

Bancor Protocol

Decentralized networks for smart contract based tokens to enable continuous convertibility between them.

Eyal Hertzog, Guy Benartzi & Galia Benartzi

October 12, 2017

Version .991¹

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."

¹ This version of the whitepaper is an interim update to version .99 that was published on May 30, 2017. It is intended to update the whitepaper to reflect the current lexicon used to describe the Bancor Protocol™. It also removes as out of date discussion of the Bancor TGE and of certain product concepts which have since evolved. Bancor is in the process of writing a new whitepaper, which will lay out the next evolution of Bancor's vision.

Table of Contents

Table of Contents	1
The Bancor Protocol™	2
Background	2
Introducing Smart Tokens™: A Solution to the Liquidity Problem	3
A New Method for Price Setting	4
Use-Cases for Smart Tokens™	5
The Long Tail of User-Generated Currencies	5
Crowdfunding a Project	6
Token Relays	6
Network Tokens	6
Advantages of Smart Tokens™	7
The Bancor Protocol™ Ecosystem	7
A Solution to the Coincidence of Wants Problem	8
Smart Token™ Initiation and Customization	8
The Bprotocol Foundation	8
Bancor Network Token (BNT) - The First Smart Token™	8
BNT Crowdsale Objectives	8
Examples and Illustrations	9
Example #1: Smart Token™ Transaction Flows	9
Example #2: Token Relay Transaction Flows	10
Illustrative Map of a Potential Bancor Network™	10-11
Price Calculation Per Transaction	12
Summary	12
Acknowledgements	12

The Bancor Protocol™

Abstract: The Bancor Protocol™ enables the creation of networks of smart contract-based “Smart Tokens™.” Smart Tokens™ hold balances of one or more other tokens--“Connectors”--and have a built-in autonomous conversion mechanism that allows any party to instantly purchase or sell the Smart Token™ for one of its Connectors, directly through the Smart Token™ contract, at a price calculated by a formula which balances buy and sell volumes.

Bancor believes that Smart Tokens™ can address the challenge of liquidity² faced by conventional tokens, cryptocurrencies, and community currencies on three levels. First, and most fundamentally, by being autonomously convertible for their Connectors, and with an unconstrained supply that grows in response to purchases, each individual Smart Token™ has built-in liquidity that does not depend on counterparties or exchanges. Second, Bancor has developed specialized Smart Tokens™ that enable inter-convertibility between any two other Smart Tokens™ or, with an added step, between any Smart Token™ and any conventional Ethereum network token. Third, Bancor’s ultimate vision is that users will create their own tokens and community currencies in the form of Smart Tokens™ that hold a common Connector, enabling any Smart Token™ in the network to be converted into any other. Bancor’s own Smart Token™, BNT, is the common Connector in the first such network, which we call the Bancor Network™.

The Bancor Protocol™ is named in honor of the Keynesian proposal³ to introduce a supranational 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 currencies⁴ 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 often issued in token sales 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-

² “Liquidity,” as used here and by Bancor generally, follows its common usage with respect to cryptocurrencies and blockchain tokens generally, i.e. the relative ease with which they can be bought or sold. It is not intended to convey any technical sense in which the term may be used in securities or other regulated financial markets. Furthermore, when used in connection with transactions with Smart Token™ contracts, the price at which a Smart Token™ is liquid is the price autonomously set by the Bancor Formula, rather than at the perceived value of the buyer or seller.

³ <https://en.wikipedia.org/wiki/Bancor>

⁴ https://en.wikipedia.org/wiki/Community_currency

scale currencies (such as community currencies, loyalty points or other custom tokens) to be convertible for 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, which we refer to as “**Connectors**,” 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 Community Currency Liquidity Problem

Smart Tokens™ are standard Ethereum ERC20 smart contract-based tokens,⁵ which implement the Bancor Protocol™. Smart Tokens™ hold a balance of at least one Connector, which can be a different Smart Token™ or any ERC20 standard token.⁶ Each Smart Token™ can be bought or sold for any Connector that it holds, directly through the Smart Token™ contract. Through the formula at the heart of the Bancor Protocol™ (the “**Bancor Formula**”), the Smart Token™ adjusts the price at which the Smart Token™ can be converted to or from its Connector(s) in response to each purchase/sale conversion.

