Overview of Cryptography and Cryptocurrency

Telkom University

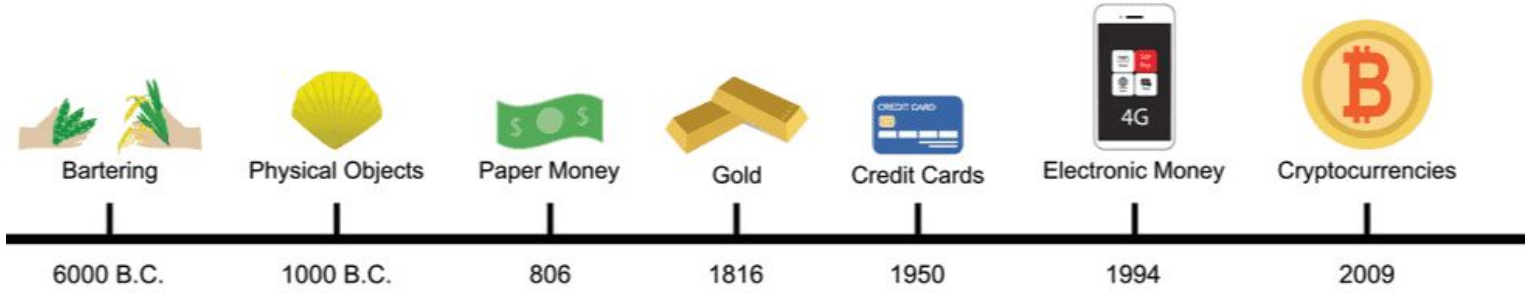
Main Questions as a Student

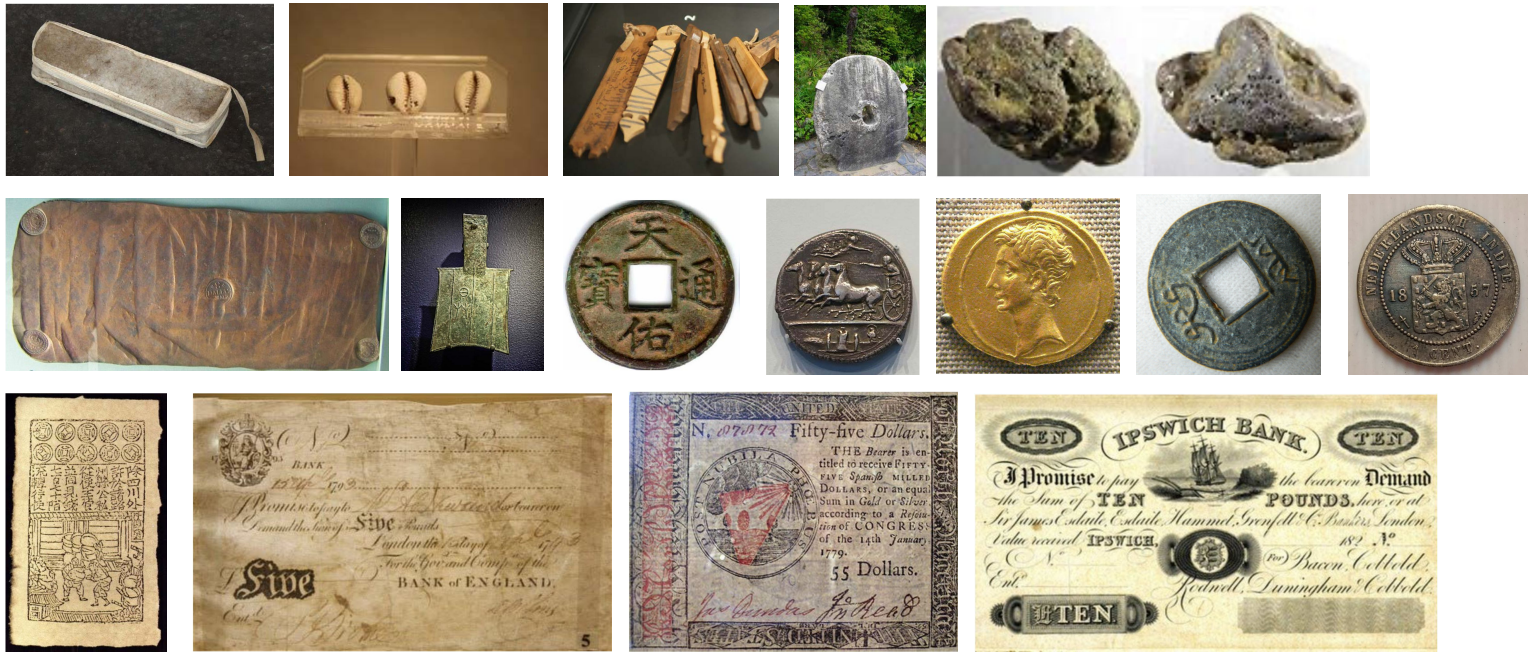
- **What** is Bitcoin and Blockchain? Why it may be a catalyst for big change in financial sector?
- **Why** so many people talk about Bitcoin and Blockchain, but no one really understand how it works?
- **How** Bitcoin and Blockchain works and who initiated those technologies?
- **How** to learn Bitcoin and Blockchain technologies?
- **What** I can learn out of this course? Your motivations and questions will define the results!

