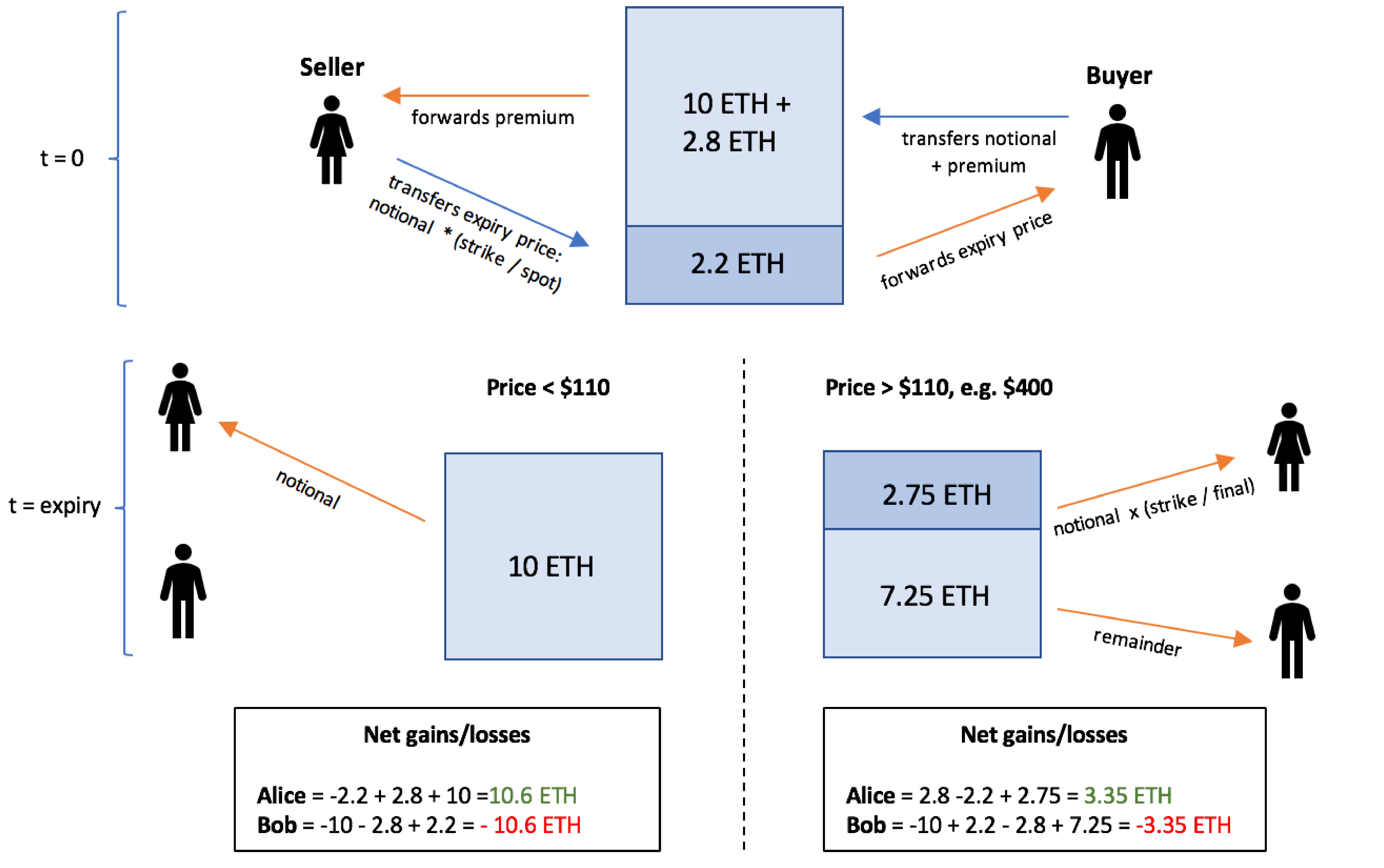
CALL OPTION

Call option for 10 ETH (notional) with 2.8 ETH premium, strike $250 and expiry in 6 months:



PUT OPTION

Put option for 10 ETH (notional) with 2.8 ETH premium, strike $110 and expiry in 6 months:



FUTURES & DIGITAL OPTIONS

- We have created futures contracts by combining the logic of calls and puts
- We have also created digital options, where the payout is capped to a certain amount
- We can combine our existing derivatives to create tailored and exotic products that satisfy the needs of market participants
- Miners, corporates, ICO treasuries and funds have an appetite for such financial products and will provide us with a source of liquidity

CONTACT

blockscholes.com

linkedin.com/company/block-scholes/

@BlockScholes

For media and investor enquiries, please contact:

+44 (0) 7737 652 583

info@blockscholes.com

27 Old Gloucester Street,
London WC1N 3AX

Blockscholes Ltd. is registered in England
Company no. 11907206