# IMPLEMENTATION OF CENTRAL BANK DIGITAL CURRENCY

**Dr. Jianjun Cui and Wolfgang Blumental**

**cui@inasset.de**

**wechat: cui8161188**

# Summary

The dual system Bigtangle and Subtangle is the only possible solution for central bank digital currency.  Subtangle is a complete centralized system that can satisfies all requirements for central bank internal usage. For the internalization of central bank digital currency there must be a public chain like Bigtangle with Near-Time Confirmation, Infinite Scalability, Fee-less, Permissionless, Trustless, and Decentralized.

Otherwise it would be another Dollar and SWIFT system. In this system USA can lock the Dollar account of China.

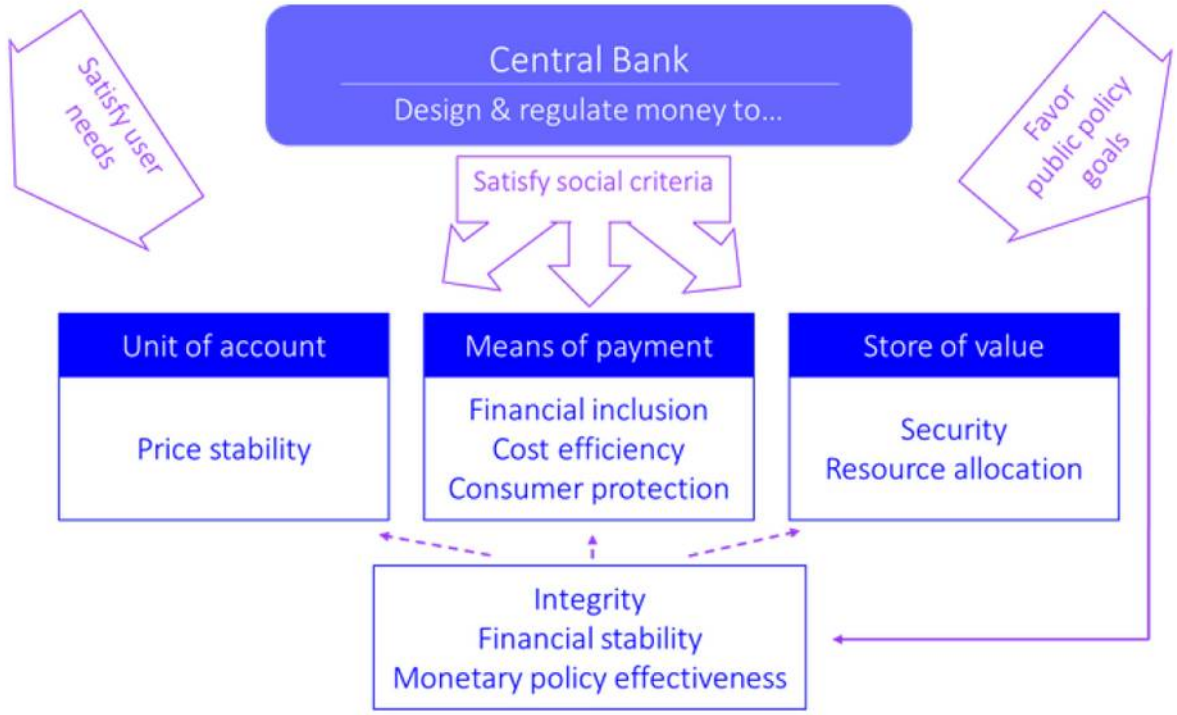
## Table of Contents



# Central Bank Digital Currency

**CBDC is a new form of money, issued digitally by the central bank and intended to serve as legal tender.**

Digitalization is reshaping economic activity, shrinking the role of cash, and spurring new digital forms of money. Central banks have been pondering whether and how to adapt.




• The impact of CBDC introduction will hinge on its design and country-specific characteristics. Critical features will be anonymity (the traceability of transactions), security, transaction limits, and interest earned. The role of cash and commercial bank deposits in payments will also matter.

• CBDC could strengthen the benefits and reduce some of the costs and risks to the payment system and could help encourage financial inclusion. CBDC will have to contend with operational risks arising from disruptions and cyberattacks.

