The Ethereum-powered Reputation Platform for Commerce

AUTHORS:
Yazin Alirhayim
Ibrahim Mokdad
Dmitriy Vorobyev, PhD

REVIEWERS:
Pavel Gabriel
Prof. Renato P. dos Santos, ScD

https://verify.as

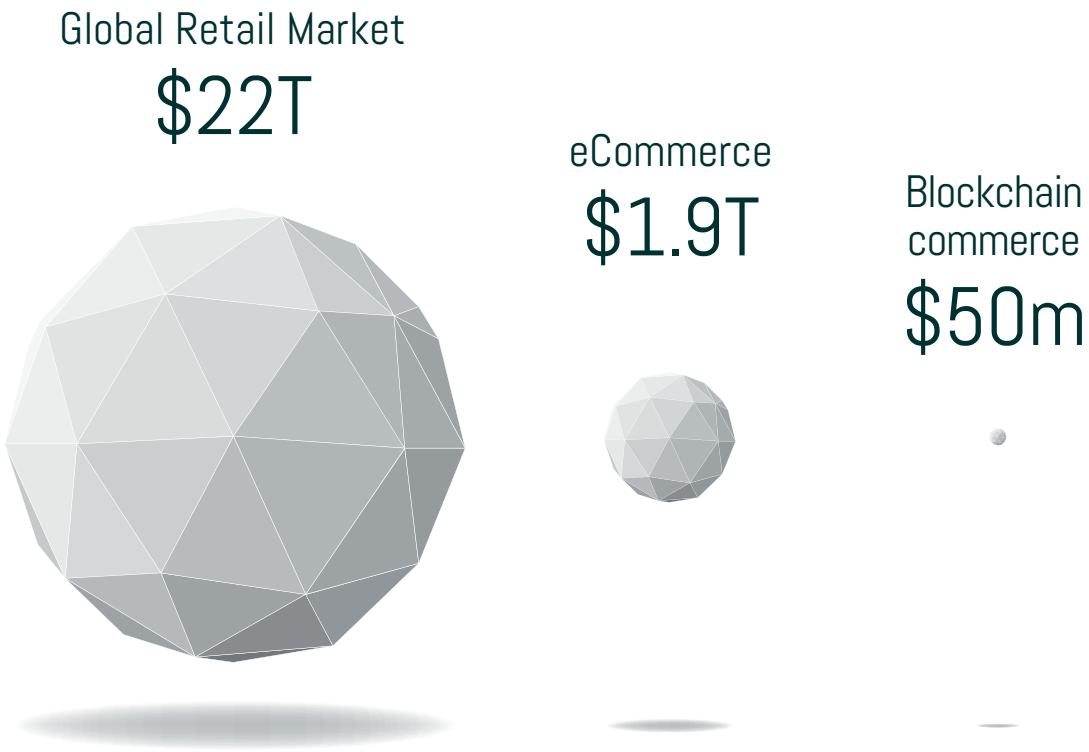
Contents

Disclaimer

All of the information presented in this whitepaper is tentative and is subject to change at any time. None of the information herein should be construed as legal, accounting, or investment advice of any kind. This document does not represent a solicitation for investment, nor does it represent an offering or sale, public or private, of any kind of financial instrument, security or otherwise, in any jurisdiction. This whitepaper is provided as-is, for informational purposes only, with the intention of describing a prospective software system.

Executive Summary

The global retail market is $22T a year, and eCommerce represents $1.9T [1], just over 8.5% of all yearly global retail. Blockchain commerce, on the other hand, represents under $50M in total volume, the sum of all products purchased using cryptocurrencies [2]. This volume is incredibly small; for every $440,000 of commerce conducted, just $1 is paid for using cryptocurrencies.



In this paper, we offer a vision for a solution that addresses the key challenges standing in the way of mainstream blockchain commerce.

This comprises a technology stack that solves 3 basic problems:

1. Lack of **consumer protection for buyers** that purchase items using cryptocurrencies;
2. Lack of a transparent reputation platform that verifies the reliability and trustworthiness of sellers;

3. eCommerce sellers across the world suffer from a high incidence rate of fraud; chargeback losses are projected to hit **$31B by 2020** [3], over 1.5% of all transaction volume [4].

We propose Verify, a distributed reputation protocol deployed on the Ethereum blockchain that monitors and continually updates the reputation of the various parties involved in a transaction. This results in a public, provably valid reputation record for buyers and sellers as rated by their counterparties. Finally, this reputation data is used in various ways to incentivize reputed sellers and buyers to continue using the Verify protocol.

A reputation protocol without data is futile; we, therefore, propose a novel solution built on the Verify reputation platform that simultaneously addresses the key consumer protection issues that blockchain buyers face today and collects the requisite data necessary to bootstrap the reputation protocol (i.e. to solve the “coldstart” problem).

By building this infrastructure layer for blockchain commerce, we foresee exponential growth in blockchain commerce in the years to come, as more buyers and sellers opt to use Verify for the protection, speed and convenience that it offers relative to traditional alternatives. Verify is built by veterans of the financial industry, having previously onboarded *thousands* of sellers on traditional credit card gateways, before acquisition of their company by Amazon in 2017 [5].

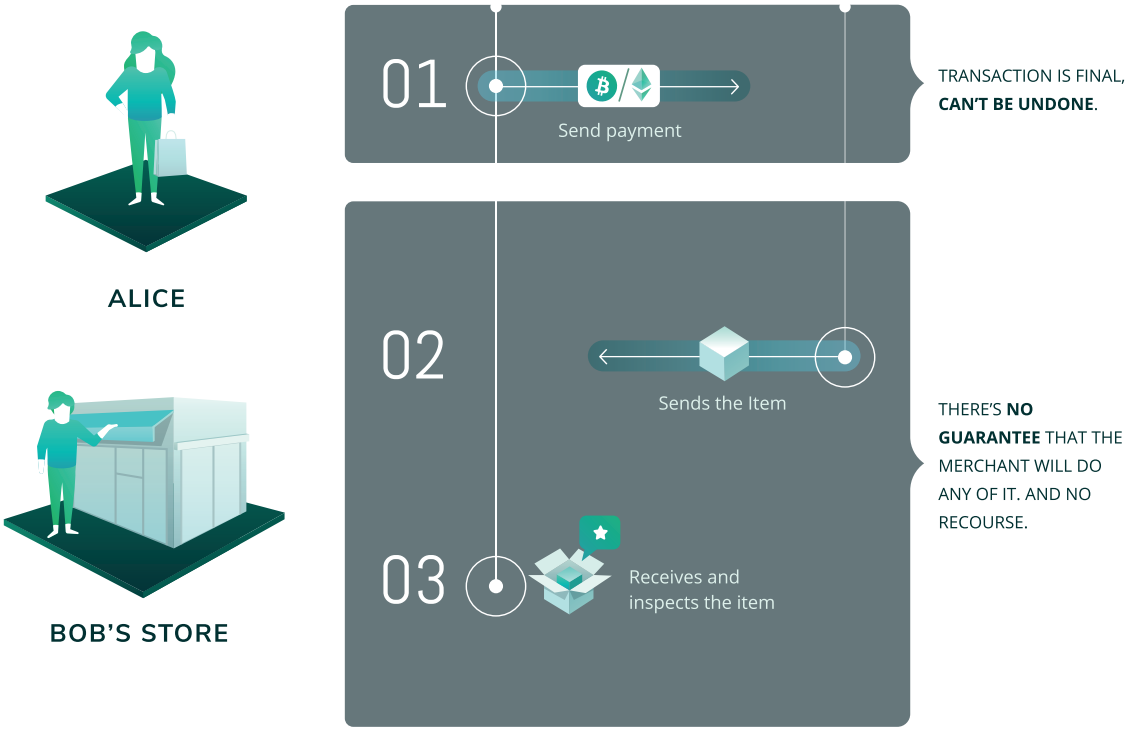
1. Introduction

The blockchain was made public in 2009 through a whitepaper published by the mysterious person or entity known as Satoshi Nakamoto [6]. Through the novel use of groups and hashes, the blockchain allows transactions to take place in a trustless environment -- one where not all of the participants can be trusted to act in a benign manner. In this way, blockchain transactions disintermediate a process that traditionally required the reliance on a trusted third party.

While undoubtedly useful in a myriad of ways, blockchain transactions do **not** fit the current commercial model of the world. This is immediately evident by close inspection of any blockchain transaction in a commercial setting. Today, you pay first *then* receive the items you purchased (e.g. through a courier). Payments represent just the first step in a series of steps that together comprise a single "transaction".

> Q: "What opportunities do you see in eCommerce?"
>
> Vitalik Buterin: *"Reputation and escrow"*, October '17 [7]

Consider the example below, where Alice attempts to purchase an item (say a pair of sneakers) from Bob's store:



A number of problems become immediately apparent, for both the buyer (Alice) and the seller (Bob):

Challenges facing buyers

- The buyer is required to pay for a transaction, with no guarantee that the good or service that they are purchasing will be delivered. Further, since blockchain transactions are **final**, Alice has made a final, irreversible payment to Bob's store with no guarantee that she will ever receive the product she paid for.

- Buying from sellers, especially sellers without a strong brand presence, is risky because one is unsure if the seller is trustworthy. Further, some sellers share "fake reviews", leading to confusion among buyers as to the authenticity of such reviews. Some sellers may even ship unoriginal products or empty boxes to buyers.

- Buyers do not have an efficient method for using cryptocurrencies to purchase physical goods. Existing solutions rely on interfacing with costly credit-card networks resulting in a circuitous and inefficient method for processing payments that provides clunky consumer protection.

Challenges facing sellers

- Low payments volume via cryptocurrencies means sellers have to rely on traditional financial instruments like credit card payments, resulting in higher transaction fees paid out by suppliers to these providers. The low cryptocurrency volume can be attributed to several factors, the primary factor being low buyer-seller trust (a particularly acute problem for newer sellers) [8, 9, 10]. If a buyer pays with a credit card and does not receive their purchase, they can file a dispute with their bank and receive their funds through a chargeback. No such recourse exists for cryptocurrency buyers. Additionally, friction in the checkout experience, exacerbated by the proliferation of coins like BTC, ETH, and many other altcoins further reduces the conversion rate for cryptocurrency payments.

- Volatility: handling payments in cryptocurrency exposes the sellers to volatility risk on their cryptocurrency holdings relative to fiat. Today, the majority of suppliers do not accept cryptocurrency payments, meaning that sellers necessarily require built-in conversion to fiat in order to meet their business payables. While converting the coin balances to fiat through a traditional exchange on a set schedule (e.g. daily) is possible, the high volatility could still expose the seller to significant losses.

The examples used throughout this paper will focus on "transactions" in the context of commerce (with an item, a buyer and a seller). This definition is evident, and the use of reputation in this context will be explored in detail. However, transactions possess a broader definition that spans any value-based exchange between two or more parties. Examples include:

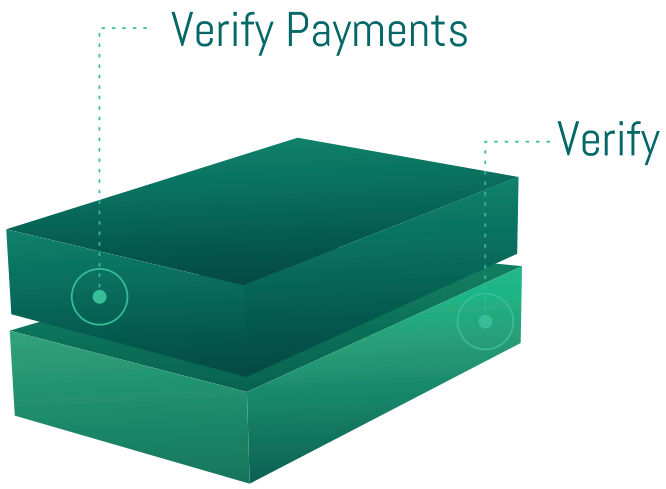
- Retail transactions conducted in person (e.g. checking out at the supermarket)

- Transactions involving digital goods and services where no shipping is required (e.g. SaaS products, eBooks, online ads)

2. Vision

Verify is composed of two connected, but distinct layers:

- Verify Reputation Protocol
- Verify Payments



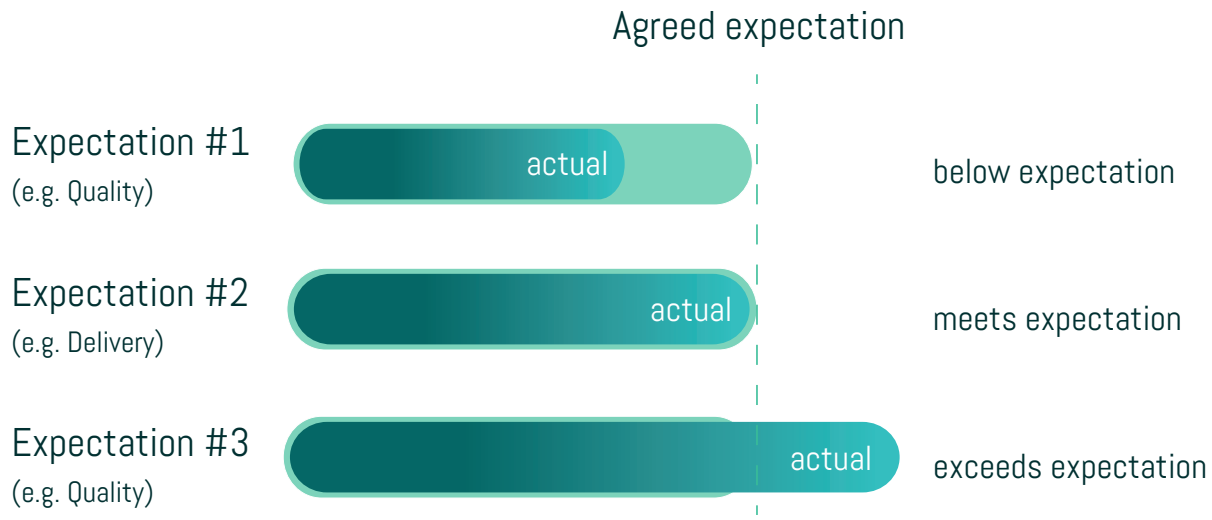
2.1 VERIFY REPUTATION PROTOCOL

Transactions cannot be conducted without some level of trust [11], and the Verify Protocol is the underlying reputation protocol that manages trust between the different participants in the network (i.e. buyers and sellers).

