

Thoughts on bitcoin mining, transacting and blockchain services

Presenter: Nikola Tchouparov



Date: April 2014

Contents

2

- **Presenter introduction**
- **Mining**
- **Transacting**
- **Blockchain services**
- **Accounting concepts**

- Nikola Tchouparov
 - from Bulgaria
- Independent IT Consultant
- Specialize on Front Office Trading Systems (Murex)
- Implementation projects (greenfield, upgrade, patching, customizing, support)
- 8+ years experience in 10 countries (Europe, Asia, Africa, North America) and a dozen organizations
- Validating pricing and valuation models, P&L reconciliation, developing risk reports, setting-up accounting engine, business analysis, etc.
- Currently working at SBSA on IRD book migration and CRD book migration

- **Blockchain enthusiast**
 - Transacting in bitcoin/crypto
 - Trading bitcoin/crypto (lost funds in Mt. Gox fiasco)
 - Mining crypto (bitcoin, litecoin, solarcoin, unobtanium, ethereum testnet)
 - Learning about bitcoin/crypto
 - Want to build services using the blockchain technology

What is Murex?

4

esmxasia02 (UAT) MX [PID:691814 NPID:14764 SID:4987...UREXBO> Simulation : Portfolio simulation by trade

File Edit View Tools Data Settings Screen Navigation Help UI Tools

IRJBSBSAMERRIL Connect to realtime Calculation On Trade capture On 22 Jan 2014 22

Fx Rates Securities Credit Main

Real time X

GAMMA IRD PV01 IR Options IRD Vega Bonds FX Delta Open positions FX Futures

Portfolio	Cur	Group	Daily PL<USD>	MTD PL<USD>	YTD PL<USD>
IRJBSBSAMERRIL	Total IRJBSBSAMERRIL		3,528	-28,095,093	-28,095,093
	EUR	SCF	0	36,316	36,316
	USD	SCF	0	6,562	6,562
	ZAR	FXD	-0	-374	-374
		IRS	3,528	-28,244,896	-28,244,896
		SCF	0	107,300	107,300
	Total ZAR		3,528	-28,137,970	-28,137,970



For more info:
www.murex.com

Order Management System for derivatives trading:

- Pricing
- Structuring
- Risk Management
- PLA, IPV, Provisioning
- Processing/validation
- Settlement

Simulation / Portfolio simulation

Display setting LDN_PLVAR_1yt Currency USD

Calendar NO_HOLIDAY Additional Outputs View

Family 1	Family 2	Step Name	Description
Theta analysis	Initial State	Initial state	Initial state
	Time Decay	Time	Pure time decay
PL variance	Market data variation	Yield curves	Yield curves
		Basis curves	Basis curves
		Inflation curves	Inflation curves
		Bond/Fut prices	Bond/Fut prices
		Bond/Fut spreads	Bond/Fut spreads
		Ir vols	Ir vols
	Trades	Ir smiles	Ir smiles
		Fx spots	Fx spots
		Fx vols	Fx vols
		Fx smiles	Fx smiles
		Option prices	Option prices
		Fixings	Fixings

How to Mine bitcoin

5

- Open source mining software is freely available on the Internet
- CGMiner, BFGMiner, Ufasoft miner, etc.

- CPU mining – unprofitable; interesting for learning
- GPU mining – unprofitable for bitcoin; possibly profitable for other crypto; interesting for learning (setup Linux, install miner software, set GPU setting etc,)
- FPGA mining – I never did this, so don't know
- ASIC mining – profitable; mostly plug&play; ASIC's are difficult to obtain and expensive

- Solo mining vs pooled mining
 - Solo mining bitcoin – huge upfront investment. Interesting for ASCL manufacturers, hedge funds
 - Pooled mining bitcoin – pool collects a fee, but also smoothes earnings
 - For “stupid-coins” less investment required

Mining calculations

6

- 3600 bitcoins mined per day:
 - 25 BTC per block
 - x 10 mins expected time per block
 - x 6 periods/blocks per hour
 - x 24 hours per day

- Current bitcoin network mining power circa 28 peta-hash = 28,000 terra-hash
- Assuming pooled-mining, expected values:
 - 7.7 terra-hash to mine 1 bitcoin per day