History of Money

- The Role of Money
  - Measure of Value
  - Medium of Exchange
  - Unit of Account
- The History
  - Bartering
  - Cash vs Credit
  - Electronic
  - Cryptocurrency

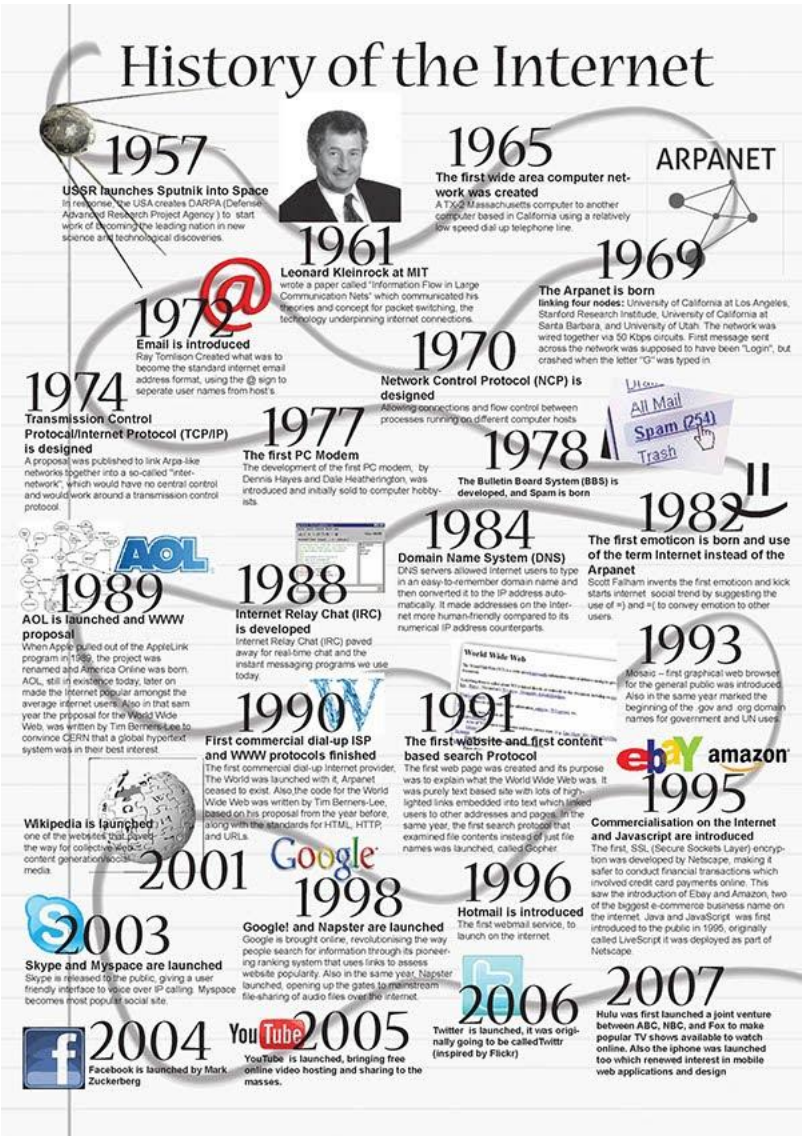
Evolution of Money





History of Internet

- The Internet
  - Ethernet
  - TCP/IP Protocol
  - HTTP and HTML
  - SSL / TLS
- Payment in Internet
  - How to Transfer $
  - Cash vs Credit
  - Avoid Cheating?