What is Reputation?

Reputation is, in its essence, a value that sums up the “rating history” of all previous transactions undertaken on the Verify protocol (as rated by the counterparty) and a confidence level in that value [10]. An example of an entity’s reputation may be: [★★★★☆, 11] where ★★★★☆ represents the rating history and 11 represents the total number of transactions conducted (the higher the number of transactions behind a rating, the more confidence we have in that rating). Note that this example is simply an illustration of the concept and does not represent the reputation data types or scales that are actually used in Verify.

Consider the broad definition of a “transaction” that we used earlier: a transaction is any financial agreement between two or more parties. The transaction has both an expected output (based on the agreement) and an “actual output” based on how the parties acted throughout the transaction. Reputation is a measure of the differences between the expected, agreed actions and the actual actions taken by each party, over the entire history of the buyer or seller.



The Reputation Protocol

The Verify reputation protocol is comprised of three key components:

- Participants on the network (i.e. buyers, sellers)
- Transactions
- CRED tokens

Every new participant on the network starts without any reputation, but this changes the moment they start engaging in transactions with other network participants. Transactions over the Verify protocol can only be processed if they have an associated “insurance policy”, which is funded using CRED tokens. These insurance policies are conceptually similar to transaction fees on traditional credit card networks and are also evaluated as a percentage of the original transaction amount. However, their primary purpose is to ensure that both buyers and sellers are protected, and that buyers can be reimbursed if they are unsatisfied with the transaction.

It bears reiterating that transactions on the Verify protocol do not necessarily refer to just eCommerce transactions; any value-based exchange between two or more parties is considered a trans-

action. The Verify protocol provides the underlying infrastructure that enables trust-based transactions.

We initially considered "importing" reputation data from various sources (e.g. Amazon, eBay, etc.) in order to provide value to users of the Verify reputation protocol from day one. However, we decided against retrieving data from third parties for several reasons:

- The logistical challenge of tying identities between the source and target platform (e.g. linking an Amazon review to an Ethereum address on Verify)
- Different platforms rate the parties on different criteria [12]; how does one map reputation in a consistent and fair manner?
- There is no incentive for merchants with large reputation data stores to share the data with 3rd parties (in fact, the incentive is just the opposite: to protect and safeguard the data).
- Importing data from central repositories exposes Verify to various reputation attack vectors (described in detail in Section 4.3 Abuse Prevention)

Choosing not to use an existing reputation repository means Verify has no reputation data present in the network's genesis state, without which the network cannot provide any value. We address this challenge directly through the introduction of Verify Payments.

2.2 VERIFY PAYMENTS

> *"lots of startups pitch these sorts of reputation systems to me, but they lack distribution or data to solve the coldstart problem"* -- Hunter Walk, Homebrew Capital

The primary challenge facing any protocol, particularly reputation protocols, is one of adoption. This challenge is similar to one that many marketplaces face early on: a marketplace is said to have "network effects" if it grows in value over time, but there remains the question of how the early users of the network will be enlisted, i.e. the "coldstart problem" [9, 13, 14]. Our solution is to introduce a "killer app", one that provides an inherent utility to users of the platform, even in the absence of the strong network effects early in the life of the platform. This killer app is Verify Payments.

Verify Payments provides a compelling, unique value proposition to buyers and sellers alike, while also growing the underlying Verify protocol and seeding it with the reputation data -- that will allow

even more applications to be built on top of it in the future. This self-reinforcing cycle will continually improve Verify Payments and the Verify protocol.

Verify Payments solves two issues previously considered irreconcilable on both sides of any commercial transaction:

- It allows buyers to receive 100% purchase protection on any and all orders they place
- Reputed sellers to get paid almost instantly on the majority of their orders

This is achieved at a low fee for sellers, comprising only a per-transaction “insurance fee”. These features are incredibly important and must be resolved in order for cryptocurrencies to be used safely online. In fact, US CFPB announced on 18 October 2017 that any payment solution must provide users with a mechanism for disputing transactions that are processed on their platform. [15]

The mechanism behind this groundbreaking solution is described in detail in Section 4. Before discussing the Verify Payments solution, it is important first to understand the reputation protocol it is built on: the Verify Reputation Protocol.

3. Verify Reputation Protocol

So far, we have discussed the core components of a reputation protocol, namely: the participants, transactions and reputation. Before we proceed to discuss *how* the reputation system is designed, it is important to clarify a crucial point around transactions: trust.

Trust-based transactions form a central part of a reputation protocol, and a distinction must be drawn between transactions that do not rely on trust and those that do. “Automated” transactions, which are deterministic and have a guaranteed outcome, are transactions that **do not** require trust. An example is a distributed exchange with cryptographically enforced smart-contracts that atomically swap one token for another (e.g. 0x, Airswap). The outcome of such transactions is guaranteed, regardless of the reputation of any of the parties involved.

However, most “normal” transactions we encounter in our day to day lives are not of this form. The action is carried out by the parties directly determine the outcome of the transaction, an outcome that is *not* guaranteed. This applies to the vast majority of commercial transactions, whether they are carried out online (e.g. a purchase from a seller’s website, where the item is later delivered) or in person (e.g. buying an item from a store). In the case of eCommerce transactions, the seller commits to shipping the item that the buyer has purchased, but there is no guarantee that this will take place. The buyer must trust the seller to deliver the item. It is these transactions, which carry reputation, that a reputation protocol is designed to facilitate.

3.1 REPUTATION: HOW IT WORKS

Reputation is essentially an entity’s history of all previous transactions conducted over the Verify protocol, and the resulting feedback (positive or negative) imparted by the counterparty. While reputation primarily refers to the seller’s score (as rated by the buyer), it is maintained for all participants in the network including buyers. Buyer’s reputation is important to track, especially in the context of fraud-prevention, which will be discussed in detail in Section 4.3.

> Reputation is similar to one’s CGPA at university:
>
> cumulative and permanent.

A key feature of reputation is that it can only be influenced by verified transactions, transactions that have taken place over the Verify protocol. This property is important to protect against multiple reputation attack vectors (addressed in Section 4.3).

The mechanism governing reputation calculation in the general case is described as follows (see Section 5.1 for implementation in Verify Payments):

1. Establish clear expectations from the parties engaging in the transaction. These expectations vary depending on the transaction, but an example may be:

    a. Buyer to pay a certain *amount* (in stablecoin)

    b. Seller to provide *item* by *date* in *condition*. The item should be described in as much detail as possible.

2. Buyer initiates the transaction by fulfilling their obligation and transferring the mutually agreed amount to the Verify escrow account.

3. A portion of the transaction amount is set aside as an "insurance fee" on the transaction and retained by Verify as company revenue. This amount must be settled in CRED tokens.

4. The remaining funds are stored in escrow until the transaction is completed (either through a confirmation from the seller or once the deadline has passed). When the transaction is closed, there are two possible outcomes:

    a. Buyer is satisfied: funds are immediately released to the seller in full.

    b. Buyer is unsatisfied: funds remain on hold, and the dispute resolution process is initiated (the exact process is discussed in Section 4.1.3).

5. Reputation is updated for both parties **simultaneously** (to prevent retaliatory attacks [16, 17]). The impact that a transaction has on each party's reputation is defined by application but consistently applied across all users of the application.

Applications built on the Verify protocol extend the core process established here with application-specific implementations.

3.2 CRED TOKENS

Retaining a dual meaning for both credibility and credit, CRED tokens are core to the Verify protocol and have the following properties:

- Just as no transaction can take place in the absence of trust, the same stands true for CRED tokens and the Verify protocol. In essence, the CRED represents the “trust” in a transaction, and no transaction can take place on the platform without an “insurance policy” in the form of CRED tokens.

- Using the vending machine analogy, when you insert CRED tokens into a (protocol) vending machine, you receive an “insurance policy” that can be used to cover a commercial transaction (e.g. when buying an item, you are insured against seller fraud. Your purchase of the CRED token funds this protection policy)

Traditional payment instruments levy transaction fees on all transactions, a relic of the traditional financial infrastructure where each party adds a layer of fees atop the layer below. It comes as no surprise that credit card processors have instituted multiples forms of hidden fees including transaction, interchange, card processing, setup, currency conversion and chargeback fees. It is not fitting to retain this same fee structure on the blockchain, where many of these fees are baseless, and even the mining fee used to process a transaction is exceedingly low compared to the median transaction value.

For this reason, Verify foregoes the transaction fee altogether and only levies an insurance fee of 1% of the transaction value from the sellers. This fee may be reduced as the provider (seller) gains reputation to reflect the reduced insurance risk that they represent. Applications built on the Verify protocol (like Verify Payments) may choose to levy their own fees to better reflect their cost structure, but this represents the cost structure for these applications (the insurance fee is retained by Verify and recognized as company revenue).

4. Verify Payments

Verify Payments is the first application built on the Verify protocol. In this section, we describe the core features that make Verify Payments superior to any payment solution in existence, for both buyers and sellers. Further, the Verify Payments solution will bootstrap reputation data on the Verify protocol, enabling it to grow at a much faster rate, incentivizing other providers to build applications on the Verify protocol further fueling this growth cycle.

4.1 BUYER PROTECTION

The cryptocommerce economy is in dire need of a consumer protection facility [18]. An eCommerce transaction simply cannot be safely conducted online without some form of consumer protection. With the ongoing proliferation of websites, there are billions of potential outlets for online sales and every transaction is a risk. Conversely, many buyers have chosen to limit their shopping to specific outlets (e.g. Amazon, Walmart) resulting in ever higher centralization on the Internet.

Verify Payments offers 100% buyer protection against all forms of seller fraud, including:

- Non-delivery
- Delivery to an incorrect address
- Lost shipments
- Delivery of the incorrect item
- Delivery of an item that does not meet the description provided by the seller

It is important to note that *every single transaction* conducted on the Verify Payments network will receive this level of protection.

Further, sellers have the option to offer “no questions asked” refunds for a set duration of time after delivery, and this guarantee is cryptographically enforced by a smart contract. Sellers that offer this option send a strong signal to their buyers that they care deeply about their customers, and are willing to stand by their word. Verify Payments employs several mechanisms to protect sellers against buyer abuse of this feature; these techniques are discussed in Section 4.3.1.

Buyer Protection is also supported by several key mechanisms described below.

