Bancor Protocol

Continuous Liquidity and Asynchronous Price Discovery for Tokens through their Smart Contracts; aka “Smart Tokens”

Eyal Hertzog, Guy Benartzi & Galia Benartzi

May 30, 2017

Draft Version 0.99

The phrase "double coincidence of wants" was coined by Jevons (1875). "The first difficulty in barter is to find two persons whose disposable possessions mutually suit each other's wants. There may be many people wanting, and many possessing those things wanted; but to allow of an actual act of barter there must be a double coincidence, which will rarely happen."

Table of Contents

The Bancor Protocol

Abstract: The Bancor protocol enables built-in price discovery[1] and a liquidity mechanism for tokens on smart contract blockchains. These "smart tokens" hold one or more other tokens in reserve, and enable any party to instantly purchase or liquidate the smart token in exchange for one of its reserve tokens, directly through the smart token's contract, at a continuously calculated price, according to a formula which balances buy and sell volumes.

The Bancor protocol is named in honor of the Keynesian proposal[2] to introduce a supranational reserve currency called Bancor to systematize international currency conversion after WWII.

Background

We live in a world where anyone can publish an article, song or video, create a discussion group and even run an online marketplace. We are now beginning to witness the emergence of user-generated currencies. Different types of stored-value ("currencies" hereafter) have been issued and circulated for centuries in the form of bank notes, bonds, equity, gift cards, loyalty points, community currencies[3] and others. Bitcoin was the first ***decentralized*** digital currency, followed by a wave of new cryptocurrencies that have been issued since, and recently we've seen the rise of a new asset class of "tokens" that are typically issued in crowdsales ("ICOs") through smart contracts.

However, currencies, which are essentially networks of value, do not connect to each other in the same way that information networks do. While the switches on Internet exchange points (IXs) interlink information networks, active traders on ***exchanges*** are effectively interlinking currencies.

The current exchange model for currencies/assets has a critical barrier, requiring a certain volume of trading activity to achieve market-liquidity. This inherent barrier makes it nearly impossible for small-scale currencies (such as community currencies, loyalty points or other custom tokens) to be linked (exchangeable) to other popular currencies using a market-determined exchange rate.

In the age of smart contract blockchains, tokens can be automatically managed by immutable code which controls their issuance and behavior. We realized this could mean allowing tokens to hold balances of other tokens (i.e. "reserves"), directly through their smart contracts, that could be designed by their creators and managed programmatically. These new technological capabilities warrant rethinking of the possible solutions for converting one currency to another and determining market prices.

Introducing Smart Tokens: A Solution to the Liquidity Problem

Smart tokens are standard ERC20 tokens which implement the Bancor protocol, providing continuous liquidity while automatically facilitating price-discovery. The smart token's contract

[1] https://en.wikipedia.org/wiki/Price_discovery
[2] https://en.wikipedia.org/wiki/Bancor
[3] https://en.wikipedia.org/wiki/Community_currency

instantly processes ***buy*** and ***sell*** orders, which drive the price-discovery process. Due to this capability, smart tokens do not need to be traded in an exchange in order to become liquid.

A smart token holds a balance of least one other ***reserve token***, which (currently) can be a different smart token, any ERC20 standard token or Ether. Smart tokens are issued when purchased and destroyed when liquidated, therefore it is always possible to purchase a smart token with its reserve token, as well as to liquidate a smart token to its reserve token, at the current price.

A New Method for Price Discovery

A smart token utilizes a novel method for price-discovery which is based on a “Constant Reserve Ratio” (CRR). The CRR is set by the smart token creator, for each reserve token, and used in price calculation, along with the smart token’s current supply and reserve balance, in the following way:

$$Price = \frac{Balance}{Supply \times CRR}$$

This calculation ensures that a constant ratio is kept between the reserve token balance and the smart token’s market cap, which is its supply times its price. Dividing the market cap by the supply produces the price according to which the smart token can be purchased and liquidated through the smart contract. The smart token’s price is denominated in the reserve token and readjusted by the smart contract per each purchase or liquidation, which increases or decreases the reserve balance and the smart token supply (and thus the price) as detailed below.