OR

 - 1 terra-hash to mine 1 bitcoin in 7.7 days

- Assuming solo-mining:
 - 194 terra-hash to get one block per day (25BTC + fees)
 - Estimated 2 million USD investment plus working capital and overheads
 - High risk due to advances in ASIC technology and bitcoin price volatility

- Calculation differs for other crypto

CPU mining

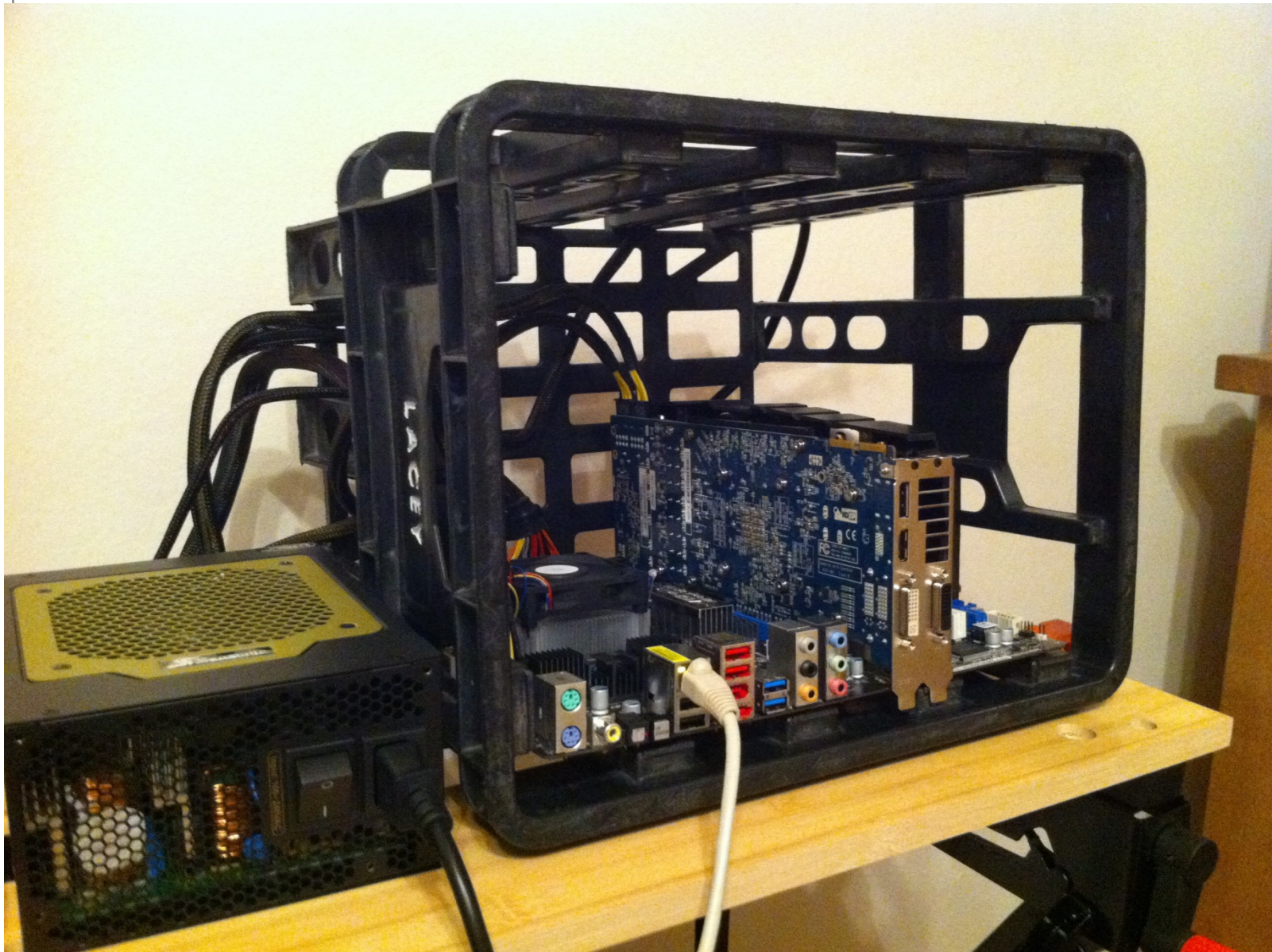
7

- Don't bother
- Might become feasible again in the future with new ASIC-resistant mining algorithms
 - e.g. Ethereum's Dagger and Slasher
 - Solarcoin's photovoltaic panels
 - Other new things (NXT?)



