# BLINDTALK
# A Crypto-Messaging Platform

http://blindtalk.net

By Abdullah Daud, chelahmy@gmail.com

6th November 2017

## Abstracts

An unknown party of two makes eavesdropping difficult. Blindtalk is a crypto-messaging platform where the receivers are unknown and the senders anonymous. The receivers will regularly visit the platform looking for messages. The visitors are crypto-savvy and will attract like-minded advertisers such as those who want to promote their own initial coin offerings (ICOs). The platform limits the premium spaces for advertisers so that to entice bidding for placements. The bids are paid using Blindtalk cryptotokens. The fluctuation of the biddings will positively influence the price of Blindtalk cryptotokens. As a crypto-based platform more business opportunities will emerge especially those that involve minute charges which cryptotokens are best at handling.

## Introduction

An unknown party of two makes eavesdropping difficult. It's like listening to someone talking over the phone. One party is loud and clear. The other is silent.

Blindtalk is a crypto-messaging platform where senders just leave signed messages and expect the receivers to collect them. The senders are anonymous and the receivers are unknown to the platform. Blindtalk has no proof that the receivers had received the messages.

The receivers must search Blindtalk for messages intended for them.

Blindtalk keeps all messages in its database for a limited period of time. Anyone may search the entire database. Thus, the contents of the messages are open to the public. It is up to the senders to encrypt the messages. However, an encrypted message is a clear indication that the message has an intended receiver.

## How Does Crypto-Messaging in Blindtalk Work?

Alice and Bob had initially agreed to communicate secretly using Blindtalk. The agreement took place somewhere else. They share their anonymous cryptocurrency addresses. Alice signs a message using her address and post it into Blindtalk. Bob searches Blindtalk for messages signed by Alice's address. Bob may reply to Alice by signing a reply message using his address and post it into Blindtalk. And Alice will search Blindtalk for reply messages signed by Bob's address. The communication may go on and on.

Once Bob or Alice receives a message he or she may verify it to ensure that the message was indeed signed by the sender.

## Message Signing

Blindtalk does not implement any cryptography. The messages are expected to be signed using cryptocurrency wallets. The addresses used for message signing are cryptocurrency addresses. Verifications of the signed messages by receivers will also be done using cryptocurrency wallets.

Cryptocurrency message signing is decentralized. Thus, the signed messages are anonymous.

## Premium Messaging Spaces

The Blindtalk's front page is meant to show only the search bar like Google's.

However, people may want to use Blindtalk to advertise since the platform attracted many visitors, especially visitors who most probably have stakes in cryptocurrencies. Thus, the area below the search bar is designed to show a limited set of blocks of messages intended for the public. The messages will be sorted by bid amounts. The message from the highest bidder will float to the top. The amount of the bids will be deducted hourly so that the messages will slowly sink to the bottom and eventually exit the list. Those who want their messages to keep on floating will have to add up to the bids.

If Alice and Bob decide to bid then their messages may appear in the front page of Blindtalk.

## Development

Most Blindtalk's features have been specified in this paper. The designing works of Blindtalk had already started many months earlier since the rapid rise of cryptocurrencies in 2017. The message signing capability of cryptocurrencies had triggered the designing of Blindtalk. While most people are busy talking about blockchains, Blindtalk is focusing on cryptocurrency message signing. The development of Blindtalk application is expected to be straightforward due to its simple features.

Blindtalk is going to be a simple message posting, searching and listing mobile-friendly web application. The front page is exhibiting premium messaging spaces which are priced and sorted according to the highest bidders. The premium messages will be gradually removed from the spaces to make ways for new messages. The speed of message removal will also depend on biddings.

The message signing is not part of Blindtalk. There is no user profile. And there is no membership sign-up and subscription. However, postings may involves payments in Blindtalk cryptotokens.

The Blindtalk web application should not take more than six months to develop. The following is the Blindtalk development road map:

Milestone 1 – Message posting, searching and listing capabilities.
Milestone 2 – Front page premium messaging spaces with gradual message removal.
Milestone 3 – Documentations, guides, FAQ and news.
Milestone 4 – Payment gateway.
Milestone 5 – Promotions, publicity and user acquisitions.

Blindtalk may evolve into a feature-rich application in the future that utilizes its cryptotokens ever more. One example is paid comment where the public will have to pay to make comments on messages. Another example is paid image display where the sender will have to pay to make an image to show up in her message. In a cryptocurrency world some tiny payments will not deter users away. Software is dynamic. Hence, the potential financial opportunity with Blindtalk cryptotokens is open-ended.

## Blindtalk Cryptotokens

Blindtalk cryptotokens will be based on Waves (https://wavesplatform.com). There

will be a fixed amount of 100 million Blindtalk cryptotokens. All of them will be offered in an initial coin offering (ICO). They can be purchased and traded in the Waves decentralized exchange.

Initially, the Blindtalk cryptotokens will be used as bidding payments for the limited premium messaging spaces located at the Blindtalk's front page. Other usage will be introduced as Blindtalk evolves.

Blindtalk will only accept payments in Blindtalk cryptotokens. This will create demands for the cryptotokens. The demands will be exhibited in the biddings of the premium messaging spaces.

All cryptotokens received by Blindtalk will be sold back through the exchange. Since Blindtalk initially will be a major receiver of the cryptotokens so it will exercise its best effort to keep the cryptotokens in a healthy state which will benefit the investors.

## Publicity

Blindtalk is a messaging platform. Publicity and promotions are required for initial user acquisitions. These early users will invite their friends and acquaintances into the platform because messaging involves at least two parties. The word of mouth will ever expand the platform into more users.

Publicity and promotions will be continuously run in social media and on-line advertisements. Crypto-savvy writers will be employed to continuously write about Blindtalk. And the writings will be posted into prominent blogs.

The success of Blindtalk depends on mass user acceptance. Thus, Blindtalk has to continuously communicate with the public.

## Conclusion

The influx of ordinary people into cryptocurrency in 2017 is the sign of public acceptance on the decentralized digital monetary system. Cryptocurrency denotes another paradigm shift since the introduction of the Internet. The world is entering a new era.

Cryptotokens enable startups to source for initial and ongoing crowd-fundings. Hence, all new businesses should opt for cryptotokens as sources for running

capitals. In fact, the acceptance of the businesses cryptotokens by the public shows the credibility of the businesses themselves.

Blindtalk should have its own cryptotokens.

Blindtalk's business is on the Internet. Since it is making use of cryptocurrency-message-signing capability so enabling its own cryptotokens goes without saying. It will be awkward if Blindtalk does not have one.

Crypto-messaging is another extension to the anonymous and no-knowledge properties of cryptocurrency. The sender is anonymous behind the cryptic address. If the sender send a message to a receiver's address then the sender's address is already associated with the receiver's address. Hence, the two addresses are known to have been messaging each other. Eavesdropping may take place. Blindtalk breaks that association by making the receiver unknown.

A platform will always bring people together. Hence, business opportunities such as advertisements will emerge. In fact, people are willing to pay for anything as long as the price is right. A small price is almost always right. And cryptocurrencies can handle small prices pretty well.

Blindtalk has a solid business use case.