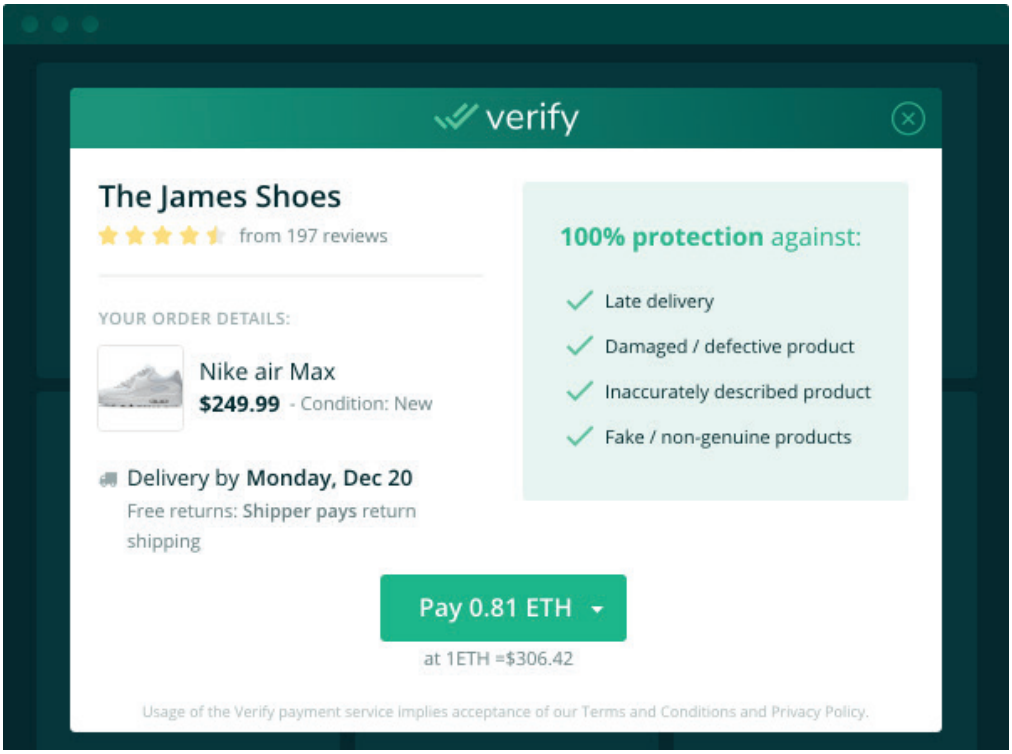
4.1.1 Improved Checkout

This may seem unintuitive at first glance but buyer protection actually begins *before* the transaction takes place. It is essential that both parties to a transaction establish clear expectations; taking the time to do this prior to a transaction is often all that is required to avert numerous disputes down the road.

The seller's expectation of the buyer is straightforward; the buyer should pay the seller the transaction amount. The buyer's expectation, however, is more nuanced, and depending on the product or service being provided could include:

- *What* is the item being sold?
- What *condition* is the item being sold in?
- *When* will the item be delivered?
- Who pays the *return shipping cost* if the buyer is unsatisfied with the item?

Verify Payments provides an intuitive way for sellers to share this information with their buyers prior to the transaction settlement, and record it alongside each transaction that is completed. All of this information is automatically retrieved from the website's shopping cart system.



The buyer is also able to see the seller's reputation, as rated by previous buyers.

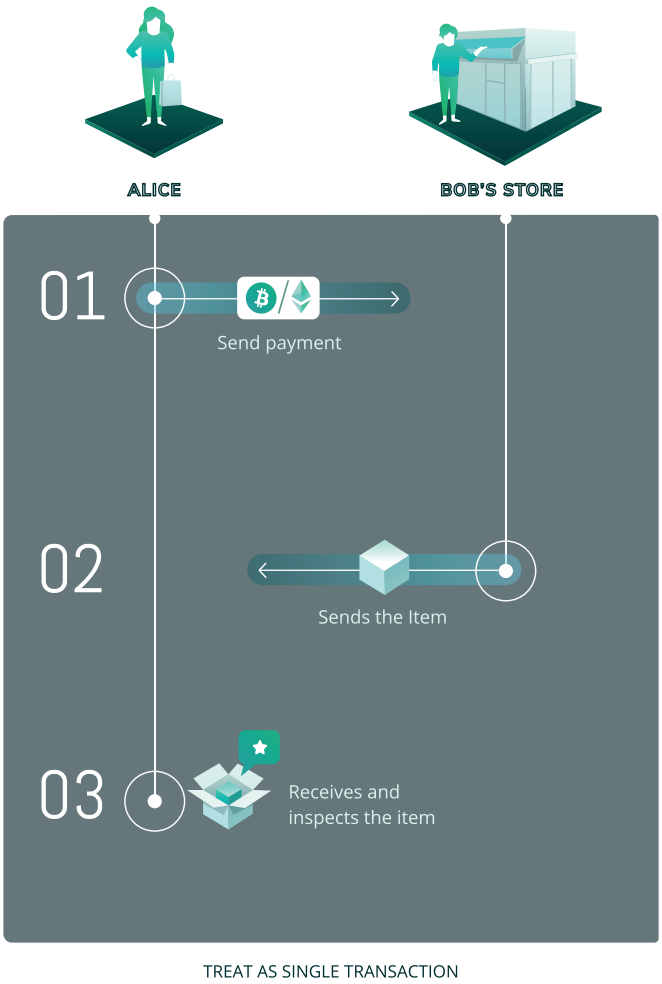
Additional features include:

- Buyers are able to pay in any cryptocurrency they like.
- The checkout page is continually improved, based on conversion data leveraged from the entire Verify Payments ecosystem.
- One-click integration with all major shopping cart providers (Shopify, WooCommerce, Magento, etc.)
- Buyers receive an email confirmation once the transaction is completed, with all of the details related to the purchase. Further, this email contains a link for filing a dispute directly through Verify Payments.

4.1.2 Built-in Escrow for Atomic Transactions

Verify Payments lies between the buyer and the seller, and all buyer payments are made directly to the Verify Payments smart contract. In this manner, Verify Payments is able to solve the trust disparity between the two parties and provide buyer protection across the entire transaction lifecycle. Furthermore, this trust layer allows buyers to transact in confidence with unfamiliar sellers, a feature that is particularly important to new sellers and those that sell expensive items.

A key point to note is that the *entire* transaction is treated as a single atomic unit; either the whole transaction is successfully executed (and the funds are released from buyer to seller), or the entire transaction is rolled back (with the buyer receiving their funds, *and* the seller receiving their item):



This seamless solution offers buyers peace-of-mind. In addition, the advance payment feature provides the seller with a powerful incentive for using Verify Payments, a topic we cover in detail in Section 4.2.

4.1.3 Decentralized Dispute Resolution

In the case of a dispute, buyers and sellers are given the opportunity to resolve the dispute mutually by direct chat over the Verify Payments platform. If a resolution is not reached, the Verify Payments team will step in to arbitrate the dispute.

The dispute resolution process is described below:

- The buyer initiates the dispute by clicking on the “File a Dispute” link in the confirmation email they received from Verify Payments when they completed the payment. Alternatively, the buyer is able to search for their purchase through the Verify Dashboard using the email address used during the purchase. Once the email address is provided, a confirmation code is sent to the address to confirm the user’s identity before any details are displayed.

- The buyer provides details about the reason for the dispute. Since Verify Payments is aware of the items ordered and the shipment status (due to our integration with 3rd party shipping APIs), the buyer selects from a predefined list of the most common dispute reasons based on the shipping stage.

- The buyer is connected directly with the seller, and they are given 3 days to reach a mutual agreement.

- If the buyer and seller are unable to resolve the dispute amicably within the defined period, a member of the Verify team will step in to review the evidence and arbitrate the dispute. With visibility to the evidence submitted by both parties, the reputation of both parties, the chat log from the buyer/seller discussion and up-to-date product and shipping information, a decision is then reached and shared with both parties. The decision could either be (a) no refund to the buyer (if the claim was found to be fraudulent or without basis), (b) a partial refund or (c) a full refund of the entire transaction amount. If a refund is approved, the buyer returns the item to the seller and shares the shipping tracking number before the refund is disbursed. The seller's predefined policy regarding shipping fees takes effect (the seller can either choose to cover the cost of return shipping, or request that buyers pay the shipping fees). This policy is highlighted on the checkout page before the buyer makes the payment.

Common issues will be reviewed and codified into smart contracts, automatically resolving future occurrences of identical issues and decentralizing the dispute resolution process. The role of human resolution operators, when required, will ultimately be reduced to that of human oracles with the limited responsibility of reviewing evidence and classifying the dispute into one of several categories (with the effects of this classification automatically executing the desired end result, via a smart contract). This reduces the opportunity for human error, while also ensuring fair, consistent treatment to all buyers and sellers across the platform.

A key component of the dispute resolution process is establishing clear expectations from both parties before the transaction has taken place. By creating a custom checkout experience for buyers, we are able to incorporate this crucial information directly on the checkout page - thereby reducing the occurrence of disputes stemming from mismanagement of expectations. This approach was described in detail in Section 4.1.1.

It should be clear from the above description that this process is very different from a traditional escrow or multi-sig wallet:

- Verify Payments integrates directly into the checkout process. This ensures minimal friction to buyers, who would otherwise resort to a manual, off-chain escrow service facilitated by a trusted 3rd party. Further, Verify Payments is able to register seller-specific details (IP address, browser fingerprint, etc.) later utilized in fraud-detection, a process described in detail in Section 4.3.1.

- Verify Payments is designed for the explicit purpose of facilitating commerce transactions, unlike generic escrow services. By integrating with providers both on and off-chain, Verify Payments is able to reduce the opportunity for human error, resulting in more fair and consistent treatment to buyers and sellers alike.

- As sellers develop a reputation on the platform, they are able to leverage their reputation in increasing their credit ceiling, resulting in improved cash flow over time (especially valuable to seller's as order volume increases). This mechanism is described in detail in the following section.

4.2 ADVANCE PAYMENT TO SELLERS

4.2.1 Credit Ceilings

It has already been established that most transactions of the type we encounter in our daily lives require trust in order to take place. The insurance fee levied in CRED tokens helps facilitate this trust on the Verify protocol. This arrangement is sufficient to provide buyer protection, since the entire transaction value is retained in escrow until the buyer receives their item and indicates their satisfaction. However, this comes at the expense of sellers -- who, in traditional escrows, are left waiting for transactions until delivery (in addition to a buffer period to allow the buyer time to respond). Depending on the shipping option used, this could take well over a month and cause sellers dramatic cash flow challenges. If left unaddressed, this could represent a severe hindrance to the market adoption of the Verify Payments platform.

To address this issue directly, the Verify Payments platform has established a credit facility built directly on the underlying Verify reputation protocol. A Credit Ceiling is defined as the maximum **fiat** amount that a seller is **currently** allowed to obtain in credit as **advance payment** for transactions already **shipped**.

There are several key features in the previous statement worth dwelling on:

- Limit in fiat: The credit ceiling is allocated to individual sellers, in fiat currency. All sellers start with a credit ceiling of $0, and the ceiling increases with reputation. The goal is to eventually allow most reputed sellers to receive immediate payment for the majority of their orders.

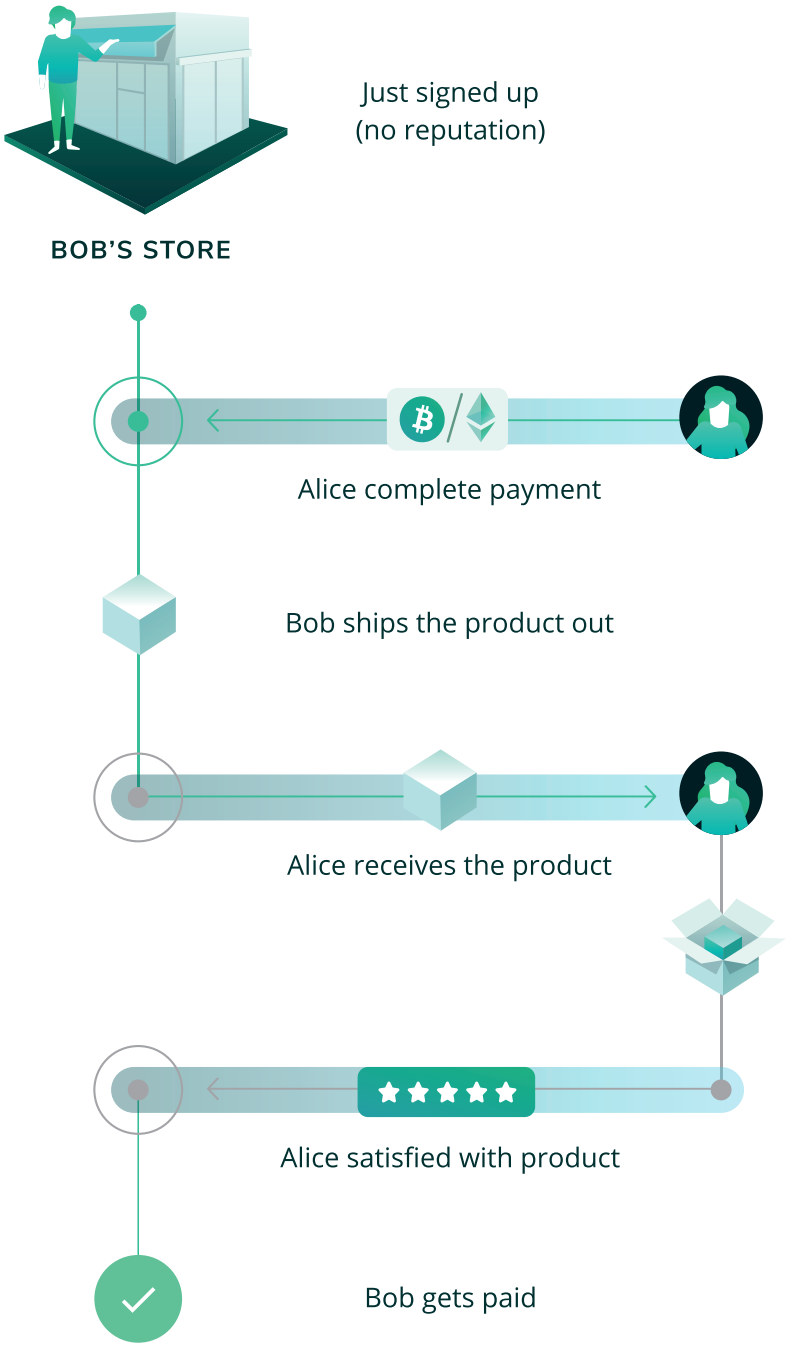
- The ceiling can increase or decrease over time, depending on several factors including the reputation distribution over the Verify protocol. Reputed merchants will always be offered higher credit ceilings than non-reputed ones.