• CBDC is unlikely to affect monetary policy transmission significantly, although operations may need adaptation. Transmission could strengthen **On the supply side, central banks play a pivotal role and ensure that money delivers on its three functions.** For central banks, this role means two things. First, because they are accountable to the public, central banks must design the money they issue—and regulate private forms of money—in a way that satisfies the user needs stated earlier. Second, because they are public policy institutions, they must ensure that money also meets important social criteria:

1. As a *unit of account,* money is an important public good that requires price stability in all economic circumstances. The design of money can favor or interfere with this goal. For instance, because cash pays no interest, central banks find it difficult to offer deeply negative interest rates following sharp recessions.
2. As a *means of payment,* money must be universally available and verifiable as well as efficient, while ensuring appropriate consumer protection and minimal cost to taxpayers.
3. As a *store of value,* money must be as secure as possible, but it must also allow for efficient allocation of resources.

**In addition, central banks will prefer forms of money that support, or at least do not undermine, three other public policy goals: financial integrity, financial stability, and monetary policy effectiveness.** In turn, each of these further supports the three functions of money. Financial integrity covers, among other things, anti–money laundering and combating the financing of terrorism (AML/CFT) rules, including customer due diligence measures and additional measures aimed at fighting corruption and fostering good governance.

**The last leg of the conceptual framework is to determine competitors to CBDC.** These fall into four categories, but will vary by country: cash, commercial bank deposits, narrow finance, and cryptocurrencies. All except cash are evolving and rapidly gaining market share.

***Commercial bank deposits* are going through notable improvements.** Payments have traditionally been facilitated by debit card networks. Today, two continuing transformations are notable, especially in advanced economies. The first stems from "wrapper" technology, which allows transactions to take place between mobile devices (bypassing expensive point-of-sale terminals) and adds a layer of security. The other is central-bank-provided fast-payment solutions ("fast payments"). These allow payments of any size and type (person to person, person to business, business to business) to be settled instantaneously by the central bank in reserve money through a dedicated platform running continuously at negligible cost.

***"Narrow finance solutions"* is a term introduced in this discussion note to capture the various new forms of private money backed one for one by central bank liabilities, either cash or reserves.** These offer stable nominal value, security, liquidity, and potentially close to a risk-free rate of return. The parallel here is with currency boards (such as in Hong Kong SAR) or metal-backed banknote systems (such as the gold standard). Two versions of narrow finance solutions are relevant. The

first is *stored value facilities17* such as AliPay and WePay in China, PayTM in India, M-Pesa in Kenya, and Bitt.com in the Caribbean. These provide *private e-money* to users against funds received and placed in custodian accounts. Transactions occur between electronic wallets installed on handheld devices, can be of any size (although they are usually not large), and are centrally cleared, but are restricted to participants in the same network. However, holding these forms of money entails some risk. Nonetheless, this segment is gaining widespread and very rapid acceptance. The second version of narrow finance solutions—*narrow banks*—is only beginning to materialize. It covers institutions that invest client funds only in highly liquid and safe government assets—such as excess reserves at the central bank—and do not lend. However, they allow payments in their liabilities through debit cards or privately issued digital money.

**One important criterion stands out: the ability to make anonymous transactions.** Regarding money, anonymity covers the extent to which identity and transactions are, or can be, disclosed to transaction parties, third parties, and the government. There are legitimate reasons people may prefer at least some degree of anonymity—potentially when it comes to everyone except the government, and regarding the government unless a court order unlocks encrypted transaction information. It is a way to avoid customer profiling—commercial use of personal information, for example, to charge higher mortgage rates to people who purchase alcohol. Another advantage of anonymity is limiting exposure to hacking. Moreover, anonymity is often associated with privacy—widely recognized as a human right (as stated in the Universal Declaration of Human Rights [Article 12] and elsewhere).

# Bigtangle

The Bigtangle is new generation of blockchain. The Bigtangle extends the blockchain technology  with integration of Markov Chain Monte Carlo (MCMC).  Thus BITCOIN and ETHEREUM are special cases in Bigtangle.

Through the use of industry-grade big data technology in conjunction with its parallelizable architecture, Bigtangle is a successor to Bitcoin that can fulfill economically important key use-cases.

