Bitcoin : Dijital Para Birimi

Para Hakkında Tüm Bildiklerinizi Unutun !

Mert KILIÇ

Gündem

- Bitcoin Nedir ? Ne Değildir ?
- Kısa Tarihçe
- Nasıl Çalışır ?
- Nasıl Kullanılır ?
- Sanal Para Birimlerinin Artıları ve Eksileri
  - Günümüzde
  - Gelecekte
- Sonuç

Bitcoin Nedir ?

- Bitcoin (sembolü: ฿, kısaltma: BTC) herhangi bir merkez bankası, resmi kuruluş, vs. ile ilişiği olmayan elektronik bir para birimidir. Bitcoin ağı 3 Ocak 2009'da hayata geçti. Maksimum bitcoin sayısı 21 milyonla sınırlıdır.

Bitcoin Ne Değildir ?

- Kesinlikle bir Fiat Para birimi değildir !
- Altın veya Herhangi bir karşılığı bulunmamaktadır.
- Banka veya Kurumlara ihtiyaç duyduğunuz bir araç değildir !
- Sınırları veya Sahibi yoktur.
- Vergilendirilebilen ve Kayıt altında tutulabilen bir para birimi değildir.

Geçmiş

Bitcoin 2008 yılında, Satoshi Nakamoto tarafından yazılan manifesto ile duyurulan, 2009 yılının başında da işlevsel hale gelen, ilk sanal para birimi ve protokolün ismidir. Bitcoin'in yaratıcısı Satoshi Nakamoto'nun kimliği ile ilgili pek bilgi bulunmamakla birlikte, sistemi tasarlayan kişi ya da kişilerin kullandığı takma bir isim olduğu tahmin edilmektedir.

Geçmiş

Bitcoin, ilk yılın sonuna kadar maddi anlamda değer kazanamazken, Mayıs 2010 gibi 1 bitcoin 0.01 dolar civarinda bir değere erişmişti. 2010 Yılı başında 13 dolar değerinde olan bitcoin, şuan itibariyle 500 Dolar civarında satılmaktadır. (www.sanalmangir.com)

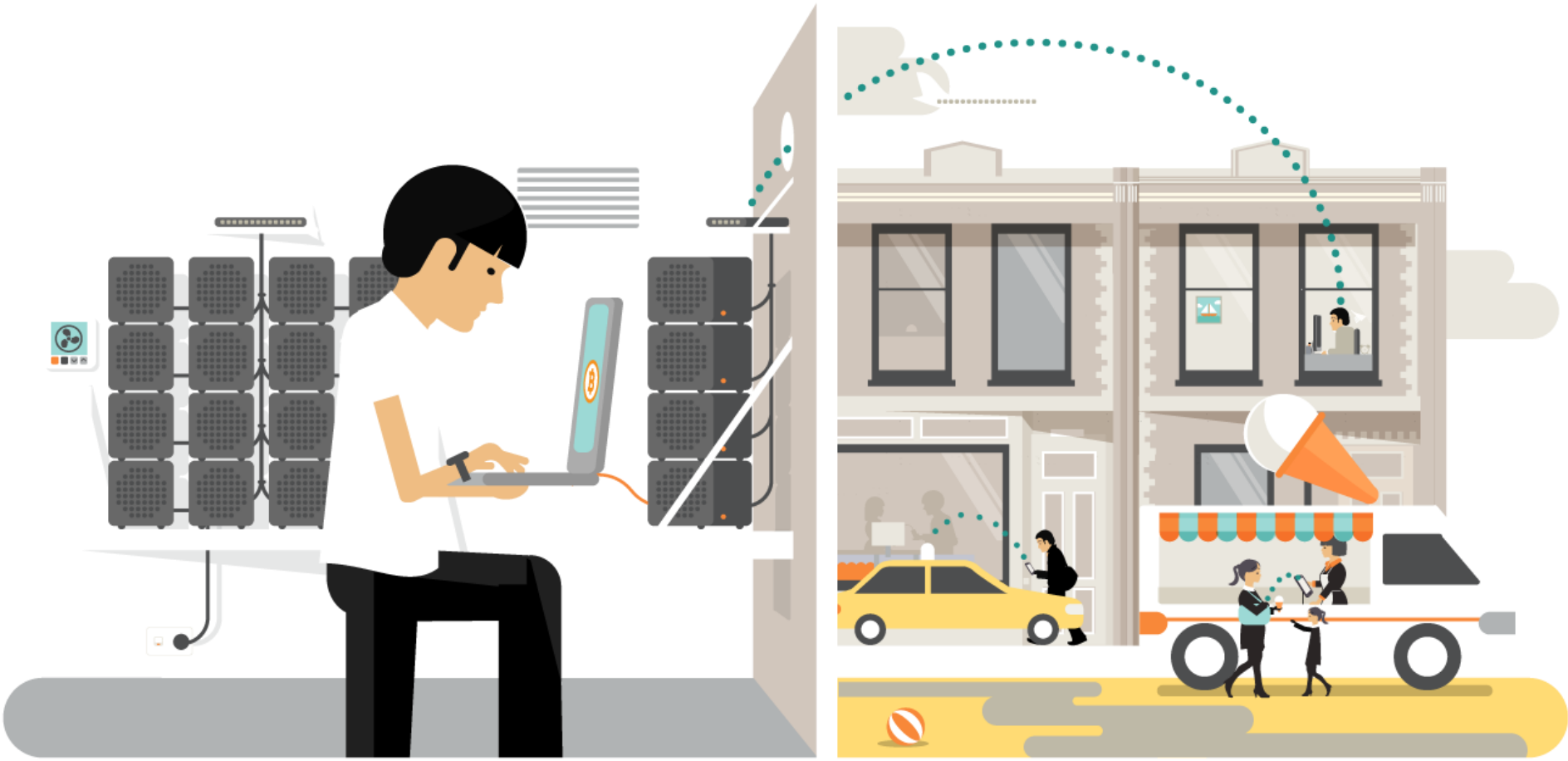
Nelere İhtiyacımız Var ?