GPU mining

8



Nikola Tchouparov, April 2014, Sofia & London

GPU mining

9

■ Technical specs

■ Your Order

Invoice E2044693
Date 01/05/2013 17:02

Product	Quantity	Price

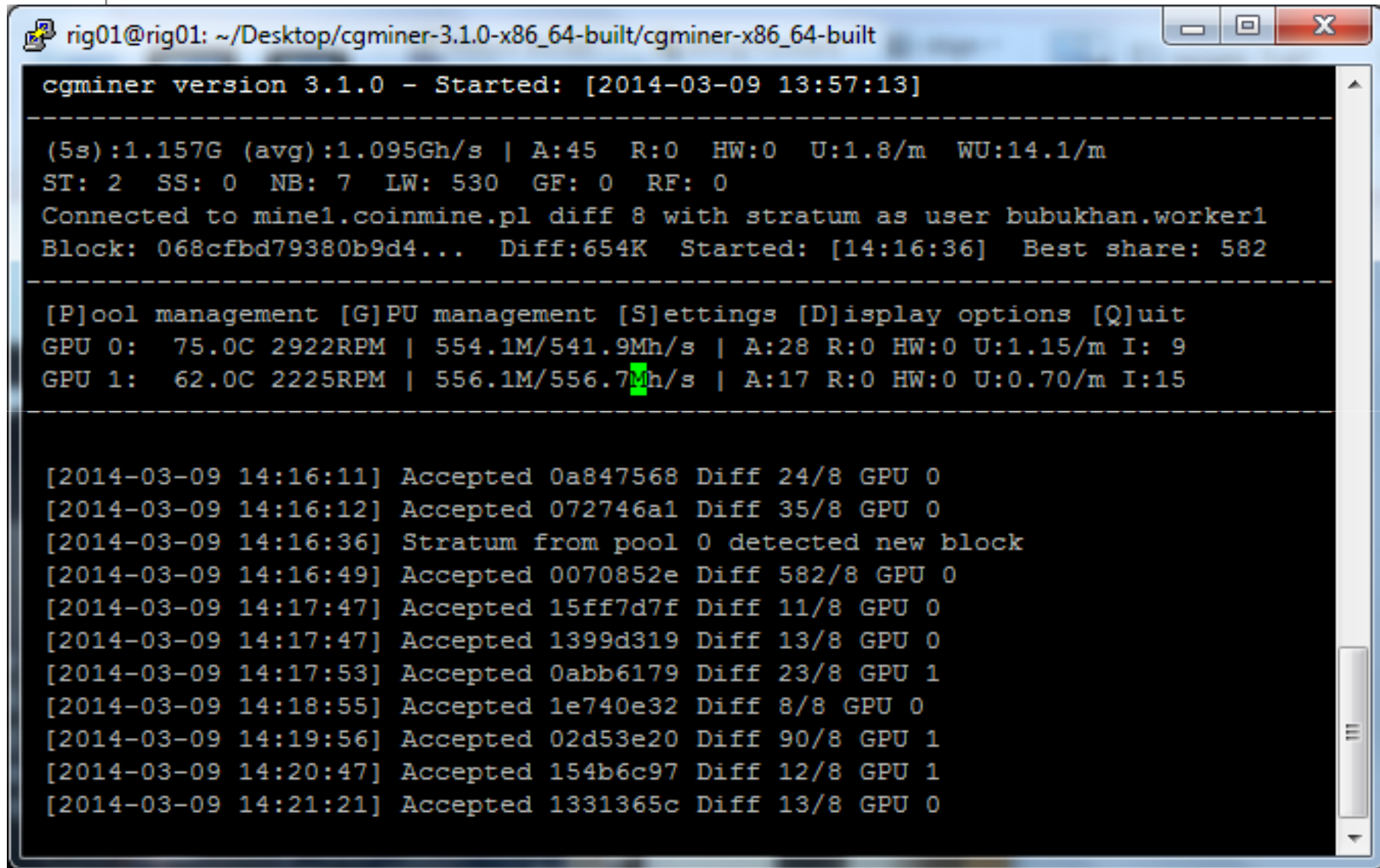
500GB Western Digital WD5000BPVT Sc	1	£34.89
1250W Seasonic X-Series SS-1250XM,	1	£182.12
ASRock 970 Extreme4, AMD 970, S AM3	1	£62.97
4GB Corsair DDR3 XMS3, PC3-10666 (1	1	£22.40
3GB Sapphire Radeon HD 7970 Dual-X,	2	£272.79