SSL / TLS – 1996

HTTP- 1990

TCP/IP - 1974

Ethernet - 1974

PayPal 1998

amazon 1994

CISCO 1984

3COM 1979

The Bank Ledger

Current Structures

- Central Bank
- Commercial Bank
- Financial Users

Recording of Accounts

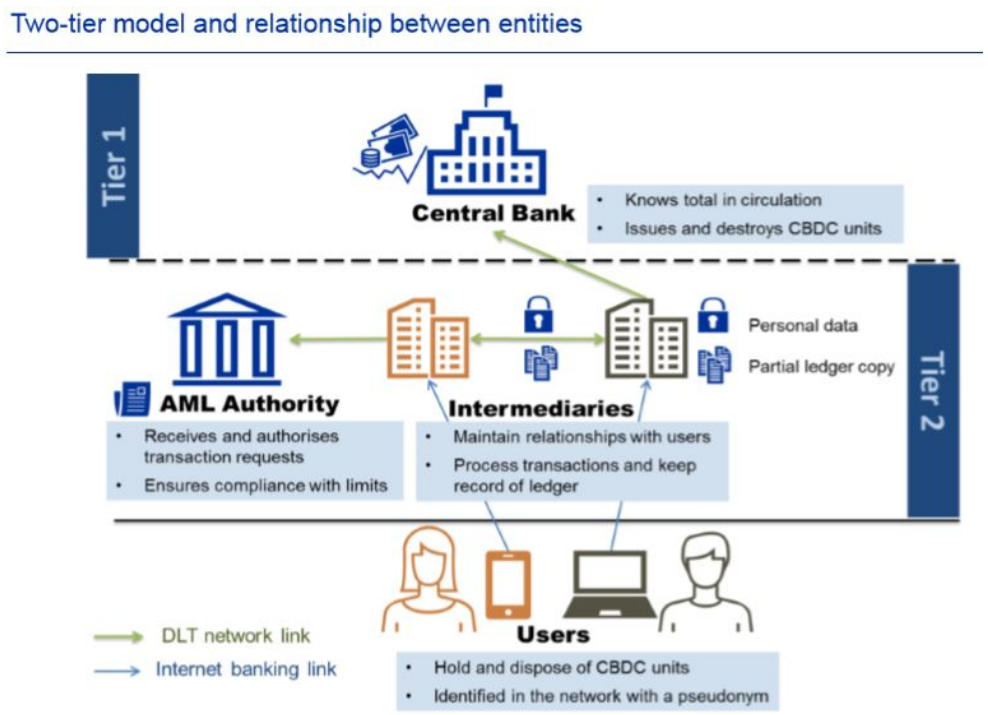
- Economic Activities
- Financial Relationships

Types of Ledgers

- Transactions vs Balance
- General vs Supporting or Sub
- Single Entry vs Double Entry

Characteristic of Good Leaders

- Immutable and Consistency
- Timestamped
- Ownership
- Accuracy and Comprehensive
- Description of Transaction



Ledgers – Early Money

Image by Sandstein on Wikimedia. License: CC-BY

Tally Sticks - England

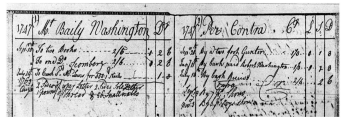
Image by Fusuke Kawasumi on Wikimedia. License: CC-BY