When smart tokens are purchased (in any of their reserve currencies) the payment for the purchase is added to the reserve balance, and based on the calculated price, ***new smart tokens are issued*** to the buyer. Due to the calculation above, a purchase of a smart token with a less than 100% CRR will cause its price to increase, since both the reserve balance and the supply are increasing, while the latter is multiplied by a fraction.

Similarly, when smart tokens are liquidated, they are ***removed from the supply*** (destroyed), and based on the current price, reserve tokens are transferred to the liquidator. In this case, for a smart token with a CRR less than 100%, any liquidation will trigger a price decrease.

This asynchronous price-discovery model works by constantly readjusting the current price toward an equilibrium between the purchase and liquidation volumes. While in the classic exchange model price is determined by two matched orders in ***real-time***, smart token prices are calculated ***over-time***, following every order.

The above formula calculates the current price, however, when a purchase or liquidation is executed, the effective price is calculated as a function of the transaction size. The calculation can be described as if every transaction is broken up into infinitely small increments, where each increment is changing the smart token’s supply, reserve balance, and thus its price. This ensures that purchasing the same amount of smart tokens in a single or multiple transactions would yield the same total price. Additionally, this method ensures that the CRR will be kept constant and the reserve can never be drained. Essentially, the effect of the transaction size on the price (due to its

changing the smart token's supply and reserve balance) is incorporated into the effective price for any transaction. The mathematical functions for calculating price per transaction size are presented further in this document.

Using this method, the Bancor protocol can enable liquidity and asynchronous price discovery for ***existing standard tokens*** -- through smart tokens holding them in reserve, enabling backward compatibility. This use-case and others are described in detail below.

Use-Cases for Smart Tokens

The Long Tail[4] of User-Generated Currencies

The long tail phenomena can be observed in many different online ecosystems such as publishing (blogs), videos (YouTube), discussion forums (Reddit, Facebook Groups) and more. In each of these examples, the long tail has become significantly larger in scale than everything that preceded it. The forming of a long tail begins as soon as the barriers to its existence are removed (e.g. YouTube making it simple for anyone to upload and share user-generated videos).

There are many examples of user-generated currencies, such as group currencies (community oriented currencies), loyalty points (business oriented currencies), and the most recent being hundreds of cryptocurrencies (protocol oriented currencies). However, the need to achieve and maintain liquidity for these small or new currencies remains a significant barrier for their viability.

Smart tokens are unique in that they can be purchased or liquidated by a single party, using the calculated price, ***removing the need for two opposite wants to be simultaneously matched***. This effectively means that by using the Bancor protocol, small-scale currencies with a low expected trade volume can offer continuous liquidity, thus, removing the barrier for them to be linked to the global economy.

Enabling the long tail of currencies is likely to bring about a new generation of creative use-cases. Though it's improbable to predict all of them, some of the more likely use-cases are listed below.

Crowdfunding a Project

The crowdfunding space has been growing rapidly. Smart tokens can be used for crypto crowdfunding initiatives, where the participants receive tokens which are liquid and market-priced. For example, a musician may collect funds to record an album, which would be sold online exclusively in exchange for the issued tokens. A successful album would generate high demand for the tokens, driving up their price and rewarding those holding them. Many other examples exist such as crowdfunding a venture capital fund or raising initial capital for a credit-creating neighborhood currency.

[4] https://en.wikipedia.org/wiki/Long_tail

Token Changers

Token changers are smart tokens that hold multiple reserve tokens, with a total CRR of 100% and can be used to exchange between any standard ERC20 tokens they hold in reserve. A token changer is designed to provide an exchange service between its reserve tokens through a two-step process of purchasing the smart token with one reserve token, and immediately liquidating it for another.

Due to the price calculation formula, each time reserve token X is converted to reserve token Y -- the price of X decreases, while the price of Y increases. Larger transactions will move the price more sharply, however, a higher reserve balance would reduce price volatility.

As noted, any standard ERC20 token can be used as a reserve-token even if it is already traded in other exchanges. In such a scenario, a gap may open between the calculated price of a reserve token and its price in an outside exchange. This situation creates an arbitrage opportunity which ***incentivizes arbitrageurs to restore economic equilibrium***, thus keeping the token changer prices in sync with the prices at which their reserve tokens are traded in other exchanges.