	Net Total	£857.95
	Carriage	£9.99
	Tota	£1,029.54



GPU mining

11



```
rig01@rig01: ~/Desktop/cgminer-3.1.0-x86_64-built/cgminer-x86_64-built

cgminer version 3.1.0 - Started: [2014-03-09 13:57:13]

-----
(5s):1.157G (avg):1.095Gh/s | A:45  R:0  HW:0  U:1.8/m  WU:14.1/m
ST: 2  SS: 0  NB: 7  LW: 530  GF: 0  RF: 0
Connected to mine1.coinmine.pl diff 8 with stratum as user bubukhan.worker1
Block: 068cfbd79380b9d4... Diff:654K  Started: [14:16:36]  Best share: 582
-----

[P]ool management [G]PU management [S]ettings [D]isplay options [Q]uit
GPU 0:  75.0C 2922RPM | 554.1M/541.9Mh/s | A:28 R:0 HW:0 U:1.15/m I: 9
GPU 1:  62.0C 2225RPM | 556.1M/556.7Mh/s | A:17 R:0 HW:0 U:0.70/m I:15
-----

[2014-03-09 14:16:11] Accepted 0a847568 Diff 24/8 GPU 0
[2014-03-09 14:16:12] Accepted 072746a1 Diff 35/8 GPU 0
[2014-03-09 14:16:36] Stratum from pool 0 detected new block
[2014-03-09 14:16:49] Accepted 0070852e Diff 582/8 GPU 0
[2014-03-09 14:17:47] Accepted 15ff7d7f Diff 11/8 GPU 0
[2014-03-09 14:17:47] Accepted 1399d319 Diff 13/8 GPU 0
[2014-03-09 14:17:53] Accepted 0abb6179 Diff 23/8 GPU 1
[2014-03-09 14:18:55] Accepted 1e740e32 Diff 8/8 GPU 0
[2014-03-09 14:19:56] Accepted 02d53e20 Diff 90/8 GPU 1
[2014-03-09 14:20:47] Accepted 154b6c97 Diff 12/8 GPU 1
[2014-03-09 14:21:21] Accepted 1331365c Diff 13/8 GPU 0
```


ASIC mining – KnC Miner Jupiter

12



ASIC mining – KnC Miner Jupiter

13



Login	Password	Found blocks	Current shares	Score	Last share at	Mhash/s*
████████.worker1	████████	1	4645565	481752.5537	0 minutes	543133.432
████████.worker2	████████	0	3875740	386921.8342	0 minutes	453129.806