Rai Stones - Yap

Ledgers

Principal Recordings of Accounts

Proto Cuneiform
Uruk, ca 3000 B.C



Personal Ledger
George Washington
1747

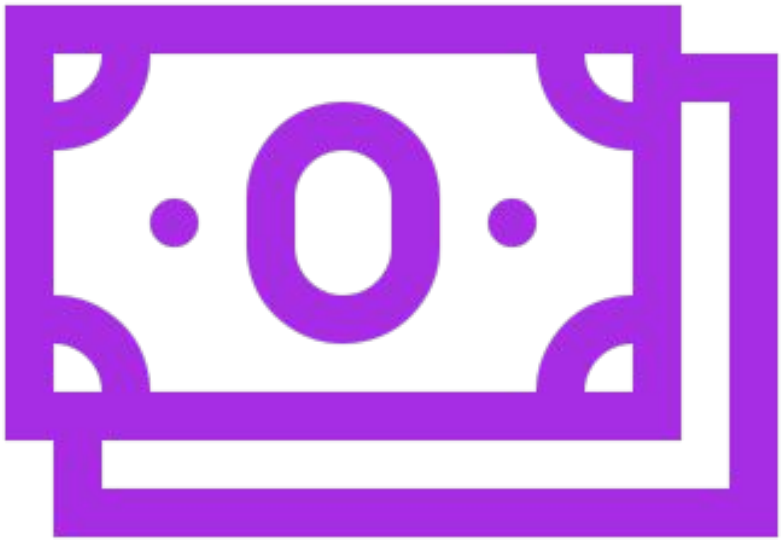
Private Bank Notes

Australia

United States

Canada

England



The Design of Cash Money

1. Durable
2. Portable
3. Divisible
4. Uniform/Fungible
5. Acceptable
6. Stable - Limited supply - Hard to Counterfeit
7. Token vs. Account Based
8. Physical vs. Digital
9. Private Sector vs. Central Bank
10. Widely Accessible vs. Wholesale

Credit Card

- A **credit card** is a payment card issued to users [cardholders] to enable the cardholder to pay a merchant for goods and services based on the cardholder's accrued debt [i.e., promise to the card issuer to pay them for the amounts plus the other agreed charges]. The card issuer [usually a bank or credit union] creates a revolving account and grants a line of credit to the cardholder, from which the cardholder can **borrow money for payment** to a merchant or as a cash advance.

Deposits & Negotiable Orders

Credit Cards

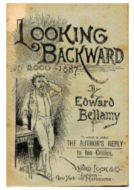


Image is in the public domain.

Term 'Credit Card'
Edward Bellamy's
Science Fiction
'Looking Backward'
1887

Charge Plates &
Credit Coins
Late 1880s – 1960s

Merchant Credit Cards
Late 1920s – 2000s

First Bank Card
Charge-It
First National Bank
Brooklyn, 1946

© Bloomingdales, First Bank, Ft. Worth General Tire Company, and Hotel La Salle. All rights reserved. This content is excluded from our Creative Commons license. For more information, see https://ocw.mit.edu/help/faq-fair-use/