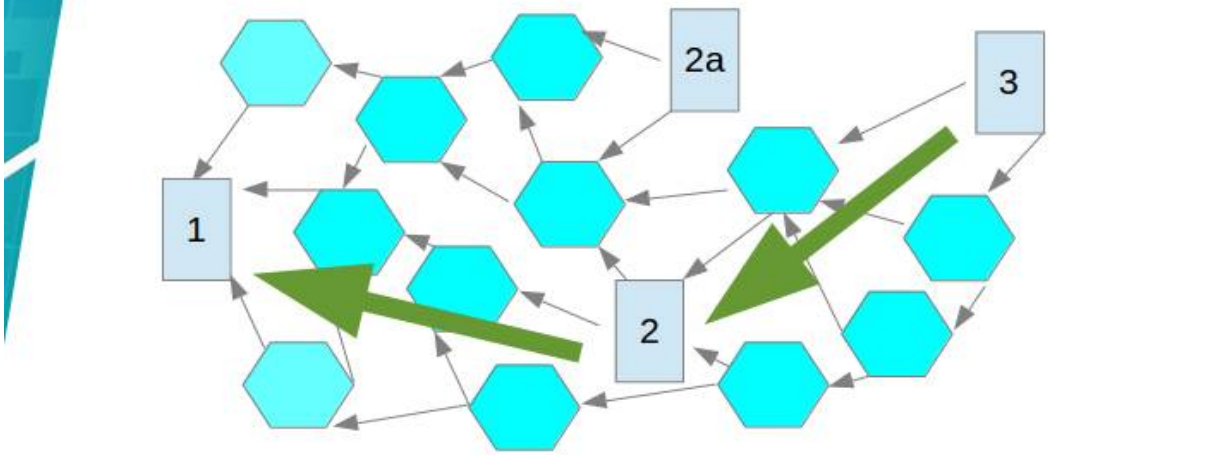
The Bigtangle is a decentralized cryptocurrency, payment, exchange, supply chain and e-commerce platform with the advantages:

1. Near-Time Transactions ,
2. Infinite Scalability,
3. Smart Contracts, Permissionless, Trustless,
4. Decentralized Exchange,
5. Ease of use,
6. Completely Feeless,
7. Quantum Security.

Bigtangle is inherently a client and server architecture.  The Bigtangle requires the same power consumption as Bitcoin as any systems based on PoW.

However, comparing the transactions per seconds (TPS), e.g. 10 TPS in Bitcoin or 200 TPS in Ethereum, Bigtangle with 10 server nodes in our clusters can achieve 1 Million TPS with the same power consumption. Big Data and blockchain parallelization are the only solution to get significant TPS at affordable costs. Keep in mind that replacing other technical processes with the Bigtangle network will also reduce total power consumption.

## *Maximum security, decentralization, scalability by integration into a genealogical tree*




Block with Transactions. Transactions are usually independent except for double spends. The MCMC consensus algorithm performs the selection process to solve conflicts.

Mining Reward Blocks are blocks with coinbase transactions only. Mining reward block must be in a chain over the Tangle. In the example above, blocks 1, 2 and 3 are such a chain. Let blocks 2 and 2a be in conflict. The MCMC consensus algorithm will solve this conflict by (in this case) having selected block 2 due to higher rating.

# Subtangle

The Bigtangle software can be deployed in private or other trusted environments, allowing one to run private, owned Bigtangle networks with different rule sets.