- Advance payment: The credit ceiling is applied *exclusively* to advance payments on fulfilled transactions. It cannot be used for any other purpose and is *not* a business loan.

- Shipped: Only transactions where the order has already been shipped are eligible for advance payment. This incentivizes the seller to ship products as soon as possible, while also ensuring that they share the shipping details on the Verify Payments network. The shipping details are cross-verified with the integrated shipping APIs to ensure validity.

Every seller on the platform starts off with no reputation and therefore, a $0 credit ceiling. As this seller transacts on the network and gains reputation, their credit ceiling is raised -- enabling the seller to receive advance payments on transactions up to their credit ceiling. As the seller continues to use the platform, this ceiling is further raised until the seller is able to receive virtually immediate settlement for all transactions made on Verify Payments.

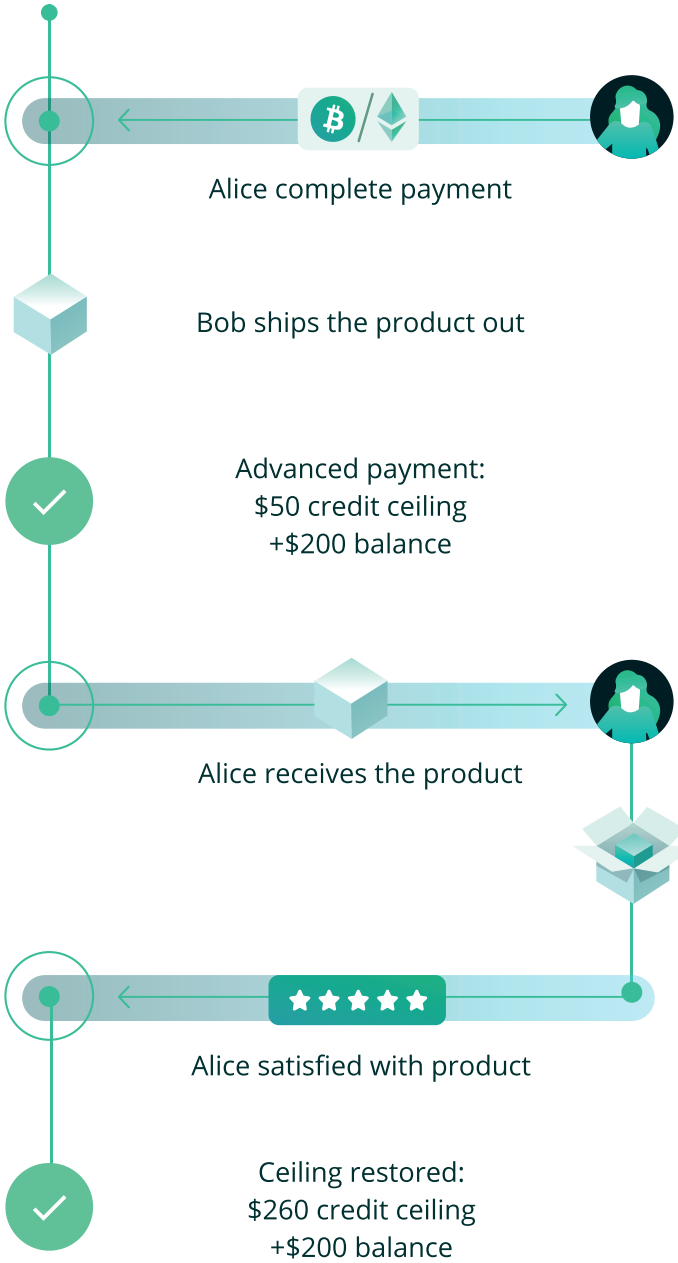
Consider the example below, where Alice wishes to purchase a pair of $200 sneakers from Bob's store. Bob has just started using Verify Payments, and has no reputation on the platform:



Scenario 1: New seller, credit ceiling is $0 (No advance payment)

BOB'S STORE

250$ credit ceiling
0$ balance



Scenario 2: Established seller, credit ceiling for seller is $250

In this scenario, Bob must wait until Alice indicates her satisfaction with the product before the funds are settled to his account. However, as Bob transacts on Verify Payments, his credit ceiling is raised to reflect the increase in his reputation. Consider the transaction flow below at a point where he has already earned a $250 credit ceiling:

Take a moment to consider the implications here. Alice receives 100% buyer protection, and Bob receives immediate settlement on the same transaction. This is unheard of and differentiates Verify Payments from *every* escrow solution on the market. Without a reliable underlying reputation platform, it would be impossible to extend credit (which is essentially what an advance payment is) to sellers without some guarantee of return. By utilizing the Verify reputation protocol, Verify Payments effectively holds the seller's reputation as collateral for a transaction. Once the transaction is successfully completed, the credit ceiling for the seller is restored (using the transaction amount released from escrow) and the seller's credit ceiling is increased (to reflect the seller's increased reputation).

The credit ceiling is facilitated through the use of the Verify Fund, described in the following section. The rules governing the issuance of credit ceilings to prevent abuse can be found in Section 4.3.2.

4.2.2 The Verify Fund

In order to fund the credit ceiling extended to sellers, we will set aside a portion of the total available CRED tokens for funding the Verify Fund. The Verify Fund is the source of the credit ceiling allotted to reputed sellers on the network. While the Verify Fund is funded entirely in CRED tokens, the credit ceiling is allocated in fiat based on the current exchange rate the moment the credit is utilized.

The goal of the Verify Fund is to incentivize adoption of the Verify Payments platform; addressing the key objection standing in the way of sellers using the platform in the first place is the most effective method for doing so. The platform has visibility to the reputation of all the participants on the network and can efficiently allocate capital to the most promising sellers (those with the lowest fraud/default risk).

4.3 ABUSE PREVENTION

Verify Payments introduces several innovative features that facilitate crypto-commerce and enable buyers and sellers to safely and securely transact over the blockchain. However, it is crucial to ensure that these features are properly used, and limits are put in place to prevent abuse by malicious parties.

This section describes various attack vectors and the mechanisms used to mitigate the risks posed by these threats.

4.3.1 Buyer Protection

The goal of buyer protection is to protect buyers on Verify Payments from seller fraud and non-delivery due to various other non-malicious reasons. However, it is also important to protect sellers against buyers that consistently and repeatedly abuse this feature. This is especially important to sellers that offer generous return policies like the “no questions asked” policy described in Section 4.3.1.

Verify Payments will employ several mechanisms to protect sellers against buyer abuse. The atomic transaction mechanism described in Section 4.1.2 applies both ways. At the end of a transaction, if the buyer is unhappy then they would receive a full refund for the transaction only *after* the item is returned to the seller and the seller confirms that they have received and are satisfied with the returned item. It is crucial that the refund only be processed after the item is returned, thereby rolling back the entire transaction and achieving the desired atomicity. Knowing that they would need to return an item before their refund is processed will discourage many potential abusers.

Further, the Verify protocol is used to track reputation of both sellers *and* buyers. By asking sellers to rate their experience with buyers, the Verify Payments system is able to track abusive buyer patterns and take appropriate action against these parties. A question remains around how to uniquely identify an abusive user when it is cheap to generate a new cryptocurrency address. This is referred to as a whitewashing attack, where an attacker with a bad reputation attempts to “reset” that reputation by registering a new account or ID and starting afresh [19, 20]. There are various patterns employed in existing eCommerce fraud detection systems that can be used to identify abusive buyers. The technique involves combining various properties to generate a persistent profile of a buyer that transcends the individual cryptocurrency address they used to pay for the transaction. This buyer profile may include the following fields:

- Order Delivery Address
- Email address used for the transaction
- Cryptocurrency address used to pay for the transaction
- Blockchain analysis tying this address with other addresses that have a high likelihood of belonging to the same account
- Client-side device fingerprinting (which involves using a combination of various properties of the device used to pay for an order to “link” different accounts)
- Other miscellaneous signals like IP address, supercookies, etc.

These mechanisms, in aggregate, can be reasonably expected to mitigate the risk presented by buyers looking to exploit the buyer protection facility.

4.3.2 Advance Payment

A key feature of the Verify Payments platform is that it addresses the biggest objection existing sellers have to using escrow platforms: advance payments. By relying on reputation (as opposed to any other tangential signal), Verify Payments is able to effectively allocate a credit ceiling to sellers based on their performance on previous transactions, i.e. the best possible indicator of their performance on current transactions.

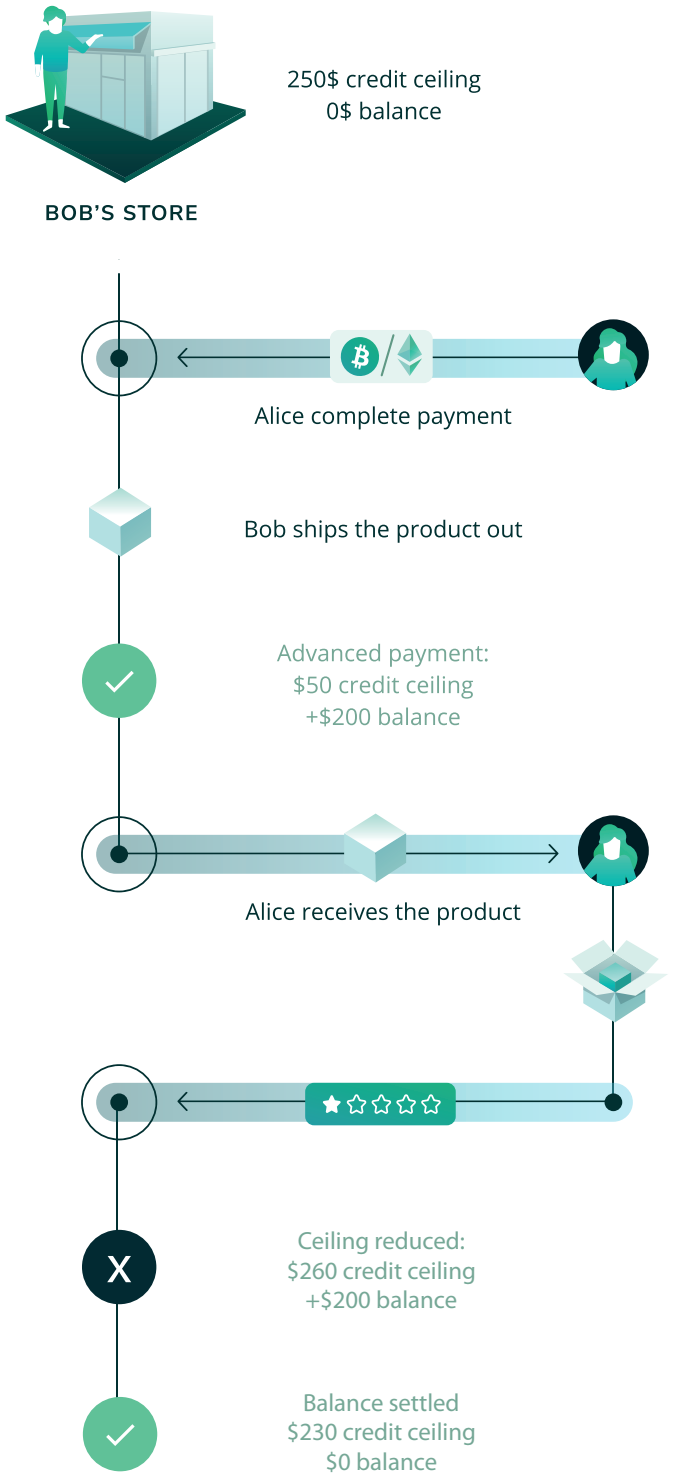
Despite this reliance on reputation, there exists a potential for abuse by sellers given the relatively high reward. In this section, we discuss various threat vectors and the corresponding solutions that will be employed by Verify Payments to curtail these risks.

An obvious risk against reputation systems is that of a Sybil attack; this is an attack that relies on forging identities in peer-to-peer networks and using them to gain a disproportionately large influence [17, 21, 22]. In the context of the Verify reputation protocol, this would entail a seller registering multiple accounts, performing many “fake transactions” in order to artificially boost his reputation and then, having accumulated a high-enough credit ceiling to make his pursuits worthwhile, withdraw this credit and depart from the platform. At this point, the entire process can be repeated, resulting in further credit theft, and so on.