When a user sends a balance of a Connector to the Smart Token™ contract, the sent amount of the Connector is added to the balance held by the Smart Token™ contract, and the contract adds the appropriate quantity of the Smart Token™ to the balance associated with the user’s Ethereum address according to the Bancor Formula autonomous calculation. Conversely, when a user sends a balance of the Smart Token™ to the Smart Token™ contract, the contract deducts the amount from the user’s balance and sends the user the appropriate quantity of the Connector, as calculated by the Bancor Formula. In both cases, the conversion happens autonomously through the Smart Token™ contract, with no need for a counterparty, at the then-current price set by the Bancor Formula.

The formulaically-determined pricing, plus the ability of Smart Token™ smart contracts to create and destroy Smart Tokens™ in response to every purchase and sale through the contract itself, means that it is always possible to purchase a Smart Token™ with its Connector, and, so long as there is a balance of the Connector, to sell the Smart Token™ for its Connector. This autonomous buy/sell capability is not unique; the standard Ethereum.org tutorial for creating a token smart contract explains how to make a token smart contract that can hold ETH and enables users to instantly buy and sell the token for ETH at a set price built into the smart contract. (See here for that tutorial, which provides excellent additional background on how Ethereum smart contracts and tokens work.) What is unique about Smart Tokens™ is (1) the Bancor Formula coupled with (2) the Smart Token’s™ ability to create new tokens when a purchase is made through the contract, and to destroy tokens when a sale is made through the contract, resulting in a token supply which is adaptable to demand, as we explain below.

⁵ While the initial deployment of Smart Tokens™ is on the Ethereum network, Bancor intends to implement Smart Tokens™ on other smart contract-based blockchains.

⁶ As we discuss below, in this regard Smart Tokens™ are no different from any Ethereum ERC20 token smart contract. The ability of token contracts (and all other smart contracts) to hold balances of Ethereum and other tokens is an intrinsic functionality of the Ethereum protocol. We note also that our use of the concept of “held balances” follows standard usage with respect to Ethereum and blockchain protocols generally—i.e. the association of a quantity of a digital asset with a public address—and is not intended to carry any legal or regulatory implications with respect to ownership or custody.

A New Method for Formulaically Determining Price

Smart Tokens™ utilize a novel method for determining the price at which they can be converted to/from their Connectors, the Bancor Formula. The formula is driven by a constant that we call the “**Weight**,” and which must be greater than 0 and less than or equal to 100%. The Weight is set by the Smart Token’s™ creator, for each Connector, and used in price calculation, along with the Smart Token’s™ current supply and the balance of the held Connector, in the following way:

$$Price = \frac{Connector}{Supply \times Weight}$$

This calculation ensures that a constant ratio is kept between the Connector balance and the Smart Token’s™ **Total Token Value** (“**TTV**”),⁷ which is equal to the outstanding supply of the Smart Token™ times its price. Dividing the TTV by the supply produces the price according to which the Smart Token™ can be purchased and sold through the Smart Token’s™ smart contract. The Smart Token’s™ price is denominated in the Connector and readjusted by the Smart Token’s™ smart contract per each purchase or sale, which increases or decreases the balance of the Connector held by the contract and the Smart Token™ supply (and thus the price) as detailed below.

When Smart Tokens™ are purchased from the Smart Token’s™ smart contract (in exchange for any of their Connectors) the payment for the purchase is added to the balance of the Connector held by the contract, and based on the calculated price, *new Smart Tokens™ are created* and added to the buyer’s balance. Due to the calculation above, a purchase of a Smart Token™ with a less than 100% total Connector Weight will cause its price to increase, since both the Connector balance and the total supply of the Smart Token™ are increasing, while the latter is multiplied by a fraction.

Similarly, when Smart Tokens™ are sold to the Smart Token™ contract, they are subtracted from the seller’s balance and *removed from the supply* (destroyed), and based on the current price, the calculated quantity of the Connector is transferred to the seller. In this case, for a Smart Token™ with a Weight less than 100%, any sale will decrease the price.