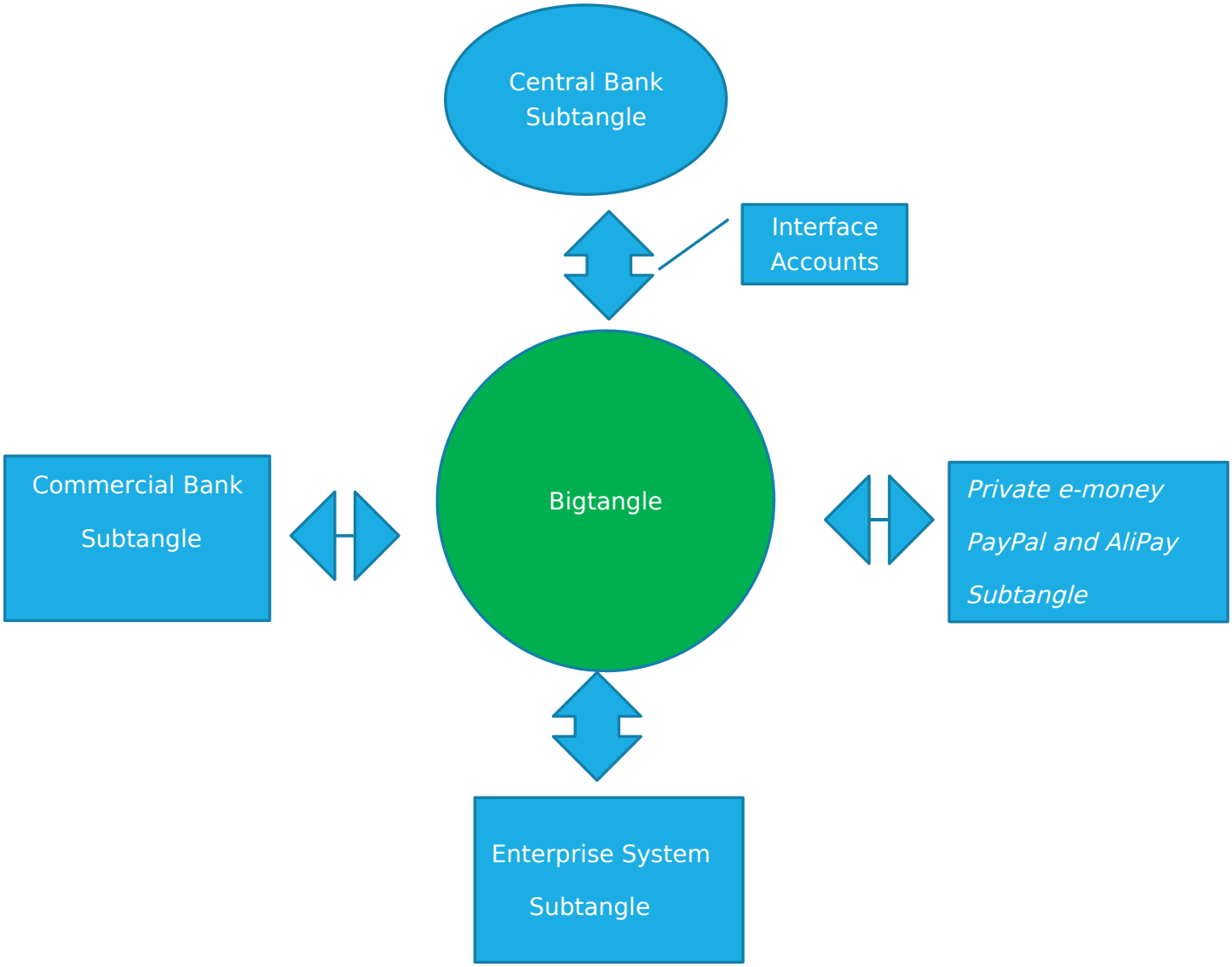
These Bigtangle networks are arranged in a hierarchy, i.e. they possess a parent Tangle such as the Mainnet between which a transfer of values is facilitated. For this purpose, each new Subtangle has its own interface accounts (addresses) possessed by the private operator from which it is possible to transfer funds into the parent Tangle and vice versa.

A user interested in transferring funds from the parent Tangle into one of its registered child Tangles can transfer tokens to one of the child Tangle's interface accounts, at which point they are either accepted into the child Tangle or returned by the trusted intranet owner.

Inside of such intranets, consensus protocol, transparency, permissiveness and other rules are set by the trusted intranet owner. Transfers of value can be performed internally as it is pleased. For example, in a work agency intranet it would be possible for clients to pay values to work forces in private and in arbitration of the owning work agency.

In general, enterprises and governments can deploy the software internally and e.g. do KYC (Know Your Customer) as well as privacy protection while remaining compatible with Bigtangle's Mainnet.

This allows Bigtangle to offer a holistic and flexible approach to value management, enabling privacy, transparency and accountability wherever needed by banks, stock exchanges or enterprises.


Central Bank Subtangle
Interface Accounts
Commercial Bank Subtangle
Bigtangle
Private e-money PayPal and AliPay Subtangle
Enterprise System Subtangle

# Implementation of CBDC

## Use Case for Central Bank Subtangle

1. Central Bank create new amount of CBDC.
2. Central Bank add new permission user account in Central Bank Subtangle
3. Central Bank transfer CBDC to user account in Subtangle.
4. Central Bank pay base interest to user account
5. Central Bank can revoke and lock CBDC of user account in Central Bank Subtangle
6. Central Bank transfer amount of CBDC via interface account into Bigtangle
7. User transfer CBDC from Central Bank Subtangle to Bigtangle.
8. User transfer CBDC from Central Bank Subtangle to commercial bank Subtangle
9. User transfer token to Central Bank Subtangle
10. Central Bank can create incremental CBDC.

