

QUANTUM-RESISTANT CRYPTOCURRENCY BALANCING PRIVACY AND ACCOUNTABILITY

Investment Highlights

Built by the inventor of Linkable Ring Signatures:

- 20+ years of experience in cryptography with technologies such as zero-knowledge proof systems and digital signatures.
- 4 years of experience in developing blockchain systems: Bitcoin, Ethereum (Eris Industries /Monax), Tendermint, R3 Corda and Hyperledger Fabric.

Huge demand for privacy focused cryptocurrencies:

- Privacy tokens such as Monero (XMR) and Dash (DASH) together represent a total market cap of greater than USD 2bn.
- They have achieved a market capitalization growth of 571x and 121x respectively since 2016, outpacing Bitcoin and the general cryptocurrency market.

World Class Collaborating Researchers:

- The Abelian team includes many world class researchers in cryptography, mathematics, computer science, software engineering and blockchain development area.

Abelian Features



Privacy

- Leveraging proven technology including ring signatures, cryptographic commitment schemes and zero-knowledge proofs.
- The Abelian platform offers a level of privacy that is unmatched in the cryptocurrency space.



Accountability

- The ability to accommodate the needs of enterprise applications and third party authorities without sacrificing the privacy of the user is built into the Abelian platform.



Quantum-resistance

- The Abelian platform is being built upon lattice-based cryptography, which allows the creation of next generation quantum resistant cryptocurrency.

Quantum Attack Possible in 5-year Time

Although the ECC technology was once endorsed by NSA, however NSA has publicly issued a warning against the use of ECC is August 2015 due to the advent of quantum computing. It is expected that quantum computing will be able to break ECC in 5-10 years. Quantum attacks loom large and this is exactly why the safety of cryptocurrency should be given a close look.

To enable quantum resistant security, we should replace the current underlying hard problems with problems that are deemed intractable for quantum computers to solve. Upgrading from ECC to Lattice based cryptography is widely considered to be a quantum resistant solution.

	ECC	Lattice-based
Mathematical problems	<ul style="list-style-type: none"> • Two dimensional • Derive a multiplicand from points on an elliptic curve 	<ul style="list-style-type: none"> • Multi-dimensional • Find a vector or a point in the lattice given some information about the lattice
Implementation concern	<ul style="list-style-type: none"> • Not considered quantum resistant, and thus at risk as faster quantum computers emerge 	<ul style="list-style-type: none"> • Practical efficiency is challenging to achieve due to large lattice-based key and signature sizes (solved in Abelian through IPFS protocol)

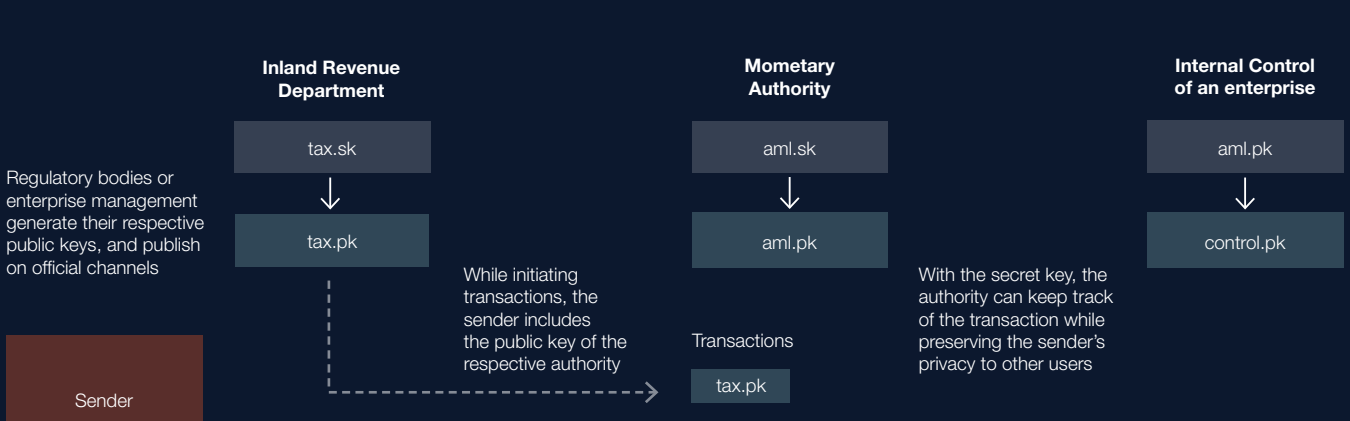
Proven Technology to Offer Uncompromising Privacy

Leveraging proven technology including ring signatures, cryptographic commitment schemes and zero-knowledge proofs, Abelian offers unmatched privacy in the cryptocurrency space.