This autonomous price-setting function works by constantly readjusting the current price toward an equilibrium between the purchase and sale 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 is actually a simplified version of the Bancor Formula. It accurately calculates the current price at any time. What it doesn’t do is incorporate the effect of a purchase or sale transaction on the net price paid/received for a given conversion size. With the actual Bancor Formula, when a purchase or sale is executed, the effective price is calculated as a function of the transaction size. The calculation can be described as if every conversion is broken up into infinitely small increments, where each

⁷ Total Token Value as used by Bancor is intended to be synonymous with the term “market cap,” which is often used in connection with tokens. Bancor believes that Total Token Value is preferable, as market cap, i.e. market capitalization, carries with it the incorrect implication that the value of a token’s outstanding supply can be equated to the outstanding value of the shares of a company.

increment is changing the Smart Token's™ supply, Connector balance, and thus its price, proportionally. This ensures that purchasing the same amount of Smart Tokens™ in a single conversion or in aggregate across multiple transactions would yield the same total price. Additionally, this method ensures that Connector balances can never be drained. Essentially, the effect of the transaction size on the price (due to its changing the Smart Token's™ supply and the Connector balance) is incorporated into the effective price for any transaction. The mathematical functions for calculating price per transaction size are discussed in more detail below.

Using this method, the Bancor Protocol™ can enhance liquidity and enable autonomous purchasing/selling for new Smart Tokens™ as well as *existing standard tokens*—which can be used as Connectors for backward compatibility. This use-case and others are described in detail below.

Use-Cases for Smart Tokens™

The Long Tail⁸ 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 or product oriented currencies). However, the need to achieve and maintain liquidity for these small or new currencies remains a significant barrier to their viability.

Smart Tokens™ are unique in that they can be purchased or sold 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 and autonomous 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 familiar use-cases are listed below.

Crowdfunding a Project

The crowdfunding space has been growing rapidly. Smart Tokens™ can be used for crypto crowdfunding initiatives. For example, a musician may collect funds to record an album, which would be sold online exclusively in exchange for the issued tokens.

⁸ https://en.wikipedia.org/wiki/Long_tail

Token Relays

Token Relays are Smart Tokens™ that hold two Connectors, with a total Weight of 100% and serve to enable the conversion among any Smart Tokens™ or *standard ERC20 token* they hold as Connectors.⁹ Token Relays are designed to provide means of converting between its Connectors.¹⁰

Per the Bancor Formula, each time Connector X is converted to Connector Y—the price of X decreases, while the price of Y increases. The Total Token Value of the Relay token, however, stays constant. This is because the TTV of the Relay token is simply the combined balances of the Connectors, which have increased (X) and decreased (Y) proportionally, a function of them each carrying identical Weight (50%) and a total Weight of 100%. As noted, any standard ERC20 token can be used as a Connector even if it is already traded in other exchanges.

As with all Smart Tokens™, a gap may open between the calculated price of the Smart Token™ or any of its Connectors and their prices in an outside exchange. This situation creates an arbitrage opportunity in which market forces function to balance the pricing between the exchanges and the Smart Token™, Token Relay or Connector’s calculated prices, in exactly the same manner that prices are balanced between multiple exchanges when their prices diverge for any reason.

A Token Relay’s creator may set a fee that would apply on each purchase/sale. Fees can be accumulated in the Connector balances.

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 Relay 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 Relay. While decentralized exchanges offer this benefit as well, Smart Tokens™ do not rely on trade volume to provide liquidity.

Network Tokens

A collection of Smart Tokens™ that use the same Connector form a *network of tokens*. The common Connector can be described as a “**Network Token**.” Since every token in the network is convertible to and from the Network Token (the common Connector), it is possible to convert between any two other

⁹ Note that Token Relays use the same smart contract code as any other Smart Token; the only distinction is in the setting of the Weight at 100%, and the use of two Connectors, each with a 50% weight.

¹⁰ The conversion technically occurs through a two-step process of purchasing the Token Relay with one Connector, and immediately selling it for the other. Bancor has developed “wrapper” smart contracts that automate this process so that from the user’s experience, the conversion from one Connector to the other occurs in a single step without the interim step in which the user holds the Token Relay.

tokens in the network via the Network Token. We call the network of tokens that hold BNT as a Connector the “**Bancor Network™**”.

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 independent 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 increase the utility and value of the Ethereum protocol itself.

An additional Network Token use-case is to interlink a set of Token Relays, each holding the Network Token as one of their Connectors and a second, standard token as the second Connector. This structure would enable converting any token in the network to another. For example, by holding the BNT Network Token as one of the Connectors in each Token Relay in the Bancor Decentralized Liquidity Network, all Token Relays and Connectors (which can be any standard ERC20 token) and all Smart Tokens™ using the BNT Connector are convertible for each other and for BNT at the formulaically determined rates.

