Bringing Decentralized Speed and Regulation to Crypto Economy
(Blinkchain Litepaper)

[WORKING-DRAFT]

Joby Reuben*
Auguth Tech Pvt Ltd.

1 Drawbacks of Current Blockchains

1. **Slower Consensus** - Leads to slower transactions and delayed confirmations.

2. **Security** - Multiple Hacks leading to users’ funds stolen due to smart contract issues in featuring loops (unpredictable output)

3. **Storage** - Heavy multiplied data with ineffective storage mechanism built into store everything the network consumes.

4. **Isolated** - Blockchains are independent entities from the shared data of global information as opposed to modern applications.

5. **Regulation** - Capital Gains and Income from cryptocurrencies and tokens are not taxed which leads to regulatory concerns and criminal activities.

6. **Cost for Computation** - Heavy cost for computing immutable logic compared to popularly available cloud computing.

7. **Single Transaction Token** - Confined to One currency for any activity carried inside the network. Creates demand and compulsory requirements for every region.

---

*jobyreuben@gmail.com
8. **Monetary Policy** - Logics are built inside blockchains to supply new tokens whereas a perfect monetary model shall include its contingency logics when it takes a downturn - restriction of spending.

2 **Solution**

- Blinkchain proposes a solution to eliminate low-throughput consensus models with a time-based model in which the propagation of blocks required to be sent across validators in a certain time period which can exponentially grow when the network nodes actively upgrade themselves with bandwidth, computation, etc.

- Accidental forks are eliminated with predictable production of blocks leading to instant confirmations. Aside from bringing speed, Blinkchain brings forth a non-native transaction fee model in which the users can pay using any token bounded by its transaction speed which directly denotes the token’s staked blocks per epoch.

- Blinkcoins solely provide access to security of the network, staking, yielding fees from blocks to delegators and producer nodes. The product is the most decentralized non-custodial staking system.

- Apart from it Blinkchain’s UTXOs are rentable which can increase scalability and eases heavy disk space consumption in high-throughput blockchains.

- Several native protocols and requirements such as oracles, wallets and more importantly onchain tax system can regulate cryptocurrencies without centralizing.

- Blink Scripts with a Parent-Child design methodology can bring scalable hybrid DApps without evading taxes.

- In short words, a bridge between real world and decentralized currencies which can regulate and legalize it’s spending without loosing its core principles of decentralization.

3 **Features in short**

3.1 **For users**

- **Fastest Consensus Algorithm** - A time-based competition for blinking speed confirmations

- **No Native Token Fees** - Transacting tokens can be paid for fees, as there is no requirement for special tokens.
• **Most Secure Transfers** - Turing Incomplete with predictable contracts removes current-issues of daily breaches.

• **Real-world Interoperability** - Native price oracles brings forth real-time market value into the Blinkchain of every asset through its Blink Oracles protocol.

• **Scalable Smart Contracts** - Parent-Child contract building design for scalable DApps with hybrid computation model

• **Cheaper Gas** - Fixing gas cost at a base fee i.e., at 0.0001 dollars for a basic transaction gas similar to Ethereum’s 21000 gas units can make computation cheaper

### 3.2 For Validators / Investors

• **Reward for work** - Hash rewards provide rewards based on the validation of individual transactions over a period of time.

• **Fastest Validation** - Parallel Validation of Transactions benefiting the Proof of Speed consensus.

• **Multi-Stake Model** - Blockchain’s novel staking system will be the first retail staking protocol without custodians. The most decentralized staking protocol.

• **Zero Slashing model** - Without slashing collateral, blinkchain punishes validators and gives back investors/delegators their staked blinkcoins for production.

### 3.3 For Governments

• **Region-based wallets** - Wallet addresses can be explicitly (publicly) identified with their region i.e., state, country, and type i.e., personal, merchant, government, non-profit.

• **Onchain Gains & Stable Taxation** - Governments can remit taxes automatically upon consuming UTXOs with their tax slabs for the type of wallets.

• **Point of Sale Tax** - Goods and Service taxes or VAT can be included in a transaction for purchasing merchant goods which shall be directly sent to government wallets making taxes on point of sale.

• **Zero Tax evasion** - Digital tax evasion is not carried out due to smart contract design, public ledger, and immutable rules.
4 Architecture

4.1 Tri-consensus Layer

1. **Proof of Speed** - A time-based competition that requires highly efficient validators to propagate mined blocks in a certain period of time. It includes mutable block size and time fixed according to the participating contestants for the next epoch election and production.

2. **Proof of Choice** - Blink’s staking protocol with a choice given to delegators to bring forth high throughput per token basis. Delegators are required to stake for their choice of tokens in blinkcoin for a specific block height which can improve the token’s tps by collateralizing the maximum amount of blocks per epoch. Validators can mine only the token’s transactions which are collateralized according to the staking requirement.

3. **Proof of Hash** - UTXOs are rented instead of stored similar to cloud storages in which the transaction fees determine the lifetime of an individual UTXO if expired a penalty is imposed to recover it. Transactions are pruned and replaced with a fingerprint after all the UTXOs in it are consumed fully. Scalability is increased and disk space is recovered.

4.2 Transaction Fees

1. **Pay in any Token** - Flexibility of paying in transacting tokens where there is no native gas fee similar to tokens like Ether, Ada, Sol, etc. Makes life easier for users.