Credit Card Processing

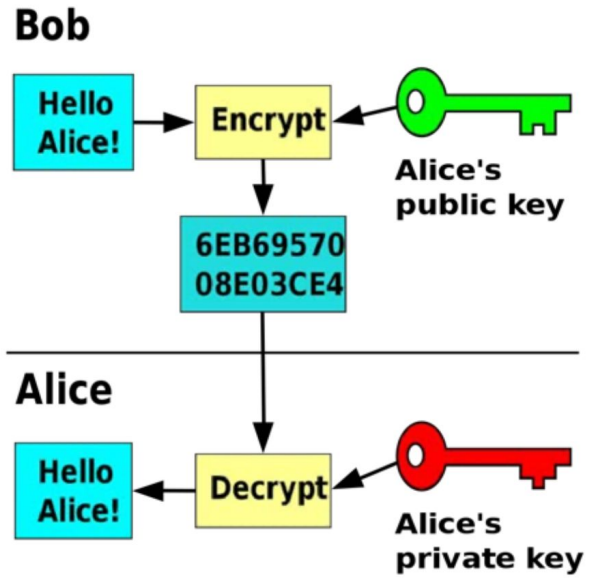
Slide Card Imprinter
1950s

Visa Imprinter
1979

Payment Terminal
2018

Scytale Cipher
Ancient Times

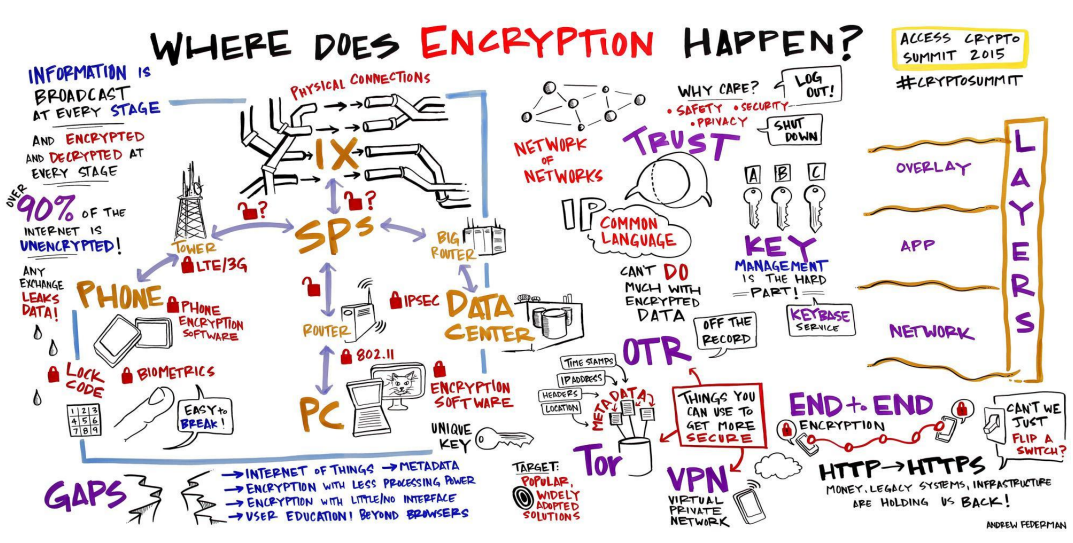
Enigma Machine 1920s - WWII



Asymmetric Cryptography
1976 to today

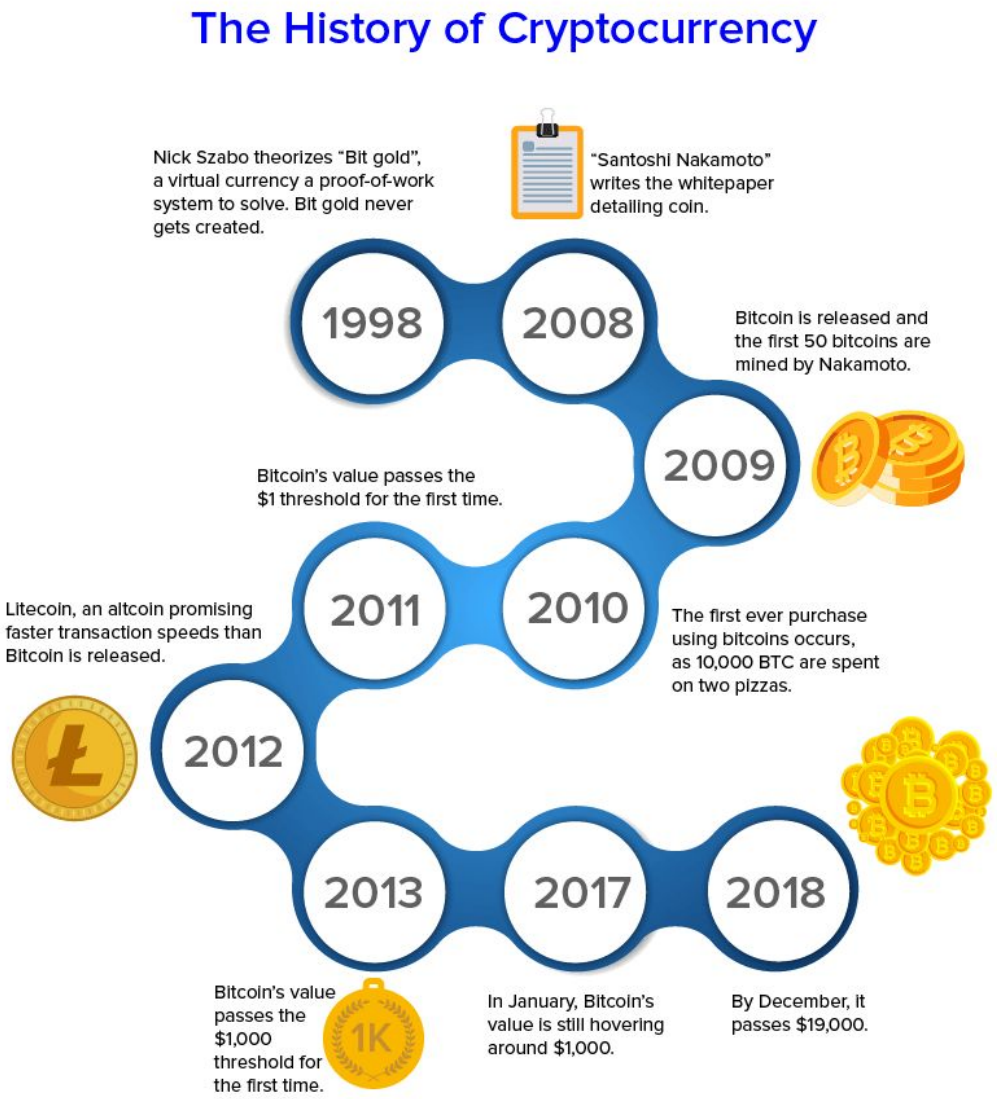
HISTORY OF CRYPTOGRAPHY

Communication in the presence of adversarial.