Advantages of Smart Tokens™

Smart Tokens™ introduce multiple advantages over the traditional token model:

1. **Continuous Liquidity** - Since purchasing and selling is done through the smart contract, Smart Tokens™ can always be converted to/from their Connector(s), irrespective of their trading volume.
2. **No Extra Fees** - The only mandatory fees applied by a Smart Token™ are the blockchain platform fees (gas in the case of Ethereum), which are relatively low.
3. **No Spread** - Since the price calculation is done formulaically by the Smart Token™, the same price applies for purchasing and selling the Smart Token™.
4. **Predictable Price Changes** - Smart Tokens™ allow pre-calculation of the price change that will result from any purchase or sale at the then-current price, before the transaction is executed.
5. **Lower Volatility** - A Smart Token™ with a 10% Weight (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 Weight, the lower the Smart Token’s™ price volatility.

The Bancor Protocol™ Ecosystem

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

- **End-Users** can receive, hold, transfer, request, purchase and sell Smart Tokens™.
- **Smart Token™ Creators** can create and issue their own Smart Tokens™, that may be used as community currencies, Ethereum application tokens, rewards points, etc. and benefit from autonomous convertibility to other tokens in the network.
- **Arbitrageurs** are organically incentivized to smooth prices between prices on cryptocurrency exchanges and the Bancor Smart Token™ contracts (just as they do prices between exchanges).

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 problem¹¹, 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 risk¹². 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 Connectors 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 deploying the necessary smart contracts based on templates Bancor has made publicly available and then depositing an initial balance of one or more Connectors and issuing the initial token supply. Alternatively, Smart Tokens™ can be initiated through a token sale, where a portion of the proceeds is allocated as the initial Connector balance. The Bprotocol Foundation™

Bprotocol is a Swiss nonprofit foundation whose core objective is the establishment of the Bancor Protocol™ as a global standard for creating networks of interlinked community currencies and tokens. The Bprotocol Foundation has issued BNT as the world's first Smart Token™ (also Network Token) utilizing the Bancor Protocol™. The Foundation will collaborate with different developers, contractors, and other ecosystem participants 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™

BNT was issued through a token sale conducted on June 12, 2017. It has ETH as its sole Connector, with the Weight set at 10%. Following the token sale, on June 22, 2017 BNT's Smart Token™ functionality was activated when the Bprotocol Foundation deposited 50,000 ETH, initiating the Connector balance. At initiation, the price at which BNT could be purchased or sold for ETH was 1 BNT = .01 ETH, which is the same price at which BNT was sold in the token sale.

¹¹ https://en.wikipedia.org/wiki/Coincidence_of_wants

¹² https://en.wikipedia.org/wiki/Liquidity_risk

Examples and Illustrations

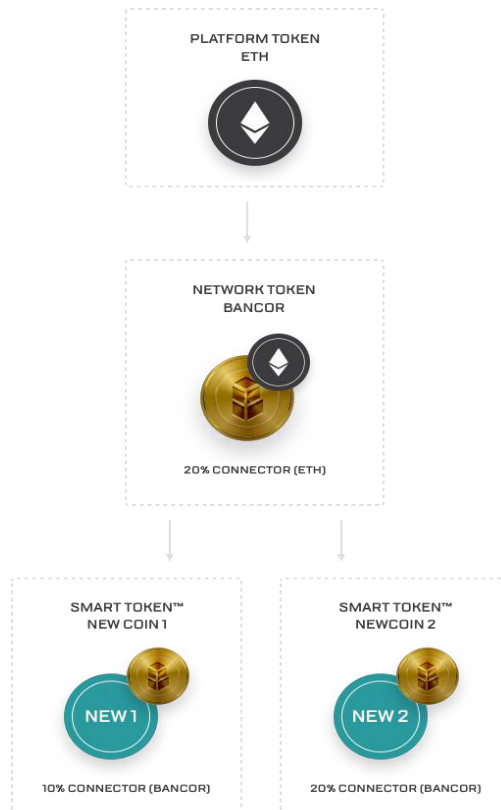
Example #1: Smart Token™ Transaction Flows

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

300,000 ABC are issued at a 1:1 ratio for ETH collected, and transferred to the token sale participants. 240,000 ETH were directed towards funding the ABC project's development and 60,000 were deposited in the ABC Smart Token's™ smart contract as its initial Connector balance.