A critical component of this attack is based on the attacker’s ability to create multiple accounts. An effective way to limit their ability to do so is to require Know Your Customer (or KYC) requirements from sellers -- collecting things like passport information of the principal, business registration and proof of address. Not only is it best-practice to request this information from sellers, but, in many jurisdictions, it is actually required by law to limit certain forms of financial crime like money laundering.

Another dimension to this solution is to make it difficult for an account to accumulate a large credit limit within a short period of time. A treatment of this solution is subtle; it is important to allow legitimate sellers access to credit, in some ways proportional to the transaction volume that they process, while also ensuring that the transactions themselves are legitimate business transactions. Our solution considers both of these aspects. The first facet of this solution is to prevent sellers from accumulating a high reputation in a short period of time through “fake” transactions. Here, we note various signature traits of a transaction (device fingerprint, IP address, source of funds and other patterns) to detect and reject repeated fraudulent transactions originating from a single buyer (or a network of illegitimate buyers). The mechanism used here is similar to the one described in the prior section on Buyer Protection abuse prevention. Further, the reputation calculation mechanism limits what proportion of one’s reputation can originate from a single party. The second facet includes management of the credit ceiling for sellers. Sellers are assigned low credit ceilings, and these are increased only once the seller has resolved any negative balance outstanding from previous credit issuances. This would mean that a seller will not be issued $20 credit if he has not successfully accepted and repaid a $10 credit.

We take things even further by requiring that sellers that have a negative account balance (i.e. that have received credit but not repaid it) settle this balance before they are paid out for any new transactions. This settlement is done automatically, and ensures that any credit extended to sellers is recouped in the shortest possible timeframe:



Another class of attacks include targeting attacks that happen when an attacker tries to downgrade (also called Slandering attack [23]) or upgrade another user's reputation or even their own account (i.e. self-promoting). This type of attack occurs by submitting a false review or even purposely rating another user once or even more than once (also called Ballot-Stuffing [17]) without truly interacting with the other party. In some cases, it can occur by hiring external entities to execute the attack (similar to a Sybil attack).

This solution to this kind of attack is as follows:

- Only users who have completed a transaction can rate each other.
- Only allow a single rating per user per transaction.
- Throttle the reputation contribution by counter-party (i.e. track repeated transactions made by the same counterparties and limit the contribution that any single counterparty can have on the overall reputation of a seller).
- The method used to calculate reputation should not rely on just the number of transactions but include other factors like transaction value, the reputation of the parties involved and transaction recency to name a few.

These solutions combined can be feasibly expected to provide protection against these attacks.

5. Proof of Concept

5.1 DETAILED EXAMPLE OF A TRANSACTION

The Verify Payments platform revolves around two primary participants: the seller and the buyer.

1. After browsing the seller's website and adding the items that he wishes to purchase into his shopping cart, the buyer proceeds to the checkout page. Here, the option to pay using Verify Payments is displayed prominently, and he selects it.

2. The buyer reviews the transaction details; these include the item(s) description, delivery date, and any guarantees provided by the seller (e.g. "no questions asked"). He can also read reviews left by other buyers on this seller.

3. The buyer completes the payment using any cryptocurrency they like, directly from their wallet.

    a. A portion of the total transaction amount (i.e. 1%) is used as an "insurance fee"; this payment is only accepted in CRED tokens. A small portion of the cryptocurrency that the buyer pays with is transparently converted into CRED through any of the available open exchanges. The CRED token is analogous to an "insurance policy" that provides protection for this specific transaction. This payment is kept in an escrow, held by Verify, until the consumer confirms receipt of the item and indicates their satisfaction with the purchase. At that point, the CRED payment is released to the Verify company as revenue.

    b. The transaction amount (excluding the insurance fee levied in CRED) will be converted into a stable cryptocurrency in order to mitigate cryptocurrency volatility risks. Various stablecoins will be considered for this purpose (USDTether, Sai Stablecoin, JibrelToken) but a decision as to which stablecoin to use will be made at a later date.

4. A transaction is considered successful once the buyer has indicated their satisfaction with the product that was purchased, or after a set deadline following the delivery date has passed. This is tentatively set at 3 days, but liable to change.

5. Upon successful completion of the transaction, the seller's account is credited with the stablecoin (assuming he does not have a negative balance on his account). Since the majority of sellers will opt to retain their payouts in a stable cryptocurrency (their costs to suppliers and other vendors are in fiat as well), they forego the conversion fee levied by most exchanges. Alternatively, this balance can be automatically converted to any cryptocurrency of their choice.

6. The reputations of both the buyer and seller are updated simultaneously at the end of a transaction, based on the rating each party left for the other.

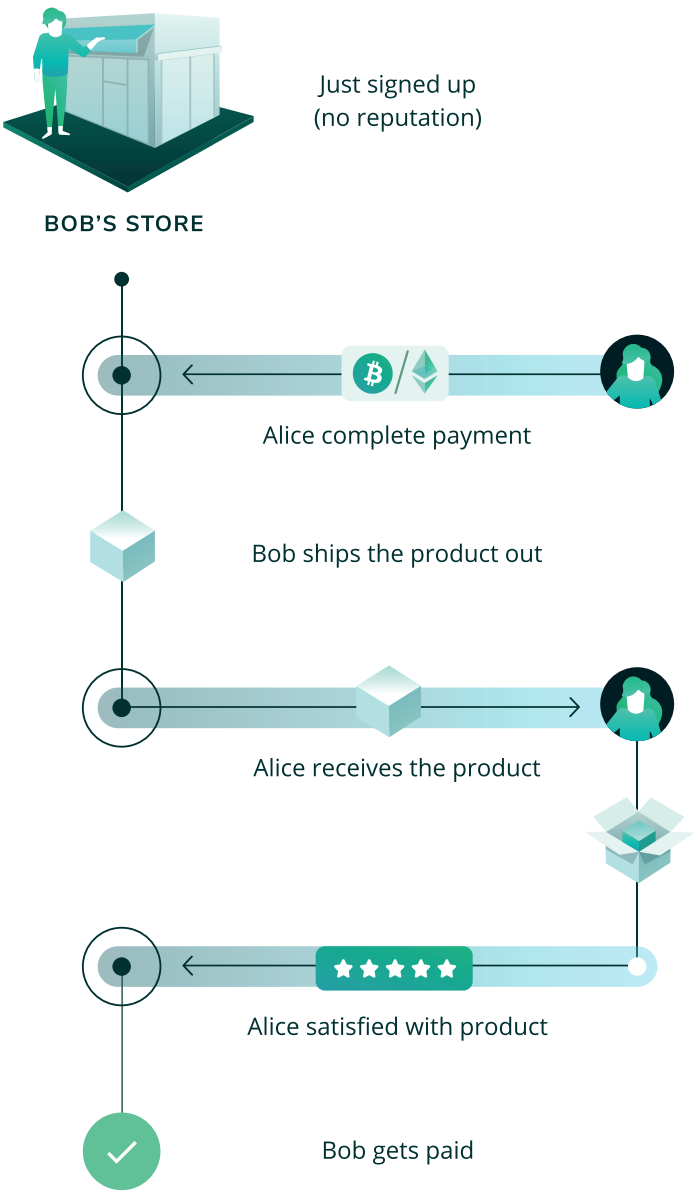
To make this more concrete, consider the example below, where:

» Alice: Buyer, purchasing a pair of sneakers

» Bob: Seller, who owns a store that sells sneakers

New seller (without credit ceiling)

When Bob first starts with Verify Payments, he has no reputation. The transaction flow would look like so:



The table below shows the change in balances:

EVENT	ALICE'S BALANCE	BOB'S BALANCE	BOB'S CREDIT CEILING	VERIFY	
				ESCROW	CRED
Alice pays for the sneakers in ETH	-1 ETH	0	$0	$0	0 CRED
Converted to stablecoin*; in escrow	-1 ETH	0	$0	$198	2 CRED
Bob ships the product to Alice	-1 ETH	0	$0	$198	2 CRED
Alice receives the product; satisfied	-1 ETH	$198	$5**	$0	2 CRED

* Assuming following exchange rates: $200/ETH; $1/CRED

** Depends on reputation (which is in turn influenced by factors including transaction amount, rating, shipping option, etc.)

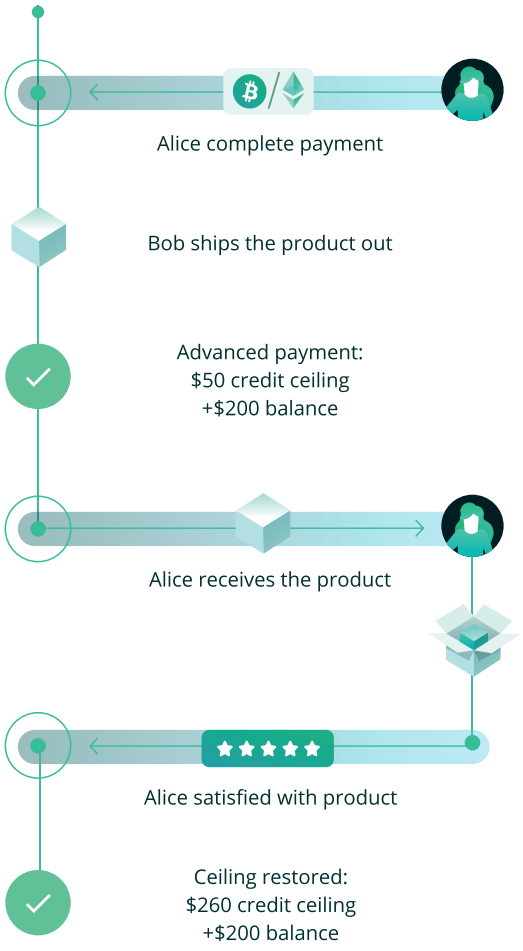
250$ credit ceiling
0$ balance

BOB'S STORE

Established seller (with credit ceiling)

As Bob's store continues to process transactions on Verify Payments, his credit ceiling grows until it eventually hits $250. At this point, Alice decides to re-order a pair of her favorite shoes.

Here is what the process looks like now:



The table below shows the change in balances:

EVENT	ALICE'S BALANCE	BOB'S BALANCE	BOB'S CREDIT CEILING	VERIFY	
				ESCROW	CRED
Alice pays for the sneakers in ETH	-1 ETH	0	$250	$0	0 CRED
Converted to stablecoin*; in escrow	-1 ETH	0	$250	$198	2 CRED
Bob ships the product to Alice	-1 ETH	0	$250	$198	2 CRED
Bob receives advance payment	-1 ETH	$198**	$52	$198	2 CRED
Alice receives the product; satisfied	-1 ETH	$198	$256***	$0	2 CRED

* Assuming same exchange rates as before: $200/ETH; $1/CRED

** This amount is withdrawn from the Verify Fund, and eventually returned to the same fund

*** The increase in credit ceiling depends on reputation (which is in turn influenced by factors including transaction amount, rating, shipping option, etc.)

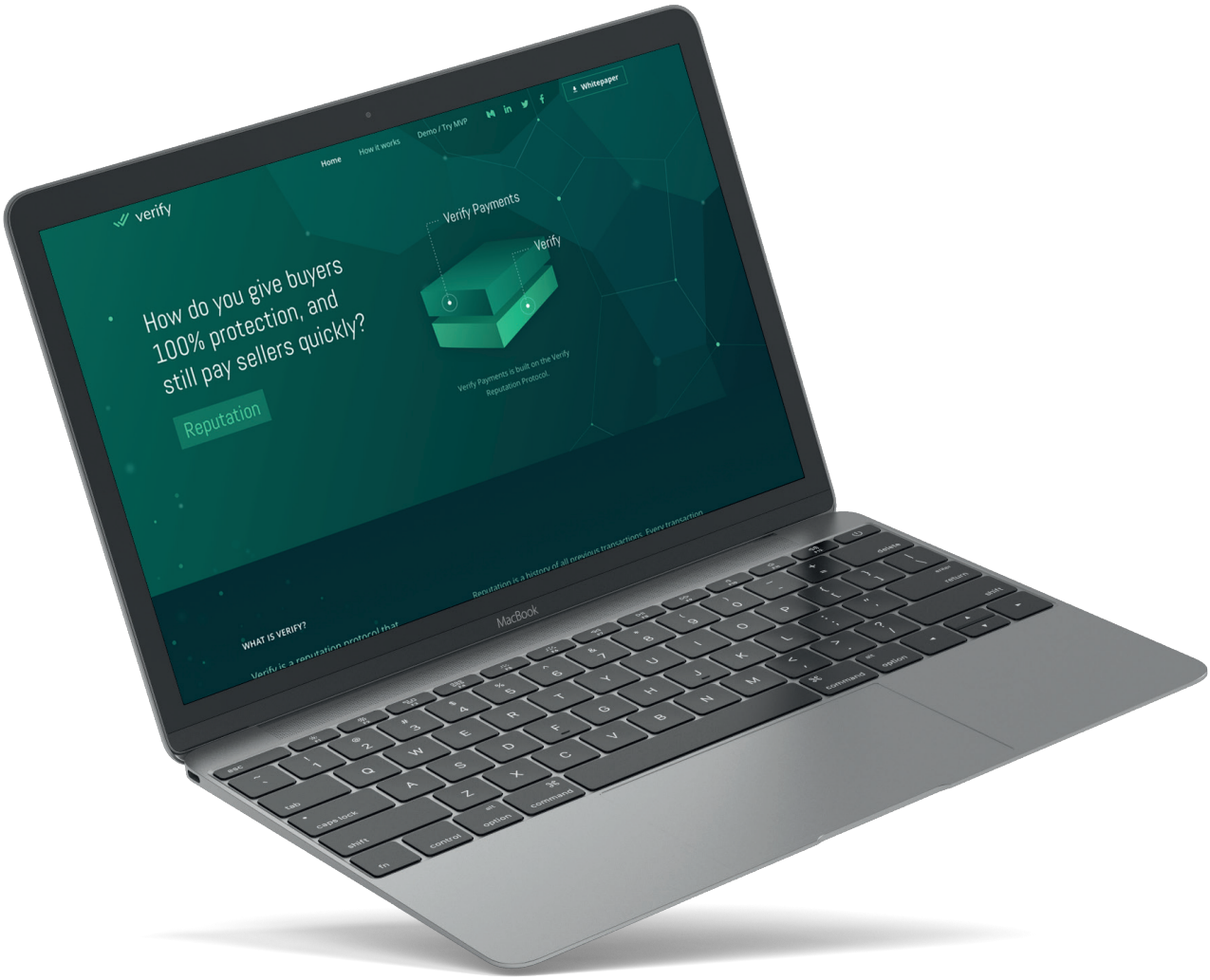
5.2 MINIMUM VIABLE PRODUCT (MVP)

A key factor in assessing the strength of a product offering is determining if a team is able to execute on the project under consideration. No matter how well thought-out an idea may be, without the operational ability to execute on the plan the project stands little chance of success.