A token changer's creator may set a conversion fee that would apply on each purchase/liquidation. Fees can be accumulated in the reserves and thus increase the smart token's price with every token conversion taking place, increasing the smart token's value. This increase will benefit the holders of the smart token, who may have deposited the original reserves when the smart token was created, or purchased it with any of its reserve token's at any time after that.

Popular exchanges such as MtGox and Bitfinex have been hacked with hundreds of millions of dollars worth of assets stolen from their accounts. Converting one token to another using a token changer does not require depositing funds in an exchange and thus removes the counterparty risk from the process. Another important benefit is that no transaction limits need to be applied, as is the case with other instant trading solutions, due to the decentralized nature of the token changer. While decentralized exchanges offer this benefit as well, smart tokens do not rely on trade volume to provide liquidity.

Decentralized Token Baskets

Smart tokens can be used as decentralized token baskets, which function similarly to ETFs or index funds, simply by holding a portfolio of reserve tokens with a total CRR of 100%. As prices of any of the reserve tokens rise or fall, so does the value of the smart token. Similar to token changers, here as well arbitrageurs are incentivized to realign the conversion rates with market prices which ensures the proper ratios are kept between the reserves according to their real-time market value. These smart tokens enable users to directly hold asset baskets, without a financial services provider as an intermediary.

Network Tokens

A collection of smart tokens that use the same reserve token form a ***network of tokens***. The common reserve token can be described as a ***network token*** which captures the combined value of the network of tokens which hold it in reserve. Increased demand for any of the smart tokens in the network would increase demand for the network token, since it is required for purchasing these tokens, and then held in their reserves. Increased demand drives up the price of the network token, which ***benefits the entire network*** since the value of the tokens' reserves increases, thus to maintain the CRR, the value of the smart tokens also increases. The network token also functions as a "token for tokens", rendering all the smart tokens in the network inter-changeable.

Network tokens can be useful for those who wish to create multiple and related smart tokens for different purposes (e.g. regional network of community currencies, a video game studio with multiple game credits, a group of independant businesses issuing a joint loyalty program). The network token model creates synergetic relationships between the member smart tokens, comparable to the way any single successful Ethereum service can drive up the value of Ether, benefiting ***all of its holders***.

An additional network token use-case is to interlink a set of token changers, each holding a reserve in the network token and a second reserve in another, standard token. This structure would enable exchanging any token in the network to another, while increasing the demand for the network token whenever a new token changer is created or appreciates.

Advantages of Smart Tokens

Smart tokens introduce multiple advantages over the traditional exchange model:

1. **Continuous Liquidity** - Since purchasing and liquidating is done through the smart contract, smart tokens are always liquid, irrespective of their trading volume.
2. **No Extra Fees** - The only mandatory fees applied by a smart token are the blockchain platform fees (gas) which are relatively low.
3. **No Spread** - Since the price calculation is done algorithmically by the smart token, the same price applies for purchasing and liquidating the smart tokens.
4. **Predictable Price Slippage** - Smart tokens allow pre-calculation of the precise price slippage, based on the transaction size, before it is executed.
5. **Lower Volatility -** A smart token with a 10% CRR (for example) is comparable to an exchange with 10% of the ***entire supply*** of a token in its order-book at all times, forming substantial market depth. In a typical crypto-exchange, the share of the supply in the market depth at any given moment is well below 1%. The higher the CRR, the lower the smart token's price volatility. The lower the CRR, the more "new credit" is created relative to the original reserve amount.

The Bancor Protocol Ecosystem

Different parties can take on different roles in the Bancor network ecosystem. The primary forms of participation are as follows:

- **End-Users** can receive, hold, transfer, request, purchase and liquidate smart tokens.
- **Smart Token Creators** can issue new, always liquid smart tokens, that may be used for trading, token changing, as token baskets or as network tokens.
- **Asset Tokenizers** (e.g. Tether-USD, Digix-Gold) can issue ERC20 tokens representing external assets, thus enabling smart tokens to use these assets as reserve tokens. (Existing crypto-exchanges that operate under their local KYC regulations are well positioned to provide asset tokenization services.)
- **Arbitrageurs** are organically incentivized to constantly reduce gaps between prices on crypto-exchanges and the Bancor network. Smart tokens work similarly to exchanges in that purchasing them increases their price and selling them decreases it, so that the same arbitrage mechanics and incentives apply.