- Purchasing and selling ABC becomes possible as soon as the token sale is completed and the Smart Token™ Connector is activated. The opening price is the last token sale price, in this example 1 ETH for the first ABC.
- ABC sellers send ABC to the Smart Token's™ smart contract, get ETH from the Connector balance, the sent ABC are destroyed (by being debited from the seller's balance with no corresponding credit elsewhere), and the ABC price decreases in the amount calculated by the Bancor Formula.
- ABC buyers get newly created ABC, their payment in ETH is added to ABC's Connector balance and the ABC price increases in the amount calculated by the Bancor Formula.

Since the Weight is set to 20%, the ETH Connector balance remains equal to 20% of ABC's TTV (i.e. the then-current price of ABC expressed in ETH times the total outstanding supply of ABC).



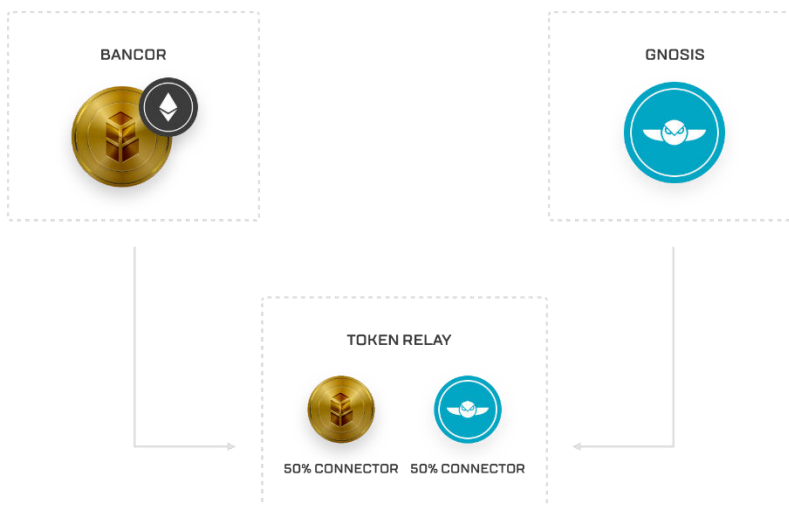
[Link to Spreadsheet](#)

Example #2: Token Relay Transaction Flows

In this example, a “ABCBNT” Smart Token™ is created to function as a Token Relay between BNT and a hypothetical existing Ethereum token, ABC. ABCBNT holds both BNT and ABC as Connectors with a 50% Weight each, for a total Weight of a 100%.

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

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



[Link to Spreadsheet](#)

Illustrative Map of a Potential Bancor Network™

- BNT - The BNT, with an Ether Connector
- ETH, DGD, DGX, REP and GNT are standard Ethereum-tokens
- NEW - New Smart Tokens™ created (e.g. token sale campaign, a community currency, etc.)
- Smart Tokens™ hold Connectors (arrows point to the Connectors)
- Token Relays have a 100% Weight, and hold two Connectors each with a 50% Weight

Smart Token™



Smart Token™



10% Weight

20% Weight

5% Weight



Token Relay



50% Weight

50% Weight

50% Weight



Token Relay



50% Weight



Price Calculation Per Transaction

The actual price of a Smart Token™ is calculated as a function of the transaction size.

C - Connector Balance

S - Smart Token™ Supply

W - Weight

- T = Smart Tokens™ received in exchange for E (Connectors), given R , S and F

$$T = S \left(\left(1 + \frac{E}{C} \right)^W - 1 \right)$$

- E = Connectors received in exchange for T (Smart Tokens™), given R , S and F

$$E = C \left(1 - \sqrt[W]{1 - \frac{T}{S}} \right)$$

[Mathematical proof](#) available¹³

Summary

Bancor Protocol™ standardizes Smart Tokens™, enabling formulaic price-setting and continuous convertibility for cryptocurrencies using constant ratios of Connectors held through smart contracts, obviating the need for counter-parties. BNT will be used to establish the first decentralized interconnected token network, which does not rely on matching bid and ask orders, thus providing for inter-convertibility among tokens in the network irrespective of 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.

¹³ The mathematical proof is available online at <https://goo.gl/HXQBUr>