A core facet of the Verify Payments solution is the checkout page. Until we provide sellers with a Checkout page that they can integrate, no buyer will be able to complete a single transaction. Therefore, the focus at the early MVP development phase was to create this checkout page to demonstrate the Improved Checkout experience described in Section 4.1.1.

By the time of this writing, we developed and deployed an early version of this demo checkout experience at https://verify.as/demo. We encourage readers to browse through to the demo site and try out the checkout experience for themselves!

A screenshot of the checkout page is included below for reference:



The decision to use a hosted checkout page (which overlays a modal dialog over the seller's website) enables us to make continuous updates to the embedded script to optimize the checkout flow, or improve conversion without the need for sellers to make any changes on their websites. This means we can deploy changes to Verify Payments instantly to all our sellers, anywhere in the world.

> Single integration, continuous improvement.

6. Launch and Roadmap

6.1 PRODUCT ROADMAP

A product roadmap should **not** be designed as a to-do list. We need to keep in mind that we are developing a business, and business risks change over time. It would be irresponsible to continue to develop a product that is unlikely to succeed, and that is especially true when the business has amassed significant funds in order to do so. If a business strategy is unsuccessful, then there is an opportunity for a pivot to something adjacent that may work. The best way to increase the likelihood of a business succeeding is to start with the riskiest assumptions, and gradually work your way down.

Ask yourself, what is the part of the business that has the highest amount of uncertainty and is most likely to fail? What assumptions have we made about the business are critical to the success of the business; what assumptions can we not afford to get wrong? These questions are extracted directly from the *Lean Startup* manual [24], the bible for starting a company.

In keeping with this approach, we have set the below product development roadmap -- and each milestone tackles a critical aspect of the business strategy that we would like to validate and de-risk.

MILESTONE #1: SECURE SELLERS ON VERIFY
Target de-risk date: Apr - Jun 2018

Focus would be on the basic infrastructure tasks and items on the critical path to allowing sellers to integrate and use Verify Payments in their stores. Without sellers offering Verify Payments, buyers will not be able to use it. This would include deploying v0.1 of the Verify Reputation protocol with the smart contract methods required to receive transactions and process reputation data at the protocol layer. For Verify Payments, implement and deploy the improved checkout experience and integrations with popular online store platforms to reduce entry barriers for sellers. It would also include design and implementation of the sellers' credit ceiling algorithm.

Expense Category	Min	Max
Operational Expenses (3 - 5 months)		
- Software Developers x 2	$45K	$75k
- Business Development x 1	$25k	$35k
- Professional services (Designers, Security, Audits, etc.)	$20k	$35k
- Fixed costs	$6k	$10K
Marketing	$10k	$15k
Legal (primarily driven by post-tokensale legal fees)	$100k	$200k
One-time costs (tokensale expenses, legal setup, etc.)	$300k	$400k
Total for Milestone 1	**$506k**	**$770k**

MILESTONE #2: BECOME THE PREFERRED PAYMENT METHOD FOR CRYPTOCURRENCY USERS (OVER CREDIT CARDS, PAYPAL, ETC.)

Target de-risk date: Dec 2018

Having validated the seller-side of the business, focus now shifts from sellers to buyers. The goal is to improve the checkout experience with a focus on establishing expectations, highlighting buyer protection features and usability. Dispute resolution features are also built out, including a dashboard to facilitate interaction between buyers, sellers and the dispute resolution team. Verify Pay-

ments should become the default payment method for all cryptocurrency users (those with an existing cryptocurrency wallet).

Expense Category	Min	Max
Operational Expenses (6 - 9 months)		
- Software Developers x 2	$90k	$135k
- Business Development x 1	$50k	$75k
- Professional services (Designers, Security, Audits, etc.)	$40k	$60k
- Fixed costs	#12k	$18k
Marketing	$50k	$85k
Legal (ongoing support)	$20k	$35K
Total for Milestone 2	$262k	$408K

MILESTONE #3: BECOME THE PREFERRED PAYMENT METHOD FOR ALL USERS, INCLUDING NEW NON-CRYPTOCURRENCY USERS

Target de-risk date: Late 2019

By this point, we have already captured a significant share of the cryptocurrency market in terms of both buyers and sellers. The goal becomes to convert users that have never used cryptocurrencies to Verify Payments users. We provide a strong value proposition to such users over existing payment methods, so focus shifts to integration with 3rd party providers like exchanges and wallets that simplify the process of purchasing cryptocurrencies using fiat (and then using them on Verify Payments). Our goal at this point is to grow the total addressable market by growing the cryptocurrency ecosystem.

Expense Category	Min	Max
Operational Expenses (12- 15 months)		
- Software Developers x 3	$270K	$338k
- Business Development x 2	$216k	$270k
- Professional services (Designers, Security, Audits, etc.)	$75k	$120k
- Fixed costs	#48k	$60k
Marketing	$85k	$135k
Legal (ongoing support)	$20k	$35K
Total for Milestone 3	**$714k**	**$958K**

MILESTONE #4: POWER OTHER APPLICATIONS ON THE VERIFY PROTOCOL
Target de-risk date: Early 2020

With a battle-tested protocol and a healthy Verify Payments business, the Verify reputation platform takes center-stage with the goal to enable 3rd party applications to directly integrate with the Verify reputation platform and support other novel use-cases (e.g. loans, micropayments, etc.). This requires the development of OAuth (or equivalent standard) interfaces and easy-to-use API documentation and developer tools for 3rd party application developers.

It is impractical to estimate milestone costs for several years out; funds will be raised as part of a second potential tokensale.

MILESTONE #5: VERIFY BECOMES THE STANDARD REPUTATION INTERFACE FOR ALL DAPPS

Target de-risk date: 2021 and beyond

Aggressive targets are set to ensure that Verify becomes a crucial part of the growing cryptocurrency ecosystem powering not just applications built on the Verify protocol but as a crucial building block of all user-facing applications on the blockchain. After all, any application that relies on user-information can benefit from the growing reservoirs of data Verify has amassed at this point.

It is important to note that these stages are not mutually exclusive and that there is likely going to be overlap between these stages. The goal is to lay a strategy detailing the most pressing foreseeable challenges for Verify and how we aim to address and overcome them to create a protocol that will not only grow itself but grow the entire ecosystem with it.

Below is a more granular, tactical list of tasks that would require development effort to complete as part of Verify.

TOTAL BUDGET

We estimate the total budget required for this project based on the minimum and maximum estimates set for each individual milestone:

Milestone	Min	Max
Milestone 1 - Secure sellers	$506k	$770k
Milestone 2 - Become default crypto payment solution	$262K	$408k
Milestone 3 - Create fiat-based solution for all Internet users	$714k	$958k
Total funds required	$1.48m	$2.14m

GRANULAR TASKS

Verify Reputation Protocol

- [ ] Create smart contract to receive transactions, CRED
- [ ] Create interface to process reputation data
- [ ] Create API / OAuth interface to allow 3rd parties to develop apps on the Verify protocol for other features

Verify Payments

- [ ] Buyer Protection
  - [ ] Improved Checkout
    - [ ] Web integration w/sellers
      - [ ] API
      - [ ] Shopping carts (Shopify, Woocommerce, Magento, Bigcommerce)
    - [ ] Mobile integration with sellers
      - [ ] Android SDK
      - [ ] iOS SDK
  - [ ] Other integrations (VR, hardware, etc.)
    - [ ] API wrappers
    - [ ] Fraud detection / prevention
      - [ ] Integration with 3rd parties (SiftScience, ClearSale, etc.) for fingerprinting, fraud detection, pattern recognition
  - [ ] Dashboard for dispute resolution
    - [ ] Built-in escrow for atomic transactions
      - [ ] Integration with shipping providers
      - [ ] Integrate with exchanges to convert incoming transactions to stablecoin
      - [ ] Interface to allow buyer/sellers to input shipping information on a return/order
- [ ] Advance Payment to sellers
- [ ] Develop algorithm to calculate credit ceiling (considering mechanism design, game theory)
- [ ] Reputation
  - [ ] Develop algorithm to calculate reputation based on relevant factors (considering mechanism design, game theory)

6.2 TOKENSALE DETAILS

The tokensale and the distribution of CRED tokens is conducted by Verify Pte Ltd, a Singaporean limited liability company. Audited smart contracts deployed on the Ethereum blockchain govern the creation, processing and distribution of these tokens.

We have set a minimum tokensale raise of 1,094 ETH. If this minimum is not met, all funds received by the smart contract will be automatically refunded to the contributors through the smart contract. The soft cap is set at 3,282 ETH and once surpassed will result in the end of the sale within 96 hours. If the hard cap of 5,471 ETH is reached, the sale will halt immediately, and no further contributions will be accepted. Any tokens that are not sold will be burnt.

CREDs will be released for purchase in a single tranche at the rate of 2,033 CRED / ETH.

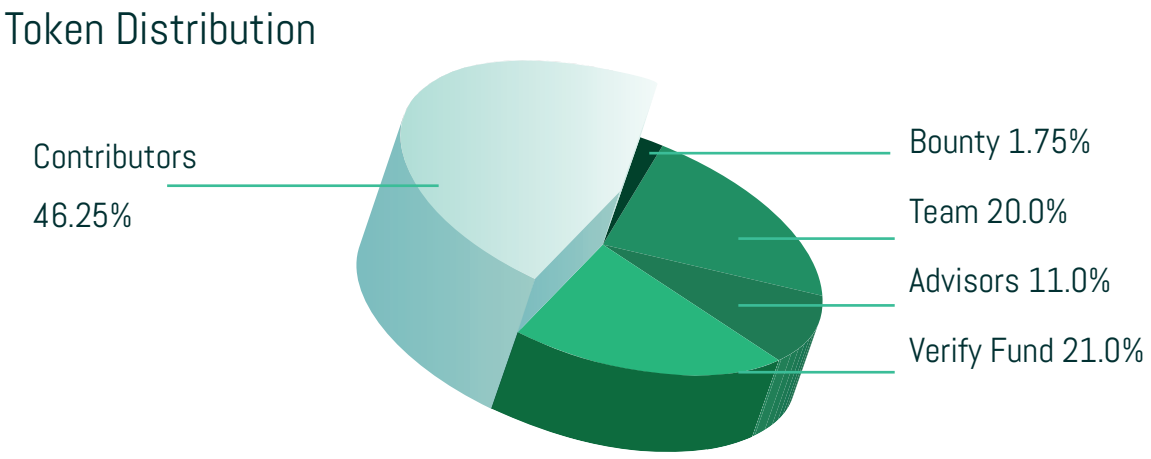
We will set limits on individual contribution amount, and that will be announced prior to the tokensale.