Optional Accountability to Enable Enterprise Adoption

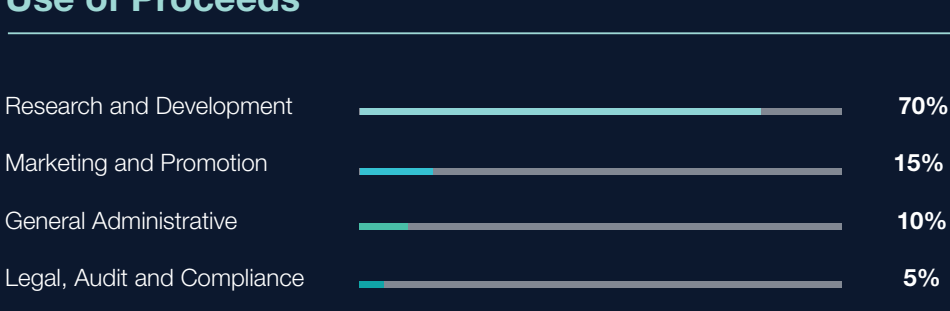
Abelian coin provides the ability to accommodate an authority's need to open up the privacy protection of a transaction and it supports enterprise applications while preventing the misuse of the protocol by parties seeking to engage in criminal activities.



Team and Advisor

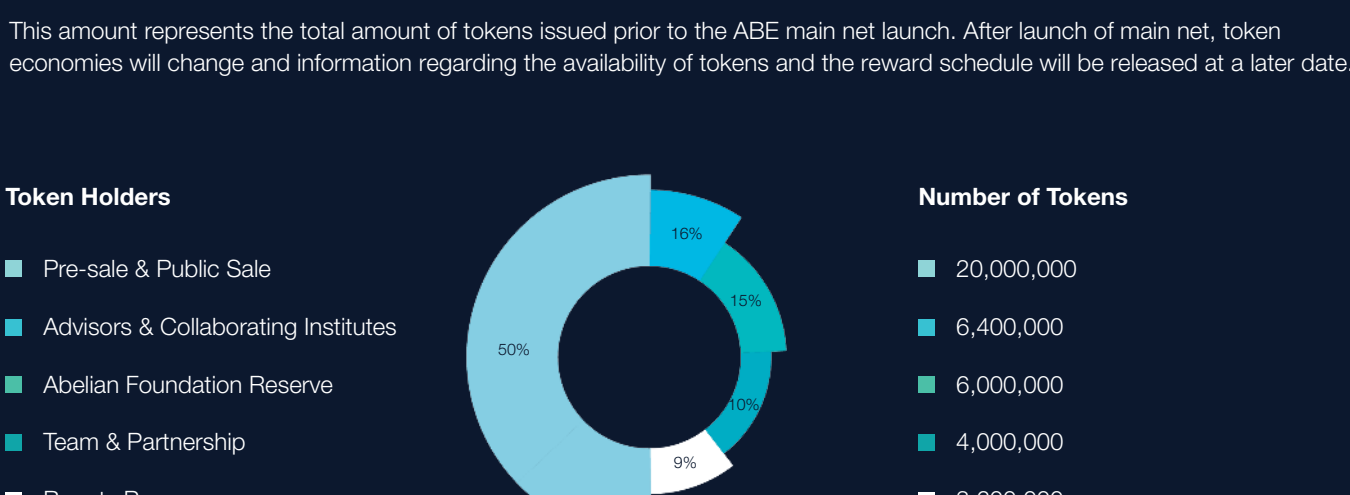
 Dr. Duncan S. Wong Co-Founder & CEO of CryptoBLK Co-Inventor of Linkable Ring Signature	 Andrew Hon Co-Founder & CTO of CryptoBLK	 Professor Huaxiong Yang Nanyang Technological University (NTU)	 Professor Guomin Yang University of Wollongong (UOW)	 Professor Liu Zhen Shanghai Jiao Tong University (SJTU)
 Dr. Khoa Nguyen Nanyang Technological University (NTU)	 Collin Thompson Co-Founder & MD at Interpid Ventures	 Kazim Rifat Özyilmaz Founder at Monolytic	 Ankit Malik Blockchain Research Manager at Interpid Ventures	 Harsh Patel EIR at Interpid Ventures

Use of Proceeds



Token Allocation

This amount represents the total amount of tokens issued prior to the ABE main net launch. After launch of main net, token economies will change and information regarding the availability of tokens and the reward schedule will be released at a later date.



Together let's unleash the magnificent power and potential of the accountable privacy and post-quantum capability of Abelian.

We are getting everything ready, follow us on:
<http://abelianfoundation.org>