SARSON FUNDS

Real. Clear. Crypto.™

DIGITAL ASSET INVESTOR GUIDE TO CRYPTOGRAPHY

PREPARED BY SARSON FUNDS

WWW.SARSONFUNDS.COM

UNDERSTANDING HOW CRYPTOGRAPHY POWERS DIGITAL ASSETS

Understanding the basics of cryptography is essential to comprehending the mechanics of digital asset transactions and blockchain security.

For the digital asset investor, advances in cryptography present exciting new blockchain investment opportunities.

As advanced cryptography solutions for digital assets begin to emerge, they represent a new frontier of exploration for digital asset investors.

PICTURED: SARSON FUNDS TEAM MEMBERS (LEFT TO RIGHT)
JACOB STELTER, LINDSEY TROSTLE, JAHON JAMALI, JOHN SARSON, BRITTANY KEELS, AND BRYAN PROHM

Sarson Funds is pleased to provide this guide to help investors understand cryptography and discover emerging opportunities in digital asset encryption.

Warm regards,

JOHN R. SARSON
MANAGING PARTNER

JAHON JAMALI
MANAGING PARTNER

VISIT US ONLINE AT WWW.SARSONFUNDS.COM FOR MORE RESOURCES.

All investment products are available to accredited and qualified investors only. No bank guarantees. Not FDIC insured. Past performance does not indicate future performance.

CRYPTOGRAPHY: A BRIEF HISTORY

CRYPTOGRAPHY COMES FROM THE GREEK ROOTS 'KRYPTO' AND 'GRAPHENE,' MEANING 'HIDDEN WRITING.'

Two inherent human needs spurred the development of cryptography: information sharing and selective communication. The roots of cryptography are found in ancient Rome and Egypt, with the first known evidence of cryptography being the use of the hieroglyph, some 4000 years ago.

Scholars moved on to using simple, mono-alphabetic substitution ciphers between 500 and 600 BC, which involved replacing letters of messages with other alphabets using secret rules. The Romans took this further with their own cryptographic substitution method, known as the Caesar Shift Cipher.

Cryptography saw improved techniques through the 15th century with Vigenere Coding, while the 19th century brought the evolution from ad hoc encryption approaches to more sophisticated methods of information security.

In the early 20th century, the arrival of devices like the Enigma rotor machine provided more advanced and efficient means of coding information. During World War II, both cryptography and cryptanalysis became entirely mathematical.

SYMMETRIC ENCRYPTION

Until the 1970s, cryptography had been based on symmetric keys. Symmetric encryption utilizes one key to encrypt and decrypt data.

In symmetric encryption, a user's message is encrypted by a password key and sent to another user, who then uses that same key to decrypt the data and translate it into an understandable format.

Data encryption makes data unreadable to anyone without the required password key, so the key must be shared in order to decrypt the data and understand the message.

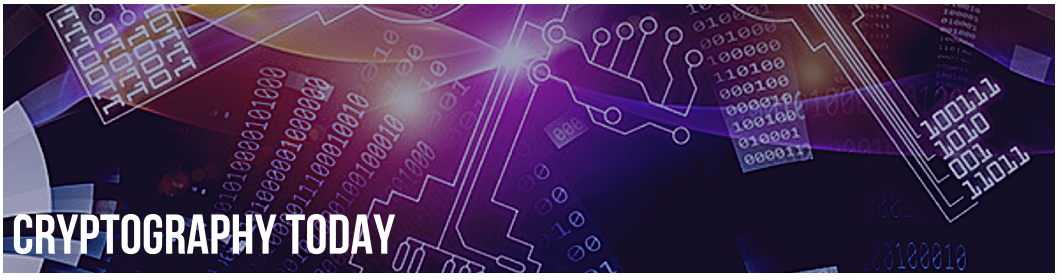
ASYMMETRIC ENCRYPTION

Asymmetric encryption, or public key cryptography, is an enhanced version of symmetric encryption that equips two password keys - one for encryption and one for decryption - to securitize a given dataset.

Many have heard the term data sovereignty: the idea that data is subject to the governing laws of the nation where it is collected. The increasingly personalized nature of your data, and the demand for its commercialization, has blurred the lines between data sovereignty and self sovereignty.

The distributed nature of the world's digital infrastructure is inspiring the drive for data self-determination past state control and into the hands of individuals themselves.

DATA SOVEREIGNTY AS A PATH TO SELF SOVEREIGNTY



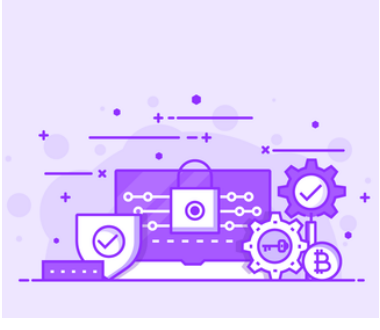
CRYPTOGRAPHY TODAY

METHODS OF ASYMMETRIC ENCRYPTION EXAMINED

In asymmetric encryption, one key, the public key, is used to encrypt data and another key, the private key, is used to decrypt that same data, with each key being the only one that can perform its assigned utility. Thus, the public key cannot be used to decrypt shared data and the private key cannot be used to encrypt that same data. In asymmetric encryption, the public key is made available for public knowledge and the private key is concealed. Asymmetric encryption is widely used in day-to-day communication channels. Popular asymmetric encryption algorithms include RSA (Rivest–Shamir–Adleman), DSA (discrete logarithm), and Elliptic curve techniques.