Cüzdan mı ?

Domuz Kasa mı ?

Tanımadığımız sayısız insan mı ?

Nasıl Çalışıyor ?



Bilmece Bildirmece El Üstünde Kaydırmaca

How a ₿itcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEP kjEPeCh 43BeKJL1yb LCWrfDpN.

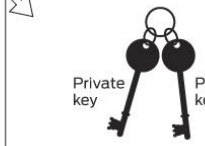
CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

Each address has its own balance of bitcoins.

SUBMITTING A PAYMENT

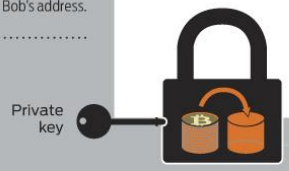
Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



Public Key Cryptography 101

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.



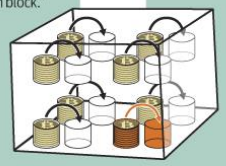
Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

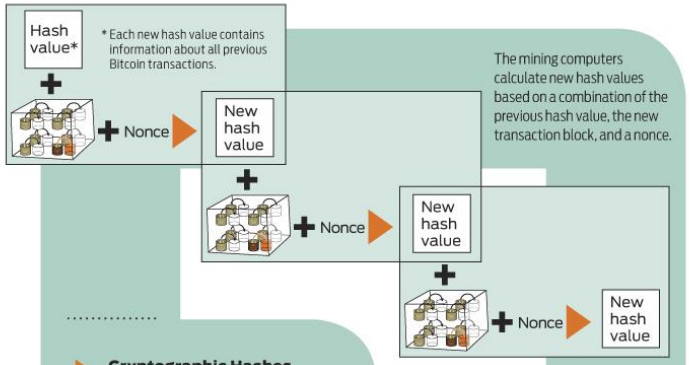
VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."



The miners' computers are set up to calculate cryptographic hash functions.



The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

Cryptographic Hashes

Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

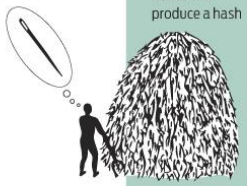
The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all evil	486c 6be4 6dde...
The root of all veil	b8db 7ee9 8392...

Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

The root of all evil???	0000 0000 0000 ...

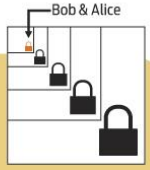
Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.



The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TRANSACTION VERIFIED

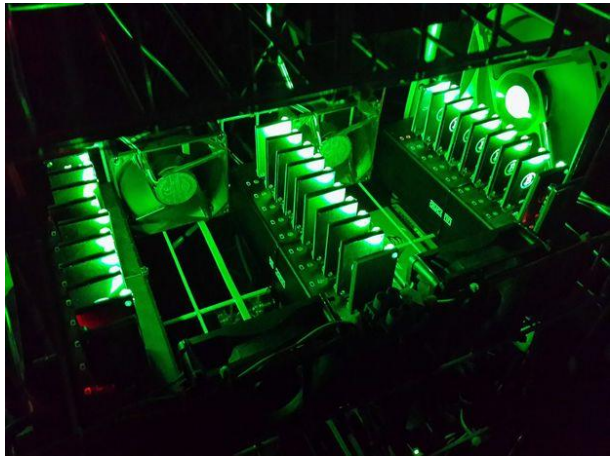


As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

JOSHUA J. ROMERO, BRANDON PALACIO & KARL SSOWWALKER INC.