CURRENCY	ETH (Ether), BTC (Bitcoin)
MINIMUM	$500,000 (1,094 ETH)
SOFT CAP	$1,500,000 (3,282 ETH)
HARD CAP	$2,503,125 (5,471 ETH)
DURATION	30 days or 96 hours after soft-cap is reached
TOKENSALE STARTS	Dec 6th, 2017
TOKENSALE ENDS	Jan 8th, 2017 (or until cap is reached)
UNSOLD TOKENS	Burnt (automatically enforced by the smart contract)

6.3 TOKEN DISTRIBUTION

A total of 50,000,000 (50 million) CRED tokens will be minted at genesis, and no further CRED tokens can exist beyond this number. The majority of the tokens will be distributed during our token-sale, following the distribution described below:

TOKENS	%	ALLOCATED PURPOSE
2,000,000	4%	Early investors
11,125,000	22.25%	Participants in Tokensale v1
10,000,000	20%	Reserved for potential Tokensale v2 (locked for 12 months)
5,500,000	11%	Distributed to advisors (vests over 2 years)
10,000,000	20%	Distributed to Verify team (locked for 12 months; vests over 2 years)
10,500,000	21%	Verify Fund (closed-ended fund to incentivize platform adoption)
875,000	1.75%	Bounty
50,000,000	100%	



6.3.1 Provision for Tokensale v2

We have reserved 10,000,000 CRED tokens for a potential second tokensale. They are locked, according to the smart contract rules, for a minimum period of 12 months following the tokensale date. The second tokensale will only take place once specific business goals are met resulting in a significantly derisked business model.

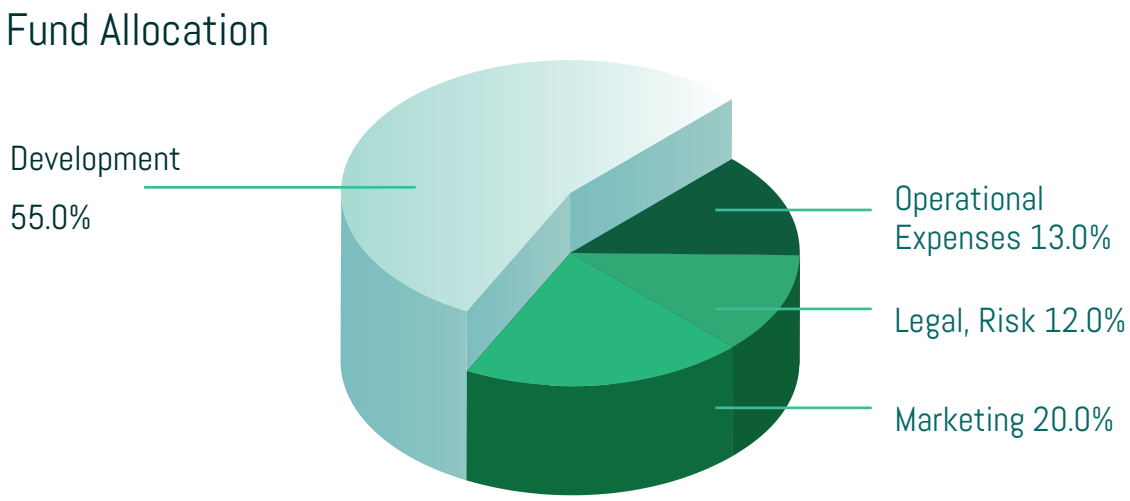
These criteria are described below:

- **A Minimum Viable Product (MVP)** of the Verify Payments platform and the Verify reputation platform is developed and deployed, allowing merchants to use the following features:
  - Complete payments using the top 3 cryptocurrencies by market capitalization (Bitcoin, Ethereum and Ripple at the time of this writing) with a plan in place to support remaining currencies based on consumer demand.
  - 100% buyer protection against all transactions made on the Verify Payments platform
  - Submit verified reviews of transactions made on the Verify protocol
  - Design, implement and deploy the algorithm that would govern how credit ceilings are allocated to sellers -- incentivizing them to use the Verify Payments platform
- **Product/market fit** is achieved, with at least 1,000 sellers on the Verify Payments platform or at least 50,000 qualified transactions conducted on the Verify reputation platform in total

Only once these criteria are met can the founding team, at their discretion, proceed to launch a second tokensale with the reserved tokens in order to fund the continued development of the Verify protocol and the Verify Payments platform. The price of the token and other tokensale parameters will be determined prior to the tokensale.

6.4 FUND ALLOCATION

In exchange for the tokens sold in the initial tokensale, we plan to use the funds raised for the following purpose:



For a detailed breakdown of what development tasks are involved, refer to Section 6.1.

6.5 BUYBACK

As detailed in Section 3.2, we have incorporated a buy-back mechanism in the core transaction processing function for the Verify reputation protocol. Every transaction processed on the network requires a corresponding insurance fee (of 1%) to be converted on the open market from the source cryptocurrency (e.g. BTC, ETH, etc.) to CRED. This balance is maintained in CRED and recognized by Verify as company revenue.

As the transaction volume on Verify increases, so too does the deflationary pressure on the CRED token resulting in higher demand for the CRED token and a corresponding rise in price. This effectively constitutes a buyback mechanism, tied to the performance of the solution.

7. Legal

GENERAL INFORMATION

The Verify token does not have the legal qualification of a security, since it does not give any rights to dividends or interests. The sale of CRED tokens is final and non-refundable. CRED tokens are not shares and do not give any right to participate to the general meeting of Verify Pte Ltd. CRED tokens cannot have a performance or a particular value outside the Verify protocol. CRED tokens shall therefore not be used or purchased for speculative or investment purposes. The purchaser of CRED tokens is aware that national securities laws, which ensure that investors are sold investments that include all the proper disclosures and are subject to regulatory scrutiny for the investors' protection, are not applicable.

Anyone purchasing CRED tokens expressly acknowledges and represents that she/he has carefully reviewed this white paper and fully understands the risks, costs and benefits associated with the purchase of Verify.

KNOWLEDGE REQUIRED

The purchaser of CRED tokens undertakes that she/he understands and has significant experience of cryptocurrencies, blockchain systems and services, and that she/he fully understands the risks associated with the tokensale as well as the mechanism related to the use of cryptocurrencies (incl. storage).

Verify shall not be responsible for any loss of CRED tokens or situations making it impossible to access CRED tokens, which may result from any actions or omissions of the user or any person undertaking to acquire CRED tokens, as well as in case of hacker attacks.

RISKS

Acquiring CRED tokens and storing them involves various risks, in particular, the risk that Verify Pte Ltd may not be able to launch its operations and develop its blockchain and provide the services promised. Therefore, and prior to acquiring CRED tokens, any user should carefully consider the risks, costs and benefits of acquiring CRED tokens in the context of the tokensale and, if necessary, obtain any independent advice in this regard. Any interested person who is not in the position to accept or to understand the risks associated with the activity (including the risks related to the non-development of the Verify protocol) or any other risks as indicated in the Terms & Conditions of the tokensale should not acquire CRED tokens.

IMPORTANT DISCLAIMER

This white paper shall not and cannot be considered as an invitation to enter into an investment. It does not constitute or relate in any way nor should it be considered as an offering of securities in any jurisdiction. This white paper does not include or contain any information or indication that might be considered as a recommendation or that might be used as a basis for any investment decision. CRED tokens are just utility tokens which can be used only on the Verify protocol and are not intended to be used as an investment.

The offering of CRED tokens on a trading platform is done in order to allow the use of the Verify protocol and not for speculative purposes. The offering of CRED tokens on a trading platform does not change the legal qualification of the tokens, which remain a simple means for the use of the Verify protocol and are not a security.

Verify Pte Ltd is not to be considered as an advisor in any legal, tax or financial matters. Any information in the white paper is provided for general information purposes only and Verify Pte Ltd does not provide any warranty as to the accuracy and completeness of this information.

Verify Pte Ltd is not a financial intermediary according to Singaporean law and is not required to obtain any authorization for Anti Money Laundering purposes.

Acquiring CRED tokens shall not grant any right or influence over Verify Pte Ltd's organization and governance to the Purchasers.

Regulatory authorities are carefully scrutinizing businesses and operations associated to cryptocurrencies in the world. In that respect, regulatory measures, investigations or actions may impact Verify Pte Ltd's business and even limit or prevent it from developing its operations in the future. Any person undertaking to acquire CRED tokens must be aware of the Verify Pte Ltd business model, the white paper or terms and conditions may change or need to be modified because of new regulatory and compliance requirements from any applicable laws in any jurisdictions. In such a case, purchasers and anyone undertaking to acquire CRED tokens acknowledge and understand that neither Verify Pte Ltd nor any of its affiliates shall be held liable for any direct or indirect loss or damage caused by such changes.

Verify Pte Ltd will do its utmost to launch its operations and develop the Verify protocol. Anyone undertaking to acquire CRED tokens acknowledges and understands that Verify Pte Ltd does not provide any guarantee that it will manage to achieve it. They acknowledge and understand therefore that Verify Pte Ltd (incl. its bodies and employees) assumes no liability or responsibility for any loss or damage that would result from or relate to the incapacity to use CRED tokens, except in case of intentional misconduct or gross negligence.

REPRESENTATION AND WARRANTIES

By participating in the tokensale, the purchaser agrees to the above, and in particular, they represent and warrant that they:

- have read carefully the terms and conditions attached to the white paper; agree to their full contents and accept to be legally bound by them;
- are authorized and have full power to purchase CRED tokens according to the laws that apply in their jurisdiction of domicile;
- are neither a US citizen or resident;
- live in a jurisdiction which allows Verify Pte Ltd to sell CRED tokens through a tokensale without requiring any local authorization;
- are familiar with all related regulations in the specific jurisdiction in which they are based and that purchasing cryptographic tokens in that jurisdiction is not prohibited, restricted or subject to additional conditions of any kind;
- will not use the tokensale for any illegal activity, including but not limited to money laundering and the financing of terrorism;
- have sufficient knowledge about the nature of the cryptographic tokens and have significant experience with, and functional understanding of, the usage and intricacies of dealing with cryptographic tokens and currencies and blockchain-based systems and services;
- purchase CRED tokens because they wish to have access to the Verify protocol;
- are not purchasing CRED tokens for the purpose of speculative investment or usage.

GOVERNING LAW AND ARBITRATION

Any dispute or controversy arising from or under the tokensale shall be resolved by arbitration in accordance with the Singaporean Rules of International Arbitration of the Singaporean Chamber of Commerce in force on the date when the Notice of Arbitration is submitted in accordance with these Rules. The arbitration panel shall consist of one arbitrator only. The seat of the arbitration shall be Singapore. The arbitral proceedings shall be conducted in English.

Appendix A: Long-term Vision

Most people are used to the buyer/seller paradigm and can understand the dynamics of this relationship and how a payments solution might help. However, the core Verify protocol exists a layer below this; it is the layer that enables applications like Verify Payments to exist, and this can be challenging to visualize.

To understand the real impact of a reputation protocol, consider a buyer and a seller in two different locations: let's say a buyer from Russia and a seller from Argentina. Having a reputation protocol would allow these two parties to transact, whereas previously it would've been too risky to do. Think about the global trade market today, and *how much larger it could become* if a reliable reputation protocol existed that would allow any two people or entities to transact, using freely accessible cryptocurrencies. Cryptocurrencies do not have the same barriers to entry that traditional financial instruments do; buyers do not need a credit card to pay for goods, and sellers do not require a merchant account to receive payments. This is the ultimate vision behind the reputation protocol: to become the fundamental layer upon which financial applications are built. Applications that extend credit to individuals that have nothing more than their reputation to go by. And really, what could possibly be a better predictor for future trustworthiness than past trustworthiness?

As for Verify Payments, the focus would be on promoting the use of cryptocurrencies for commercial purposes. This would initially start with eCommerce sellers but eventually, extend into all areas of commerce -- including physical retail. The difficulty is in setting up the initial infrastructure that would support the most complex use-case: eCommerce (which involves higher risk due to longer delivery times). Expanding to include other use-cases like digital retail and physical retail (where delivery is often instant) would be less challenging from a design perspective.

Appendix B: Token Economic Model

SETUP

Consider a simple model with 3 periods, t = 0, t = 1, and t = 2. There is 1 buyer and 1 seller. At t = 0 buyer wants to spend $\$x_0$[1] for a good from the seller. The transaction is taxed at a flat rate , and the seller will eventually receive $\$(1 - \alpha)x_0$ for the good.The seller has a credit cap $0 \leq c_0 < (1 - \alpha)x_0$ which he receives at the moment of purchase t = 0, while the rest $(1 - a)x - c$ is held in escrow[2] and will be released to him at t = 1[3] At t = 1 the transaction is completed. Also, at t = 1 buyer wants to make another purchase for the amount of $\$x_1$ ($x_1 > x_0$ would correspond to the growing Verify market, while $x_1 < x_0$ would correspond to the shrinking market). At t = 1, the seller has a new cap c_1 which may be more (if the first transaction was successful) or less (if the first transaction failed) than c_0. The second transaction will be completed at period t = 2, when no more transactions occur and the game ends.