## Use Case for a commercial bank Subtangle

1. Commercial Bank create new token for interest rate products
2. Commercial Bank do the lending as it transfers token to borrower and get paid.
3. Commercial Bank transfer CBDC to user and get the underlying asset as security
4. Commercial Ban transfer token to Bigtangle
5. User transfer token from commercial bank Subtangle to other Subtangle

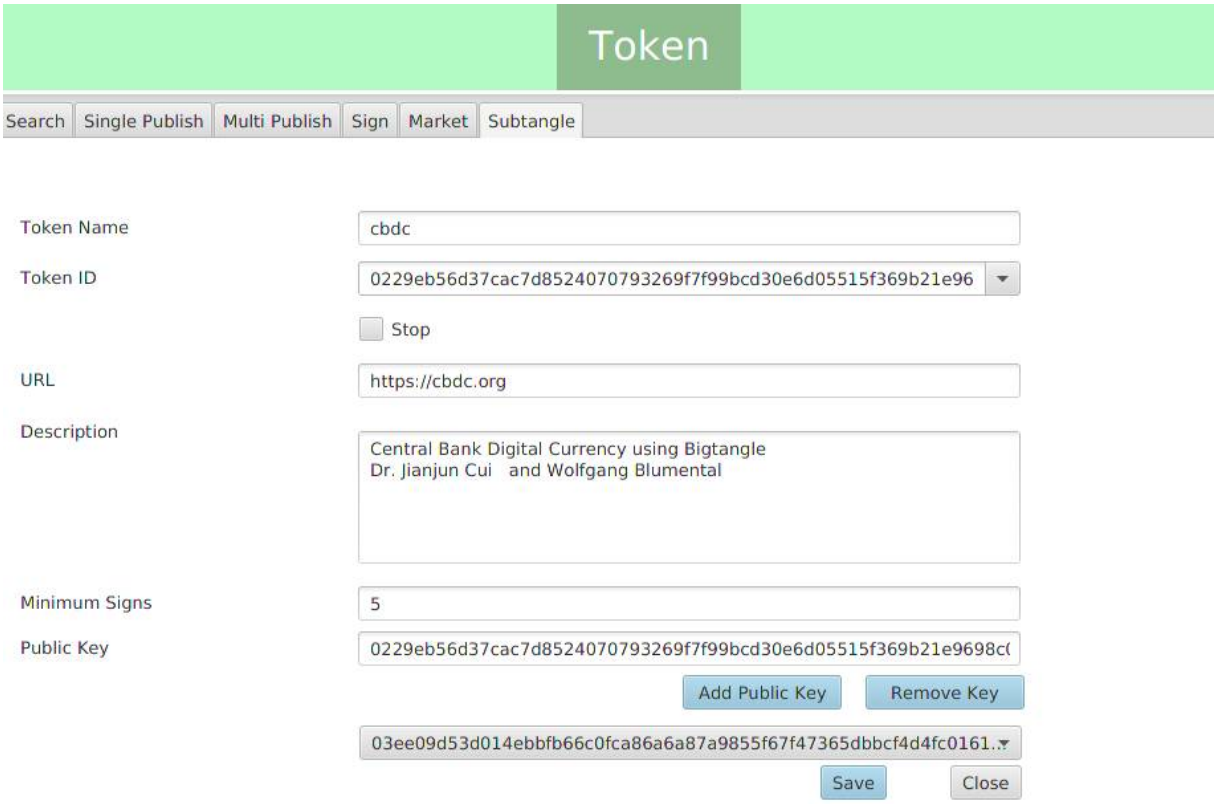
## Use Case for Enterprise Subtangle

1. Enterprise create new product.
2. Enterprise add new permission user account in Central Bank Subtangle
3. Enterprise transfer CBDC to user account in Subtangle.

4. Enterprise transfer token to Bigtangle

All above use cases are implemented in Bigtange and Subtangle. The detail description can be found in Bigtangle user guide. We show here only two important functions.

## Create CBDC Subtangle



# Transfer Token from Bigtangle to CBDC Subtangle