Uygulamaya Yönelik Entegre Devreler (ASIC)

Uygulamaya Yönelik Entegre Devreler (ASIC)



http://www.instructables.com/id/Build-your-Own-Portable-Bitcoin-Mining-Rig-Battles/

Bitcoin Nasıl Gerçek Paraya Çevirilir ?

Nerelerde Kullanılır ?

- Gıda
- Giyim
- Spor Malzemeleri
- Tüm Teknolojik Ürünler
- Hemen hemen tüm hizmet sektörü...

bitpay.com

Bitcoin’in Büyük Patlaması (Big Bang Theory)

Pizza Teslimatına Ödül 10.000 BTC

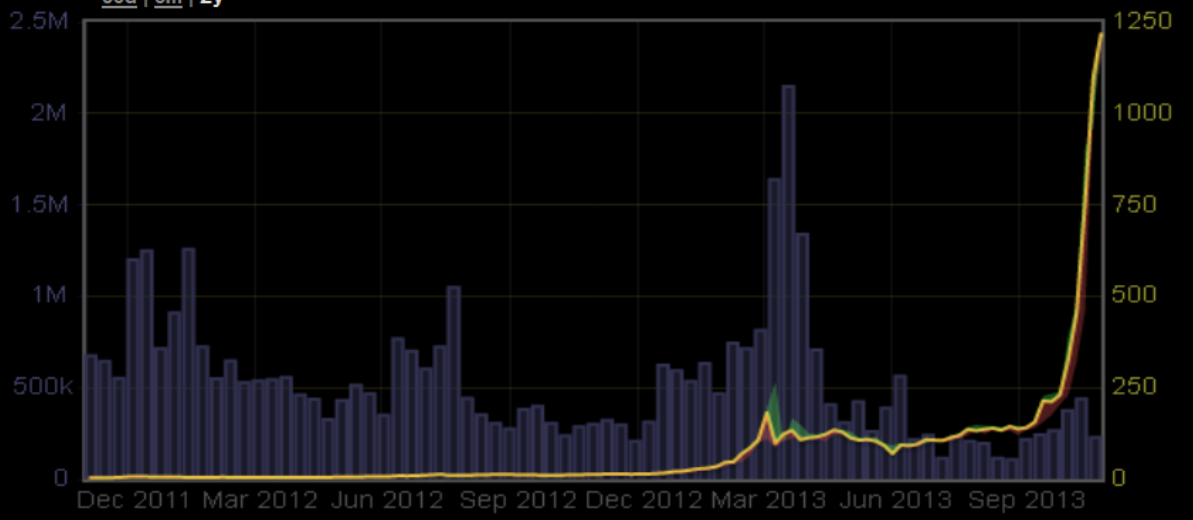
Bitcoin Fiyat Değişimi

bitcoinity.org/markets
Sponsored by Digital Currency Research

USD CNY EUR PLN JPY CAD GBP more
mtgox bitstamp btce bitfinex localbitcoins

Last change: **0.40** seconds ago
light version | WTF? | preferences

10m | 1h | 3h | 12h | 24h | 3d | 7d | 30d | 6m | 2y | change: +40647.11% high: 1219.97 low: 2.50



showing change bars for last: 1m | 5m | 10m | 30m | 1h

ALL TIME HIGH

1219.97

USD / BTC

bid: 1215.00 ask: 1215.19

mtgox	0.33	a few seconds ago	1219.97
mtgox	0.26	a few seconds ago	1216.00
mtgox	2.28	a few seconds ago	1219.97
mtgox	0.42	a few seconds ago	1219.74
mtgox	0.04	a few seconds ago	1219.51
mtgox	0.10	a few seconds ago	1219.50
mtgox	0.10	a few seconds ago	1219.39
mtgox	1.07	a few seconds ago	1219.00
mtgox	0.99	a few seconds ago	1216.98
mtgox	2.01	a few seconds ago	1219.00
mtgox	0.01	a few seconds ago	1218.69
mtgox	0.04	a few seconds ago	1218.53

Bitcoin Fiyat Değişimi

BLOCKCHAIN Home Charts Stats Markets API Wallet Search

Market Capitalization
Source: blockchain.info

Market Cap (USD)

16,000,000,000
14,000,000,000
12,000,000,000
10,000,000,000
8,000,000,000
6,000,000,000
4,000,000,000
2,000,000,000
0

Jan '09 May '09 Sep '09 Jan '10 May '10 Sep '10 Jan '11 May '11 Sep '11 Jan '12 May '12 Sep '12 Jan '13 May '13 Sep '13 Jan '14 May '14