A Solution to the Coincidence of Wants Problem

The coincidence of wants problem[5], in the current asset exchange model, creates a situation where assets are required to be traded at a certain minimal volume or else face liquidity risk[6]. The cause for this limitation is that the chance of finding a second party with opposite wants to exchange with, correlates to the asset's trading activity level. Smart tokens solve this problem through the use of reserve tokens which embed market depth directly into the smart token's smart contract.

Smart tokens are a **technological solution** to the ***coincidence of wants problem*** for ***asset exchange***, rather than a labor-based solution as used in traditional (or decentralized) exchanges. The current laborers in asset exchange are the professional market-makers who provide liquidity and facilitate collaborative price discovery. In the domains of information exchange and trade, the technologies of writing and currency replaced labor-intensive solutions (speaking and barter) with technological ones, creating mass efficiencies for societies and unlocking collaboration on a global and intergenerational level. The Bancor protocol proposes to similarly advance the domain of asset exchange by replacing the need for labor with a technological solution to the existing coincidence of wants problem.

Smart Token Initiation and Customization

New smart tokens can be created simply by depositing an initial reserve/s and issuing the initial token supply. Alternatively smart tokens can be initiated through a crowdsale, where a part of the proceeds is allocated as the initial reserve.

[5] https://en.wikipedia.org/wiki/Coincidence_of_wants
[6] https://en.wikipedia.org/wiki/Liquidity_risk

The Bprotocol Foundation

Bprotocol is a Swiss nonprofit foundation whose core objective is the establishment of the Bancor protocol as a global standard for intrinsically tradeable currencies.

By contributing to the Bprotocol Foundation, users will generate BNT - the first smart token to be deployed using the Bancor protocol, establishing the ***BNT network.*** The Foundation will collaborate with different contractors to achieve its goals, as well as governments, businesses, academia and NGOs committed to realizing collaboration potential in communities around the world.

Bancor Network Token (BNT) - The First Smart Token

The BNT will hold a single reserve in Ether. Other smart tokens, by using BNT as (one of) their reserve(s), connect to the BNT network using the price discovery method outlined in this paper. The BNT network will include user-generated smart tokens, token changers (forming a global decentralized, highly liquid exchange), decentralized token baskets as well as subnetworks.

The BNT establishes network dynamics where increased demand for ***any*** of the network's smart tokens increases demand for the common BNT, benefiting ***all*** other smart token***s*** holding it in reserve. Naturally, it is also susceptible to decreased demand. The BNT will be sold in a fundraiser scheduled for June, 12, 2017 10:00 GMT.

BNT Crowdsale Objectives

- A portion of the funds raised will be used as the Ether reserve for BNT (details on the CRR will be outlined in the crowdsale launch announcement), enabling continuous liquidity to Ether for any BNT holder, as well as any holder of a smart token using BNT as a reserve.
- A portion of the funds will be used to develop, promote and support the open-sourced, blockchain-agnostic, Bancor protocol implementations, and support related technologies and applications such as an open-source, user-friendly web service (desktop and mobile) to provide wallet, marketplace, token-conversion, new smart token creation and crowdsale solutions.
- A portion of the funds will be used to set-up and propel the first batch of token changers for popular ERC20 tokens, which function as a ***decentralized solution for token exchange*** between all the included tokens. This model introduces key advantages, incentivizing ***asset tokenizer***s to represent additional real-world assets as Ethereum tokens.
- A portion of the funds will be used to participate in and support innovative and promising future smart token crowdsales in the BNT network. These may include new, location-based and vertical-specific smart token initiatives such as regional token networks, community currencies, crowdfunded projects and other online or offline token-based ecosystems.