Advanced methods of asymmetric encryption use prime number factorization, which is used in RSA encryption. To employ this technique, two large prime numbers are found and multiplied together to get a product. Multiplying them together is simple for a computer, but deconstructing the product to find the beginning prime factors is computationally infeasible. Of course, since RSA is widely used, it has sparked intense interest in factorization approaches to encryption, so this method may weaken over time.

The discrete logarithm (DSA) approach takes prime number factorization further, and involves finding the prime factors of a randomly-generated integer along an elliptic curve that solve an associated logarithmic equation. Elliptic curve encryption uses the mathematics of elliptic curves to securitize the private key passwords associated with public key encryption. The elliptic curve approach is rooted in the assumption that based off of an elliptic model's curvature, guessing the prime factors of randomly-generated base points, the public key integers, is impractical due to how long it would take to guess the associated private key and decrypt the data. Guessing the private key is impractical because finding it involves solving the nearly unsolvable prime factorization of the discrete logarithm associated with the curve's public key.



CRYPTOGRAPHY IN BLOCKCHAIN

Cryptocurrencies use encryption techniques to securitize their data. Cryptography ensures the safety and security of a transaction by encrypting the data and value of the transaction on a blockchain. Cryptocurrencies use symmetric and asymmetric encryption, while Bitcoin specifically uses elliptic curve cryptography.

QUANTUM LEAP:
REVISITING ONE-TIME PAD AND HOW QUANTUM COMPUTING WILL DRIVE CRYPTOGRAPHY'S NEXT EVOLUTION

QUANTUM COMPUTING

Unlike ordinary classical computers, quantum computers are constructed on different underlying mechanisms of physics. Because quantum computers rely on different physical mechanisms, they are capable of performing computations much quicker than classical computers can. For some encryption algorithms, quantum computing will enable those without a private key to conduct a brute-force search through the use of a key extraction algorithm that can quickly decode the password.

Public key cryptography algorithms grow increasingly vulnerable as quantum computing becomes more developed.

REVISITING ONE-TIME PAD AND EMERGING ADVANCES IN DIGITAL ASSET CRYPTOGRAPHY

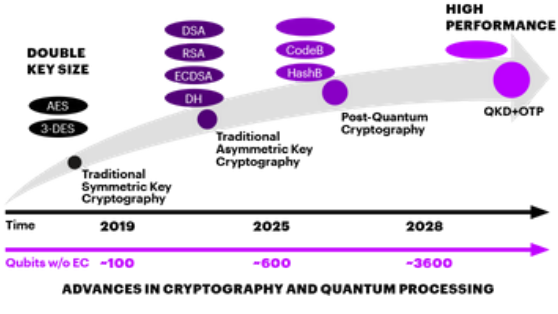
The gold standard of data encryption, one-time pad, is an uncrackable encryption technique with perfect secrecy. This encryption method pairs a data message with a randomly-generated private key, the one-time pad. The pad then uses modular addition to encrypt each character of the message by linking them with the corresponding character of the pad. The resulting encryption will only be impossible to decrypt if the key is truly random, at least the length of the original message, never reused, and kept completely secret. One-time pads will continue to remain secure even as quantum computing develops.

Legacy methods of one-time pad encryption have remained impractical as they require the use of a large private key at least the same size as the data message being encrypted. Although one-time pads have long been recognized as the blue-chip cryptographic solution, their hefty sizes deem them unreasonable to use until more practical applications arise.

Will quantum computing accelerate a market drive for the rational use of one-time pad encryption protocols? We are beginning to witness this drive today as the widespread adoption of cryptocurrencies and blockchain technology stimulate the demand for uncrackable cryptographic solutions for a digital asset fueled economy. Investment opportunities for advanced digital asset cryptography methods are emerging as a new frontier for cryptocurrency investors.

CRYPTOGRAPHY
HISTORICAL TIMELINE

400 B.C.	SPARTAN SCYTALE
50 B.C.	CAESER SHIFT CIPHER
1465	VIGNERE CIPHER
1800	JEFFERSON WHEEL CIPHER
1917	VERNAM STREAM CIPHER / ONE TIME PAD
1920	GERMAN ENIGMA
1976	DATA ENCRYPTION STANDARD (DES)
1977	RSA PUBLIC KEY ENCRYPTION
PRESENT	QUANTUM CRYPTOGRAPHY



(CHART ABOVE, COURTESY: ACCENTURE)

QUANTUM CRYPTOGRAPHY'S
FUTURE TIMELINE

Quantum computing's emergent role in driving new cryptographic solutions has many investors looking for opportunities that provide the security of one-time pad with transactional feasibility.

One-time pads are unconditionally secure in any computation model, if used properly. They are based off of cutting edge cryptographic research and have yet to be broken or show any way of being broken.

Achieving true randomness is essential to incorporating the security of one-time pad level encryption. Emerging solutions of interest to the digital asset investor will focus on creating practical applications for the one-time pad as the next generation of cryptography.