HISTORY OF CRYPTOGRAPHY

Communication in the presence of adversarial.



ELECTRONIC PAYMENT

PayPal	ERICSSON telenor	支付宝 ALIPAY	M-PESA Safaricom
1998	1999	2003	2007
Mobile App	Google Wallet	微信支付 WeChat Pay	Pay
2011	2011	2013	2014

Why They Have Failed?

- Merchant Adoption and Centralization,
- Double Spending and Consensus

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Satoshi Nakamoto

He focused to solve "double spending problem" in e-Payment by proposing "Chain of Hash" as proof or work and digital signature solution. It is cryptographic proof without "third parties" that is implemented as P2P distributed timestamp server with additional features like incentive, reclaim disk space, payment verification, combining / splitting value and privacy protection. All are implemented using well known algorithms in Cryptography and Distributed System.

"I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party." Satoshi.

How to use Bitcoin

1. **Inform yourself**

Bitcoin is different than what you know and use every day. Before you start using Bitcoin, there are a few things that you need to know in order to use it securely and avoid common pitfalls.

Read more

2. **Choose your wallet**

Free bitcoin wallets are available for all major operating systems and devices to serve a variety of your needs. For example, you can install an app on your mobile device for everyday use or you can have a wallet only for online payments on your computer. In any case, choosing a wallet is easy and can be done in minutes.

Choose your wallet

3. **Get Bitcoin**

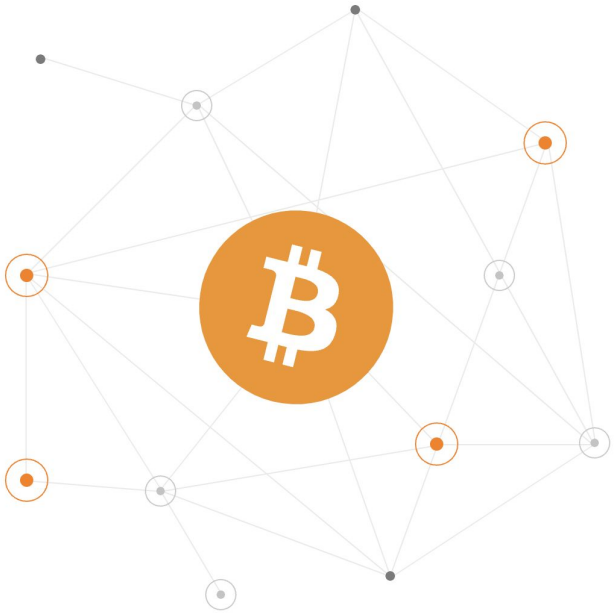
You can get Bitcoin by accepting it as a payment for goods and services. There are also several ways you can buy Bitcoin.

Buy Bitcoin

4. **Spend Bitcoin**

There are a growing number of services and merchants accepting Bitcoin all over the world. Use Bitcoin to pay them and rate your experience to help them gain more visibility.

Find merchants and products



How to accept Bitcoin

1. **Inform yourself**

Bitcoin does not require merchants to change their habits. However, Bitcoin is different than what you know and use every day. Before you start using Bitcoin, there are a few things that you need to know in order to use it securely and avoid common pitfalls.

Read more

2. **Processing payments**

You can process payments and invoices by yourself or you can use merchant services and deposit money in your local currency or bitcoins. Most point of sales businesses use a tablet or a mobile phone to let customers pay with their mobile phones.

Find merchant services

3. **Accounting and taxes**

Merchants often deposit and display prices in their local currency. In other cases, Bitcoin works similarly to a foreign currency. To get appropriate guidance regarding tax compliance for your own jurisdiction, you should contact a qualified accountant.