2. **0.05% of the Token** - Fixed cheaper transfer fee similar to existing payment solutions like VISA, Mastercard, etc. Transaction fees for a value script (UTXO which holds value) is a sum of the gas fee (computation) and transfer fee (value) whereas a logic script only charges the gas fee.

4.3 Blink Oracles

1. **Subscriber-based oracles** - Validators are asked to submit their submissions by subscribing to exchanges’ price data. Validators with the most subscribed data shall increase their block production rate at the next epoch with benefits.

2. **Benefits for exchanges** - Centralized trading platforms can register their information and submit periodic market rates for which they can charge validators per submission basis.

3. **Real-time data** - Blinkchain’s native-level price oracles can perform, calculate, and attest transactions which require real-time market data.
4.4 Regional Wallets
Segregated by States and Countries - Wallets are identified by vanity address and prefixes are chosen for a specific country, state, and type. Only vanity addresses with selected pattern transactions are approved by validators to efficiently tax the onchain registries.

4.5 Regulation compliant
1. **Capital Gains and Stable Taxes** - Independent Taxation provided to countries without giving up decentralization.

2. **White-crypto** - Fully decentralized with the ability to levy hidden taxes can make cryptocurrencies in blinkchain friendlier to nations, which leads to accepting it as a commodity or currency.

4.6 UTXO Smart Contracts
1. **Secure Turing-incomplete contracts** - Predictable arbitrary code without security vulnerabilities


3. **Most secure DAapps** - Bitcoin script is proven to be more secure than current smart contract languages due to its limited features. A hybrid on-chain and off-chain application can be constructed using the Parent-Child script design which will make DAapps more secure and in-exploitable.

5 Compare & Compete
- **Bitcoin** - Decentralized Money
  - **Competitors** - Dogecoin, Litecoin, Zcash, Bitcoin Cash
- **Ethereum** - Decentralized World Computer
  - **Competitors** - Solana, Cardano, AVAX, Avalanche, Polygon
- **Blinkchain** - Decentralized World Bank
  - A permissionless blockchain as a bridge to regulate real-world and decentralized currencies with faster consensus models and secure advantages to current smart contract chains.
6 Tokenomics

Blinkchain’s native coin is Blinkcoin - A fixed supply native token beneficial for the Proof of Choice staking protocol. It is inflationary for rewarding validators over a period of 9 years gaining the issuance rate in starting years, attaining it’s peak, and drops to 0 in the 10th year. Its tokenomics summary is stated below, Premined = 5 million coins. Supply cap = 7.25 million. Inflation rate = 45% in 9 years. Supply curve:

7 Future

Future of Blinkchain resides on the following technologies:

- **Non-Profit Financial DApps**: Native Apps that follow the Parent-Child script design to make feeless non-profit financial services such as exchanges, lending & borrowing, credits, insurance, escrows, etc.

- **Interoperable DApps**: Accessing other blockchain DApps through blinkchain with a technology known as anchored smart contracts.

- **Blink Cash**: Digital cash based offline settlement protocol that can bring digitized denomination transfers between devices and cards.

- **Auguth DAO**: A Decentralized Organization that governs the blinkchain.
• **Regulatory Features**: Working with accepting blinkchain as a legal tender blockchain, in which its assets can be spent and taxed under the specific regional rules.

• **General Smart Contracts**: Bringing Turing-complete yet secure smart contract deployment features for developers to run more arbitrary programs on top of blinkcoin.

• **Single Assets Manager**: The Layer 0 protocol for all assets secured by cryptography and a distributed permissionless network

## 8 Roadmap

The Roadmap is distributed in Phases. Each phase is represented by its pre-thought vision for the phase of time. The names are taken from Old Valyria Gods from the series of Novels “Game of Thrones” by George R.R Martin where each phase represents its deity’s importance.

1. Phase **Shrykos** - Initial Implementation of Blinkchain
2. Phase **Meleys** - Non-Profit Financial DApps
3. Phase **Tessarion** - Blink Cash - Digital Offline Money
4. Phase **Arrax** - Auguth DAO
5. Phase **Syrax** - Regulation Adoption by countries
6. Phase **Vermax** - Anchored Smart Contracts
7. Phase **Vermithor** - Generalized Native Smart Contracts

After the initial implementation - The Shrykos Phase, all the further phases, and their development will commence after its whitepaper describing the protocols is published for public review. Each Phase shall be in simultaneous development for effective time management.

## 9 Community

1. LinkedIn Auguth Employees: [https://www.linkedin.com/company/auguth/](https://www.linkedin.com/company/auguth/)
2. Open-Source Contributors: [https://github.com/blinkchain](https://github.com/blinkchain)
3. Discord Community: [https://discord.gg/2X9rcXCWa2](https://discord.gg/2X9rcXCWa2)
10 Contact

- Website: blinkchain.org
- Twitter: https://twitter.com/Blink_chain
- Discord: https://discord.gg/2X9rcXCWa2
- Reddit: https://www.reddit.com/r/projectblink
- Medium: https://medium.com/@projectblinkchain
- Github: https://github.com/blinkchain
- LinkedIn: https://www.linkedin.com/showcase/projectblink/
- Instagram: https://www.instagram.com/project_blinkchain/
- Email: mailto:projectblinkchain@gmail.com