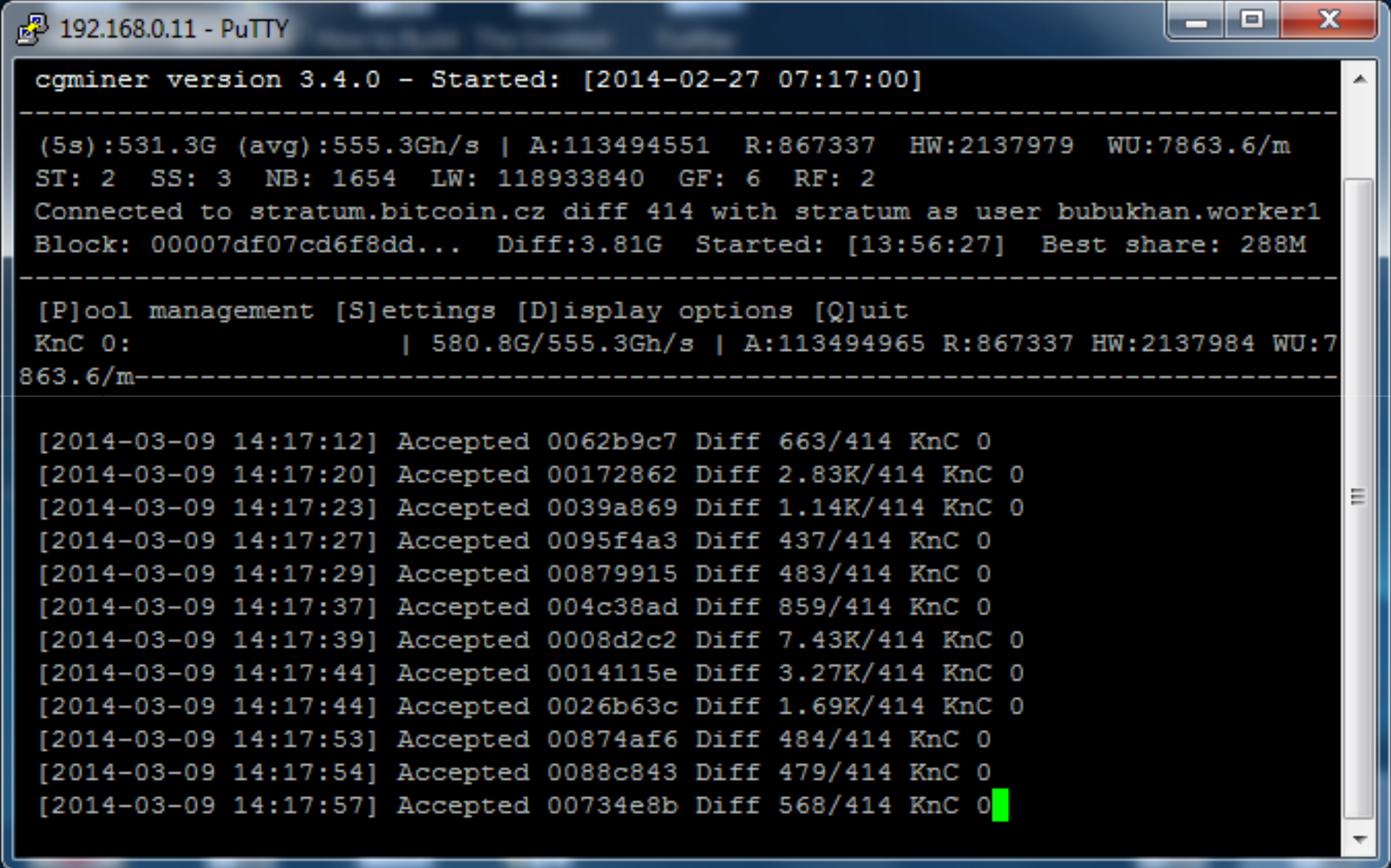
* The calculation is based on the number of shares so far, which may not be accurate for slow workers.

Found blocks

[271079](#)