When the buyer makes a purchase, the amount of tax xis entirely used to purchase tokens on the open exchange. These tokens are then taken by Verify and disappear from the market. At t = 0, the seller is allowed to purchase more tokens than needed to accept the first transaction and then use them for the second transaction at t = 1. There are also "traders" on the market. A trader is anyone who holds, sells and/or buys tokens onthe open exchange. A "trader"could be a third person, buyer, seller or even Verify themselves. All traders behave competitively on the token market, care about maximizing their profits in dollars only and initially, at t = 0 together hold T_0 tokens.

The question is: what will be the equilibrium price of tokens and how many of them will be sold in each period?

ANALYSIS

In each period, the price and quantity of tokens' sold is determined by supply and demand. Firstnote that since there are no transactions at t = 2 as this is the end of the game, there will be no market at t = 2 since nobody will need tokens. Therefore, all the

1 For simplicity, we will call "dollar" any fiat or stablecoin whose price is not affected by processes on the Verify platform. This can be actual dollars, any other exchangeable currency or cryptocurrency.

2 We plan to use the Verify Fund to finance c for the advance payment to the seller. However, we will see later

3 We assume no time discounting. That is, every agent values 1 dollar today the same as 1 dollar tomorrow. Typically, that is not the case: 1 dollar today is worth more than 1 dollar tomorrow. The model can be easily adjusted for this, but this won't substantially aect any important result.

tokens that are on handsat $t = 1$ have to be-sold at $t = 1$. We denote the token price as p_0 and p_1 at $t = 0$ and $t = 1$ respectively, and denote T_s as the number of tokens all the token holders are ready to sell at $t = 0$ (Thus, they will have $T_0 - T_s$ at $t = 1$, and all these tokens will be sold at $t = 1$).

Consider the demand for tokens at $t = 0$ and denote $E(p_1)$ as the expectation of p_1 at t_0 (what agents think at t_0 about price of tokens at t_1). Total demand consists of three distinct components. First, there is demand generated by Verify's need to exchange tax money αx for tokens:

$$D_v(p_0) = \alpha \frac{x_0}{p_0}.$$

Second, there is a demand from the seller, who may want to buy tokens at $t = 0$ to use for the transaction at $t = 1$. However, he will do so only if he believes that at $t = 1$ tokens will be more expensive than now at $t = 0$. i.e., this demand DB (p_0) is 0 if $p_0 \geq E(p_1)$ and it is $\frac{\alpha x_1}{E(p_0)}$ if $p_0 < E(p_1)$

Third, there is demand from traders. At $t = 0$ traders would like to buy tokens only if they think that at $t = 1$ these tokens will be more expensive, and they will indeed be willing to buy as many tokens as possible in this case, since every token is a positive profit. So if $p_0 < E(p_1)$ the traders' demand DT (p_0) is infinite, while if $p_0 \geq E(p_1)$ it is 0.[4]

Now supply side. Since only traders have tokens (T_0 of them), they want to sell anythingat $t = 0$ if and only if they expect that the price will fall in the next period, and they want tosell everything they have in this case. That is supply, $S(p_0)$, at $t = 0$ is 0 if $p_0 < E(p_1)$, T_0 if $p_0 > E(p_1)$ and could be anywhere between 0 and T_0 if $p_0 = E(p_1)$.

EQUILIBRIUM

Now note that the only possible equilibriumis when $p^*_0 = p^*_1$.Think what happens if this is not the case. First, in equilibrium agents should correctly anticipate future price, i.e. $E(p^*_1) = p^*_1$.[5] Second, suppose that $p_0 < p_1$. Since nobody wants to sell tokens at $t = 0$, preferring to wait until $t = 1$, while there is still positive demand, p_0 will eventually increase to the level of p_1.

Alternatively, suppose that $p_0 > p_1$. Then all the token holders wants to sell their tokens which does not mean they necessarily will be able to. They will start selling tokens, p_0 will start to increase till either 1) all tokens are sold and p_0 is still below p_1 (In this case, there will be no market at $t = 1$) or 2) p_0 equals p_1 and there is no incentive to sell tokens further.

So, at equilibrium it must be the case that $p_0 = p_1$. Let Ts be the number of tokens sold at $t = 0$ given these prices. Hence, equilibrium is defined by three equations:

4 We assume that if traders are indiferent between buying and not buying, i.e. when $p_0 = E(p_1)$, they don't buy

5 We may later consider alternative situations, where agents are not fully rational and systematically incorrectly assess future price (overestimate or underestimate). However, there must be very strong justification for such irrationality.

$$\frac{\Delta x_0}{p_0} = T_s;$$

$$\frac{\Delta x_1}{p_1} = T_0 - T_s;$$

$$p_0 = p_1.$$

$$p^*_0 = p^*_1 = \frac{\Delta(x_0 + x_1)}{T_0}.$$

CONCLUSION

What you can see from this simple model is

1. Token price will stabilize overtime, irrespective of where Verify market grows or shrinks. This is because traders will always exploit any potential price difference till it disappears. Indeed, if you allow for time discounting, p_1 will be higher than p_0, but this will be a fixed difference which will not depend on any other modelparameter.

   However, this does not mean that the price will not fluctuate over time at all. There are many scenarios that may cause the price to change in any direction. For example, there could be unexpected things that would affect an agent's expectations (e.g., the future size of the Verify market), or there could be information asymmetry (some agents will know more about the market than others), or some agents may be not fully rational in their decisions, etc. So, in fact, the token market is essentially just like any other asset market.

   I assume that x_1 is known to the buyer and everyone else on the market with certainty. It would be more realistic to assume that $x1$ is subject to some uncertainty. In this case what would matter is current actual volume and expectations of future volumes. After every period, these expectations will adjust incorporating all new information available to agents, and this will cause price fluctuations. For example, if Verify grows faster than it was initially expected, token price will rise over time, but if it will grow slower than expected, price will decrease over time.

2. If the role of the Verify Fund is strictly to extend credit to sellers, then you don't actually need Verify Fund. Given that token price is the same over time, it does not matter whether you first take tokens out of the Verify Fund to fund advanced payment and then

re-buy tokens for the money you are left with after the release of the escrow holding, or you directly take c out of $(1 - a)x$ and put the rest to escrow. However, since there's a risk component consideration as well (that Verify may or may not be able to recoup funds extended as credit to sellers), itdoes ultimately make sense to separate the two resulting in separation of concerns. This also allows Verify to introduce a slight fee on the credit extended to adjust for the risk of non-repayment by a small portion of sellers.

3. It does not matter whether transactions in Verify are successful or not. Their successor failure does not directly affect token prices. Indeed, if we assume that successful transactions will attract more agents to Verify and thus increase future volumes, success will matter. But this will be an indirect effect via volumes.

4. It does not matter what are seller's ceilings (caps) and how they change overtime.

5. It does not matter what is the initial distribution of tokens (as long as the number of tokens in one pair of hands is small relative to the total number of tokens, so that no single party is able to substantially influence prices). Only their total amount matters.

In conclusion, the token model as demonstrated tends towards stability, with the token price largely dependent on the performance of the Verify platform over time.

Appendix C: Team

Our team is primarily comprised of ex-Amazon leaders and engineers that worked directly on payment solutions within the company.

Yazin Alirhayim, CEO

Yazin was most recently VP at Amazon's "Payfort Start" division. He previously founded White Payments, a "Stripe for the Middle East". White was acquired by Payfort (and later by Amazon) just 12 months after it launched. Before White, he founded several startups and prior to that was Global Finance Leader at General Electric. Yazin is an experienced Finance executive, and a certified Lean Six Sigma Black Belt and instructor.

Ibrahim Mokdad, Head of Business Development

Ibrahim most recently lead R&D at Exa.io, a supercomputing platform for 3D graphics rendering. At Exa, he orchestrated commercial deals with enterprise and government clients. He has a strong technical background, having completed his Master's research in Machine Learning. He maintains a popular channel on Youtube on Python and Computer Vision using OpenCV.

Appendix D: Advisors

REPUTATION & TRUST

TBA

PAYMENTS

Omar Kassim

Omar Kassim previously founded, grew and exited JadoPado, one of the Middle East's pioneering eCommerce marketplaces. JadoPado was acquired by noon, a billion dollar company founded by real-estate mogul and billionaire Mohammed Alabbar. Omar is currently the CEO and Founder of Esanjo, a business that creates, builds and invests in beautiful technology businesses.

Moussa Beidas

CEO and co-founder of Bridg one of the Middle East's first Fintech startups and a regional thought leader in the space. A digital creative strategist who built customer experiences for Google Fibre, Microsoft, Skype, Emirates NBD, DeNA (Tokyo), Tata DOCOMO (India). His work in digital user experience has impacted over 300 million customers across the globe.

ECONOMICS

TBA

BLOCKCHAIN

TBA

References

[1] eMarketer. (2016, August 22). Worldwide Retail Ecommerce Sales Will Reach $1.915 Trillion This Year. Retrieved from https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-Trillion-This-Year/1014369

[2] ESTICAST Research (2017, October 21) Blockchain Market By type, By provider, By organization size, By End User, Industry Trends, Estimation & Forecast. Retrieved from: https://www.esticast-research.com/market-reports/blockchain-market

[3] Vuitton, E. (2017, March 21) Ecommerce Payment Fraud Outlook 2017-2020. Retrieved from: https://chargeback.com/ecommerce-payment-fraud-outlook-2020/

[4] Wood, L. (2016, September 14) Fraud Detection and Prevention Market Worth $33.19 Billion by 2021 - Rise in Online Businesses, Transactions & Mobile Banking - Research and Markets. Retrieved from: http://www.businesswire.com/news/home/20160914005789/en/Fraud-Detection-Prevention-Market-Worth-33.19-Billion

[5] Payfort (2017, March 28). PayFort Joining the Amazon family. Retrieved from https://www.payfort.com/payfort-joining-the-amazon-family/

[6] Nakamoto, S., Bitcoin: A Peer-to-Peer Electronic Cash System, Retrieved from https://bitcoin.org/bitcoin.pdf

[7] Bluterin, V. (2017, October 13). ETHwaterloo Keynote Speech [Video file]. Retrieved from https://www.youtube.com/watch?v=pcWEdyBBGrk

[8] A. Jøsang, R. Ismail, C. Boyd, (2007) A survey of trust and reputation systems for online service provision, *Decision Support Systems* 43. pp. 618–644.

[9] Vavilis S, Petkovic M, Zannone N. (2014). A reference model for reputation systems. *Decision Support Systems* 61: pp. 147–154.

[10] Audun Jøsang. (2016) "*S*ubjective Logic: A Formalism for Reasoning Under Uncertainty", ISBN 978-3-319-42337-1, Springer Verlag.

[11] Irissappane A., A. and Zhang, J. (2015) A Case-Based Reasoning Framework to Choose Trust Models for Different E-Marketplace Environments, Journal of Artificial Intelligence Research, 52, pp. 477-505.

[12] Y. Ruan, A. Durresi, (2016) A survey of trust management systems for online social communities–Trust modeling, trust inference and attacks. *Knowledge-Based Syst* 106 , pp. 150-163.

[13] Ahn , H.,J., (2008) A new similarity measure for collaborative filtering to alleviate the new user cold-starting problem. *Information Sciences* 178, pp 37-51.

[14] Hariharan, A. (2016) All about Network Effects, Retrieved from https://a16z.com/2016/03/07/all-about-network-effects/

[15] CFPB (2017, October 17) Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation, Retrieved from http://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf

[16] Rietjens ,B. (2007) Trust and reputation on eBay: Towards a legal framework for feedback intermediaries, *Information & Communications Technology Law* 15.

[17] Spitz, S. and Tuchelmann, Y. (2011) A Survey of Security Issues in Trust and

Reputation Systems for E-Commerce. Autonomic and Trusted Computing, 8th International Conference, pp. 203–214.

[18] "CFPB Outlines Principles For Consumer-Authorized Financial Data ...." 18 Oct. 2017, https://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-principles-consumer-authorized-financial-data-sharing-and-aggregation/. Accessed 22 Oct. 2017.

[19] Marti, S. and Garcia-Molina, H. (2006) Taxonomy of trust: Categorizing p2p reputation systems. *In Management in Peer-to-Peer Systems* 50, pp 472–484.

[20] Abbas S., Merabti M., Llewellyn-Jones D., (2010) Deterring whitewashing attacks in reputation based schemes for mobile ad hoc networks, *Proc. of IFIP Wireless Days Conf*, IEEE, pp. 1–6

[21] V. Agate, et al., (2016). A framework for parallel assessment of reputation management systems. In Proceedings of the International Conference on Computer Systems and Technologies (CompSysTech).

[22] Douceur J.R, (2002) The Sybil Attack, *Proceedings of the International Workshop on Peer-to-Peer Systems*.

[23] Hoffman K., David Z. and Nita-Rotaru C. (2009) A Survey of Attack and Defense Techniques for Reputation Systems, *ACM Computing Surverys* 42.

[24] Theleanstartup, The lean startup methodology. Retrieved from: http://theleanstartup.com/principles References

Change Log

19 Nov, 2017: Updated the bounty allocation in proportion to the reduction of the hard-cap

20 Nov, 2017: Updated bounty allocation to reflect new bounty structure.


verify