Examples and Illustrations

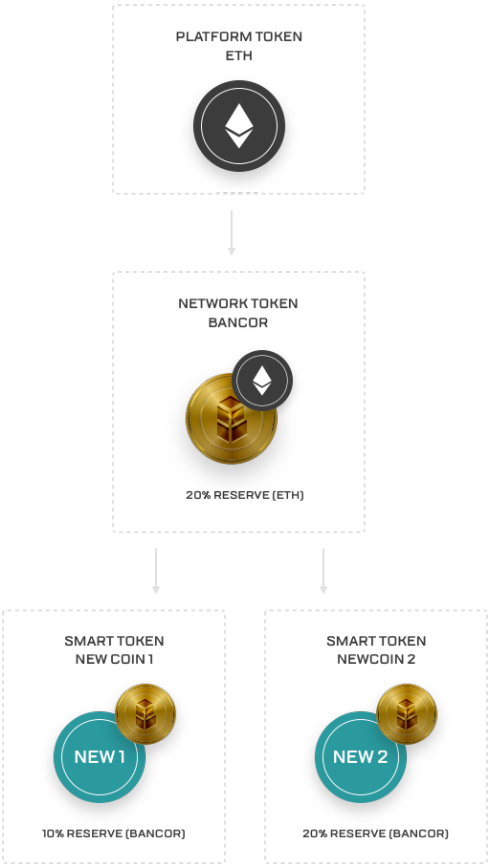
Example #1: Smart Token Transaction Flows

In this example, a crowdsale for a new token (BNT) has collected 300,000 ETH.

300,000 BNT are issued at a 1:1 ratio and transferred to the crowdsale participants. 240,000 ETH were directed towards funding the BNT project's development and 60,000 (20% CRR) were kept in the BNT smart contract as a reserve.

- Purchasing and liquidating BNT becomes possible as soon as the crowdsale is completed. The opening price is the last crowdsale price, in this example 1 ETH for the first BNT.
- BNT liquidators get ETH from the reserve of BNT, the liquidated BNT are destroyed, and the BNT price decreases respectively.
- BNT buyers get newly minted BNT, their payment in ETH is added to the smart contract reserve and the BNT price increases.

The ETH reserve always remains 20% of the BNT market cap.



Smart Token Symbol	BNT
Reserve Token	ETH (Ξ)
Constant Reserve Ratio (CRR)	20%
Initial Token Price	Ξ1
Crowdsale Proceeds	Ξ300,000
Tokens Issued in the Crowdsale	300,000

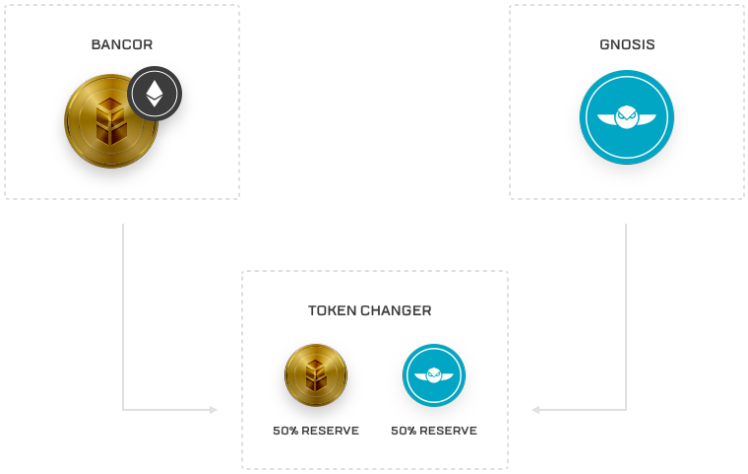
	RESERVE		PRICING			SMART TOKEN		
Activity	**ETH Recieved (Paid-out)**	**ETH Reserve**	**Effective BNT Price**	**Resulting BNT Price**	**Price Change**	**BNT Issued (Destroyed)**	**BNT Supply**	**BNT Market-cap**
Post-crowdsale initial state		Ξ60,000		Ξ1.0000			300,000	Ξ300,000
300 ETH converted to BNT	Ξ300	Ξ60,300	Ξ1.0020	Ξ1.0040	0.40%	**299**	300,299	Ξ301,500
700 ETH converted to BNT	Ξ700	Ξ61,000	Ξ1.0086	Ξ1.0133	0.93%	**694**	300,993	Ξ305,000
1302 BNT converted to ETH	Ξ(1,308)	Ξ59,692	Ξ1.0046	Ξ0.9959	-1.72%	**(1,302)**	299,691	Ξ298,460
100 ETH converted to BNT	Ξ100	Ξ59,792	Ξ0.9966	Ξ0.9972	0.13%	**100**	299,792	Ξ298,960

Link to Spreadsheet

Example #2: Token Changer Transaction Flows

In this example, a “BNTGNO” smart token is created to function as a token changer between BNT and GNO (Gnosis), holding both in reserve with a 50% CRR each, for a total of a 100% CRR.