ASIC mining – KnC Miner Jupiter

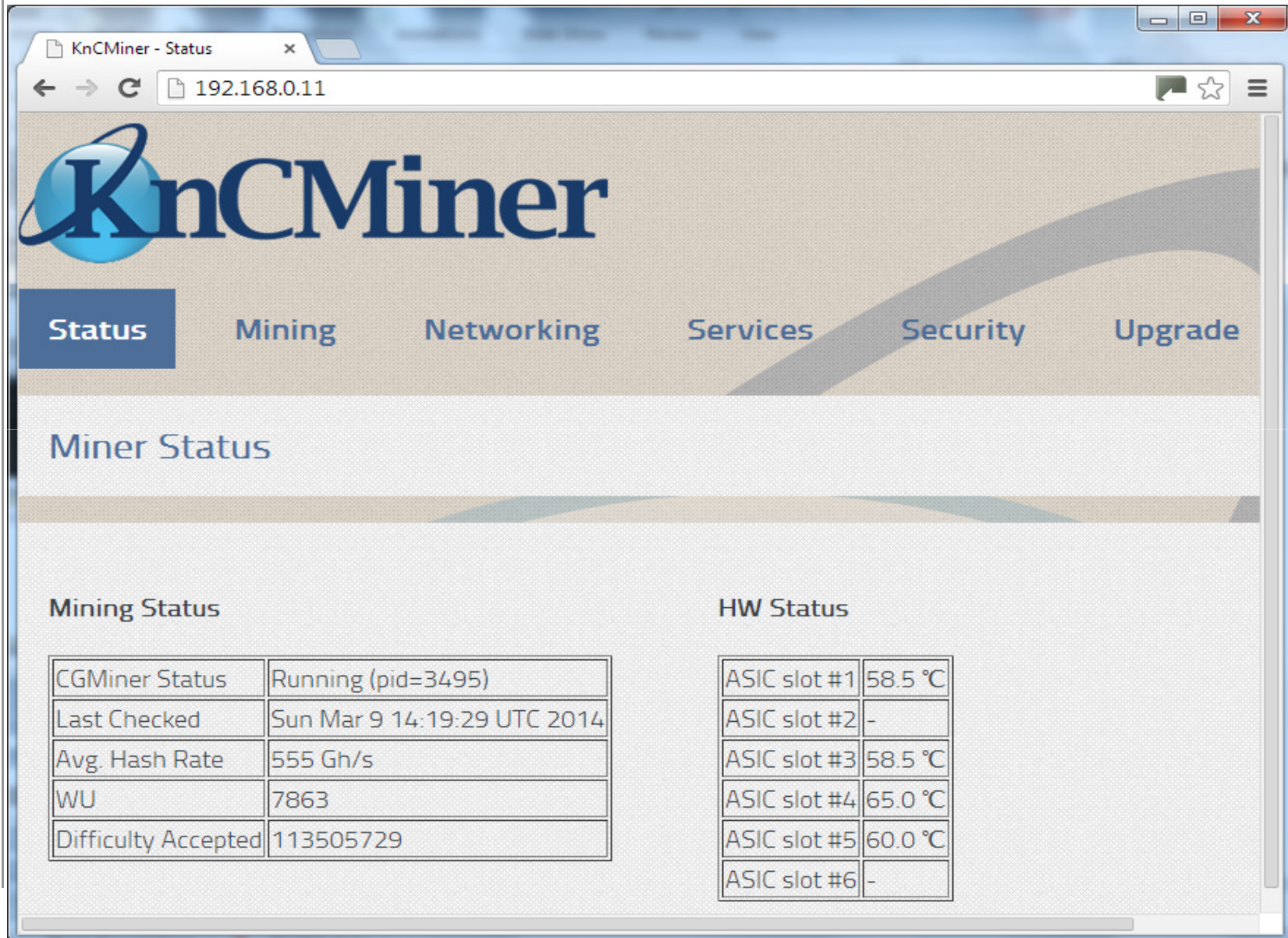
14



```
192.168.0.11 - PuTTY
cgminer version 3.4.0 - Started: [2014-02-27 07:17:00]
-----
(5s):531.3G (avg):555.3Gh/s | A:113494551 R:867337 HW:2137979 WU:7863.6/m
ST: 2 SS: 3 NB: 1654 LW: 118933840 GF: 6 RF: 2
Connected to stratum.bitcoin.cz diff 414 with stratum as user bubukhan.worker1
Block: 00007df07cd6f8dd... Diff:3.81G Started: [13:56:27] Best share: 288M
-----
[P]ool management [S]ettings [D]isplay options [Q]uit
KnC 0: | 580.8G/555.3Gh/s | A:113494965 R:867337 HW:2137984 WU:7
863.6/m-----
[2014-03-09 14:17:12] Accepted 0062b9c7 Diff 663/414 KnC 0
[2014-03-09 14:17:20] Accepted 00172862 Diff 2.83K/414 KnC 0
[2014-03-09 14:17:23] Accepted 0039a869 Diff 1.14K/414 KnC 0
[2014-03-09 14:17:27] Accepted 0095f4a3 Diff 437/414 KnC 0
[2014-03-09 14:17:29] Accepted 00879915 Diff 483/414 KnC 0
[2014-03-09 14:17:37] Accepted 004c38ad Diff 859/414 KnC 0
[2014-03-09 14:17:39] Accepted 0008d2c2 Diff 7.43K/414 KnC 0
[2014-03-09 14:17:44] Accepted 0014115e Diff 3.27K/414 KnC 0
[2014-03-09 14:17:44] Accepted 0026b63c Diff 1.69K/414 KnC 0
[2014-03-09 14:17:53] Accepted 00874af6 Diff 484/414 KnC 0
[2014-03-09 14:17:54] Accepted 0088c843 Diff 479/414 KnC 0
[2014-03-09 14:17:57] Accepted 00734e8b Diff 568/414 KnC 0
```