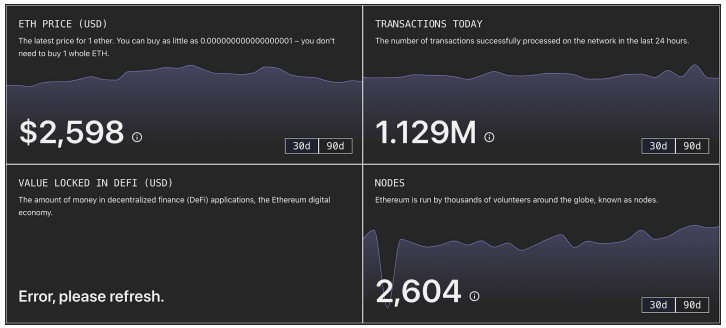
Read more

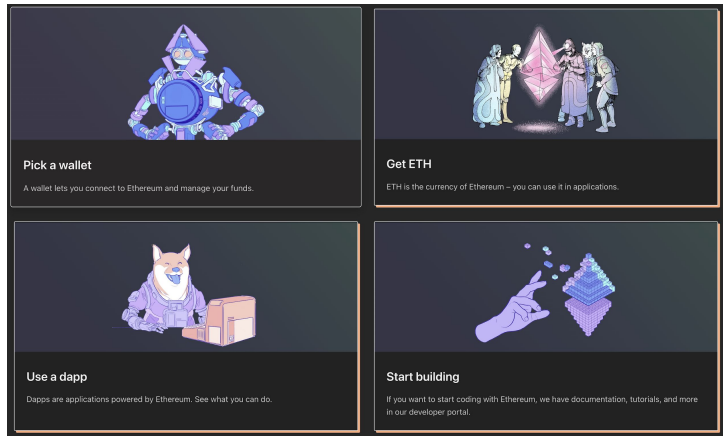
4. **Gaining visibility**

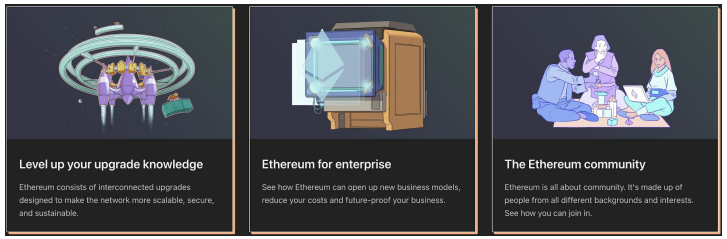
There is a growing number of users searching for ways to spend their bitcoins. You can submit your business in online directories to help them easily find you. You can also display the Bitcoin logo on your website or your brick and mortar business.

Overview of Bitcoin

- Bitcoin is largest Blockhain tthat innovates WW payment network and a new kind of money.
- Bitcoin uses P2P transaction technology to operate with no central authority or banks;
- Managing transactions and the issuing of bitcoins is carried out collectively by the network.
- Nobody owns or controls Bitcoin, everyone can take park and offers low processing fees.







Next Talk: Hash Function, SHA, Hash Pointer and Merkle Tree

Overview of Ethereum

- Ethereum is OSS powering the cryptocurrency ether (ETH) and thousands of DApps. To make digital money, global payments, and applications. The Ethereum community has built a booming digital economy, bold new ways for creators to earn online, and so much more. It's open to everyone, wherever you are in the world – all you need is the internet. Future Ethereum is:
  - The Internet of Digital Assets (NFT - Non Fungible Token)
  - A Fairer Financial System (DeFi – Decentralized Finance)
  - An Open Internet (eWallet – Secure, Free and Easy Wallet on Internet)
  - A New Frontier of Development (DApps – Distributed Apps)

W1 Home Works

Reading and Watching:

- Read Satoshi Nakamoto Paper and Summarize
- Getting Started with Bitcoin [www.bitcoin.org]
- Getting Started with Ethereum [www.ethereum.org]
- Find Your Favorite Youtube Videos that Explains Bitcoin and Ethereum

Code Hacking:

- Ethereum uses the **Keccak-256** cryptographic hash function in many places.
- Learn ETH-Hash Implementation: https://github.com/ethereum/eth-hash
- Ethereum uses Merkle Tree for Offline Data Integrity:
  - https://blog.ethereum.org/2015/11/15/merkling-in-ethereum/
  - https://ethereum.org/en/developers/tutorials/merkle-proofs-for-offline-data-integrity/
- Make Simple Codes That Uses ETH-Hash and Put in Your Git