Assuming a current market price of 1 BNT = 2 GNO, the contract can define the initial prices as 1 BNT = 2 GNO = 1 BNTGNO and in this example, 10,000 BNTGNO are issued to the depositors of the initial reserves.



- The opening prices are 1 BNTGNO = 1 BNT = 2 GNO as was set in the contract.
- The BNTGNO can be purchased with BNT or GNO.
  The BNTGNO price will increase for the reserve token it was purchased with (BNT or GNO), and decrease in the uninvolved reserve token (due to the increase in the BNTGNO supply).
- BNTGNO can be liquidated back to BNT or GNO, decreasing the BNTGNO price in the liquidated reserve token, and increasing it in the uninvolved reserve token.

This scenario demonstrates how a 100% backed smart token with two 50% CRR reserve tokens can function as a decentralized token changer, open for anyone to use, with its prices organically balanced by arbitrageurs. Both the token changer and the token basket automatically maintain their CRR ratios.

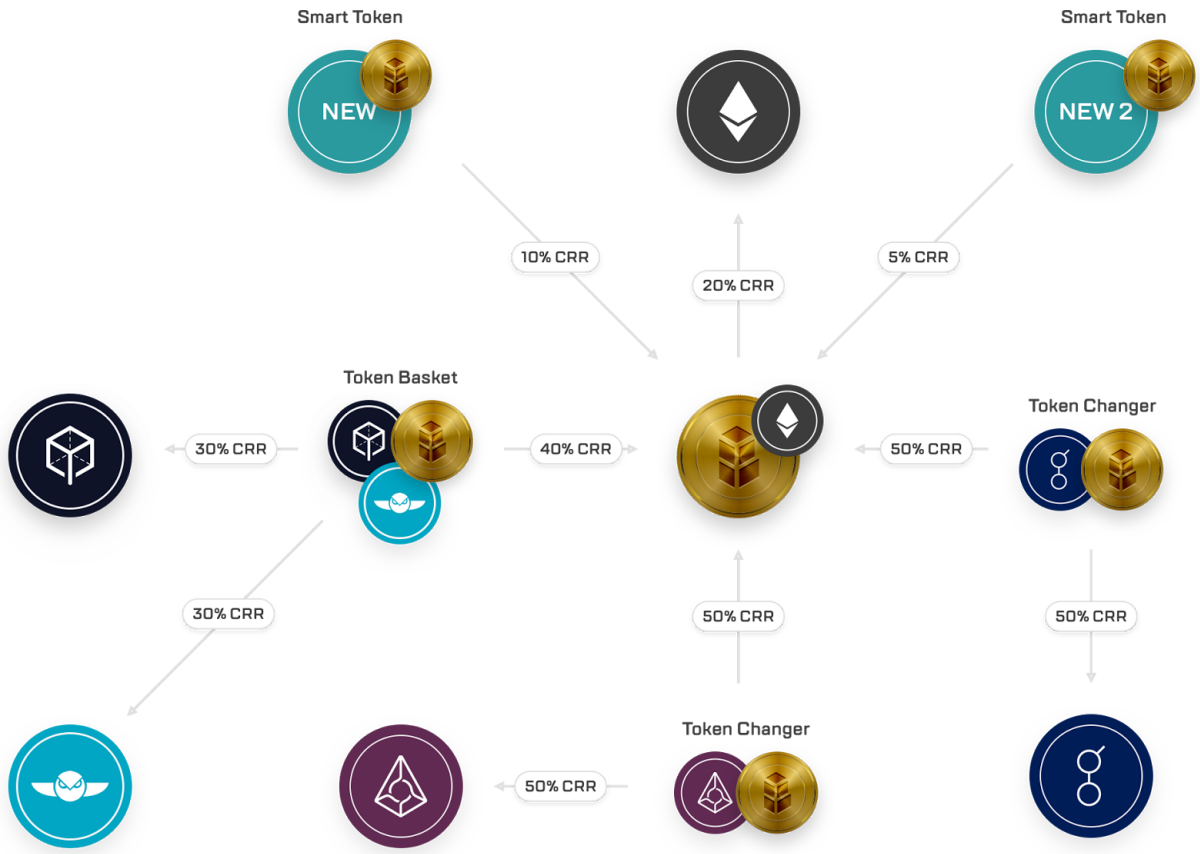
Smart Token Symbol		BNTGNO
Reserve Tokens		BNT + GNO
Constant Reserve Ratio (CRR)	**BNT**	50%
	GNO	50%
Initial Token Price	**BNT**	1
	GNO	2
Deposited Reserves	**BNT**	5,000
	GNO	10,000