30 Days - 60 Days - 180 Days - 1 Year - 2 Year - All Time

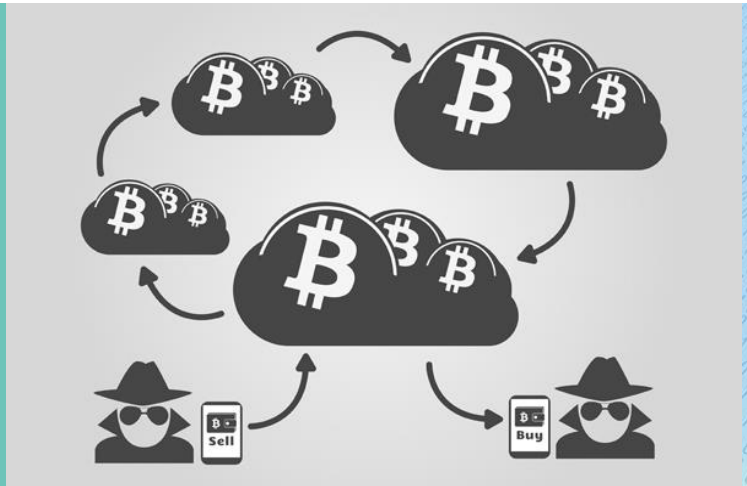
Logarithmic Scale - 7 day average - Show data points - (CSV - JSON)

Şuan ki USD Karşılığı

Total BTC	**12,641,500 BTC**
Market Capbased on latest prices	**5,160,133,885 USD** **or 3,729,242,500 EUR** **or 15,397,347,000 PLN** **or 3,337,356,000 GBP**
Transactionslast 24h	**48,850**
Transactions avg. per hour	**2035.42**
Bitcoins sentlast 24h	**373,655.54 BTC**
Bitcoins sentavg. per hour	**15,568.98 BTC**

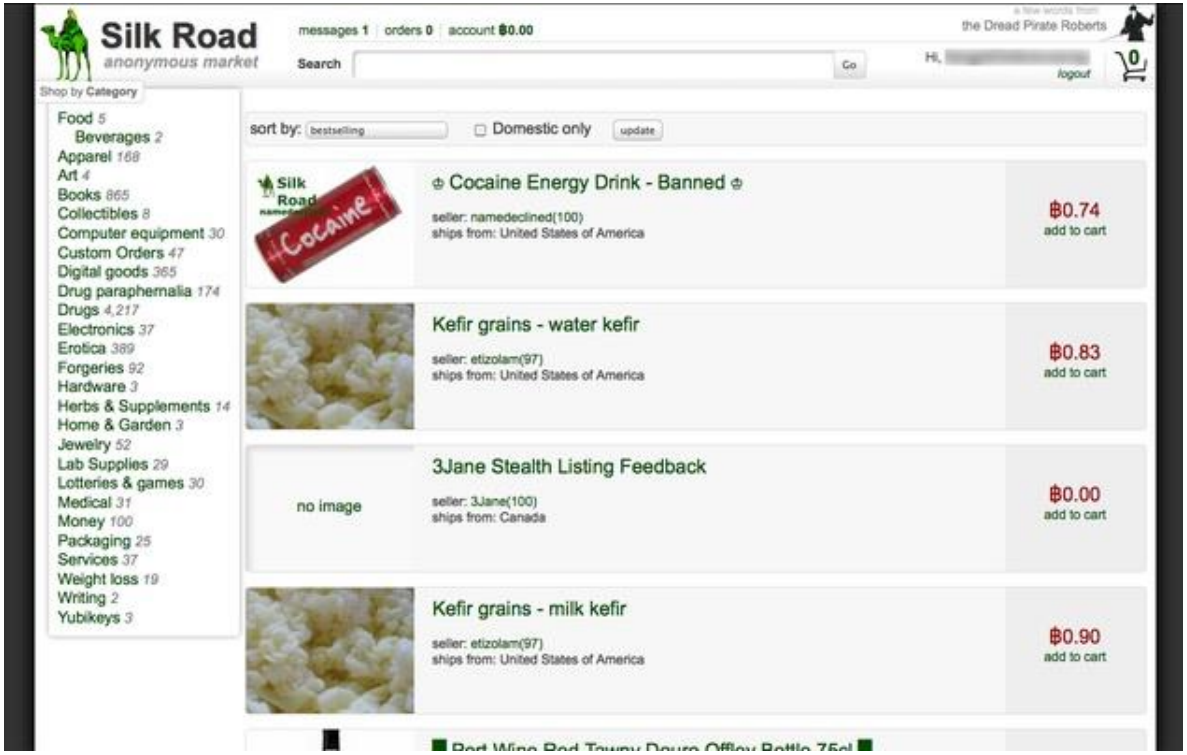
Peki Kime Güveneceğiz ?

Matematiğe !



Eğer Saklayacak Birşey Yoksa;
Bu Kadar Anonimlik Niye ?

İpek Yoluna Kaçacak değiliz.



Sabrınız ve İlginiz için Teşekkür Ederim