		RESERVE		**PRICING**				**SMART TOKEN**		
Activity		**Reserve Recieved (Paid-out)**	**Reserve Balances**	**Effective BNTGNO Price**	**Resulting BNTGNO Price**	**BNTGNO Price Change**	**1 BNT = GNO**	**BNTGNO Issued (Destroyed)**	**BNTGNO Supply**	**BNTGNO Market-cap**
Initial State	**BNT**		5,000		1.000		0.500		10,000	10,000
	GNO		10,000		2.000					20,000
Buying BNTGNO for 30 BNT	**BNT**	30	5,030	1.0015	1.003	0.30%	0.503	**30.0**	10,030	10,060
	GNO		10,000		1.994	-0.30%				20,000
Converting 70 GNO to BNT Step 1 (GNO->BNTGNO	**BNT**		5,030		1.000	-0.35%	0.500		10,065	10,060
	GNO	70	10,070	1.9975	2.001	0.35%		**35.0**		20,140
Converting 70 GNO to BNT Step 2 (BNTGNO->BNT)	**BNT**	(35.0)	4,995	1	0.996	-0.35%	0.496	**(35.1)**	10,030	9,990
	GNO		10,070		2.008	0.35%				20,140

Link to Spreadsheet

Illustrative Map of a Potential Bancor Network

- BNT - The BNT, backed by Ether
- ETH, DGD, DGX, REP and GNT are standard Ethereum-tokens
- NEW - New smart tokens created (e.g. crowdfunding campaign, a community currency, etc.)
- Smart tokens hold reserves (arrows point to the reserve tokens)
- Token changers are 100% backed, and hold two or more reserves



Price Calculation Per Transaction

The actual price of a smart token is calculated as a function of the transaction size.

R - Reserve Token Balance
S - Smart Token Supply
F - Constant Reserve Ratio (CRR)

- T = Smart tokens received in exchange for ***E*** (reserve tokens), given ***R***, ***S*** and ***F***

$$T = S((1 + \frac{E}{R})^{F} - 1)$$

- E = Reserve tokens received in exchange for T (smart tokens), given ***R, S and F***

$$E = R(1 - \sqrt[F]{1 - \frac{T}{S}})$$

***Mathematical proof* available**[7]

Summary

The Bancor protocol standardizes smart tokens, enabling asynchronous price discovery and continuous liquidity for cryptocurrencies using constant ratios of reserve tokens held through smart contracts, acting as automated market makers. The Bancor protocol enables the creation of hierarchical monetary systems with no liquidity risk. The BNT will be used to establish the first decentralized interconnected currency exchange system which does not rely on matching bid and ask orders, thus remaining liquid irrespective of its trading volume. This system proposes the first technological solution for the ***Coincidence of Wants Problem*** in asset exchange, enabling the long tail of user-generated currencies to emerge.

Acknowledgements

We would like to express our gratitude to the many people who supported us as we wrote this paper. A special thanks to Meni Rosenfeld, Yudi Levi, Amatzia Benartzi, Ron Gross, Assaf Bahat, Sefi Golan, Joshua Alliance, Brian Singerman, Adi Scope, Dory Asher, Tal Keinan, Wings.ai, TheFloor, Arie Ben-David from the Israel Monetary Change Movement, Scott Morris of Ithacash and the Bancor team, Ilana, Asaf, Or, Omry, Itay and Mati. Your support and feedback were truly important to us in improving this document. Thank you.

[7] The mathematical proof is available online at https://goo.gl/HXQBUr