ASIC mining – KnC Miner Jupiter

15



The screenshot shows a web browser window titled "KnCMiner - Status" with the address bar displaying "192.168.0.11". The page features the KnCMiner logo and a navigation menu with tabs: Status, Mining, Networking, Services, Security, and Upgrade. The "Status" tab is selected, showing the "Miner Status" section. Below this, there are two tables: "Mining Status" and "HW Status".

Mining Status

CGMiner Status	Running (pid=3495)
Last Checked	Sun Mar 9 14:19:29 UTC 2014
Avg. Hash Rate	555 Gh/s
WU	7863
Difficulty Accepted	113505729

HW Status

ASIC slot #1	58.5 °C
ASIC slot #2	-
ASIC slot #3	58.5 °C
ASIC slot #4	65.0 °C
ASIC slot #5	60.0 °C
ASIC slot #6	-







- Natively transact via bitcoin addresses (string of alphanumeric characters)
 - Requires keyboard typing or copy-paste
- Encode the bitcoin address into a QR code (or any other barcode)
 - Requires scanner or camera (smart-phones and laptops)
- With add-on services transact via SMS (Coinapult) or some other Alias (Twitter, e-mail) – great technology for reaching the unbanked and P2P micropayments
 - **Business idea:** build an integration between WhatsApp (free international SMS-like service w/ 700 million users) and bitcoin
 - Tangent: Facebook bought WhatsApp in February 2014... curious
- Payment processors (BitPay, Coinbase, etc.)
- Chip&Pin card (like debit card) can be used to withdraw cash at ATM's

- Address and private keys can be stored on HDD, laptop, USB stick, smart-phone, paper/card or any other physical carrier (tattoo??)
 - and even mnemonic or brain wallet – i.e. memorize a sentence or a string of random words that when hashed re-produce your public and private key

- Regular merchant transactions: in-store or on-line
 - For convenience, for anonymity and for security
 - No need to divulge credit card details, which can be intercepted and are then stored on someone's 'secure' database
 - No need for merchant to handle cash
- P2P transactions
 - Friends contributing to the next beer round
 - Tipping or donating to open-source developers, testers, helpers, the homeless
 - Sending money abroad without going through the banking system or sending cash by mail (HSBC charges me 17 GBP each time I send money to my sister in Bulgaria... Unicredit charges me 20 GBP to send money to UK. What if I want to send money outside the EU? What if I were in another country?)
- Donations to registered charities and churches
 - Alternative to paypal or cash
- Illicit transactions: in-person or on-line
 - Money laundering, drugs & weapons, tax-evasion, etc.
 - Already happening through fake or stolen identities, cash, gold, etc.
 - That's why we have the police and regulators to catch the baddies

Bitcoin address

21

The screenshot shows the bitaddress.org website in a web browser. The browser's address bar displays the URL: `https://www.bitaddress.org/bitaddress.org-v2.8.1-SHA1-a6e63f2712851710255a27fa0f22ef7833c2cd07.html`. The website features a Bitcoin logo and the text "bitaddress.org" in a large, green, cursive font. Below this, it says "Open Source JavaScript Client-Side Bitcoin Wallet Generator". There are several tabs: "Single Wallet", "Paper Wallet", "Bulk Wallet", "Brain Wallet", "Vanity Wallet", and "Wallet Details". The "Single Wallet" tab is selected. A "Generate New Address" button is visible. Below the button, there are two main sections: "Bitcoin Address" and "Private Key (Wallet Import Format)". The "Bitcoin Address" section contains a QR code, the word "SHARE" in green, and the address `1HFZ721RtuEMko4kevCTsLx1m5TDN19J7r`. The "Private Key" section contains a QR code, the word "SECRET" in red, and the private key `5JV6b6Vq9hR5bGXpF9ZtjQn6zSbV84fdYyHEREAs4e5bDFNsSTf`. A "Print" button is located in the top right corner of the content area.


English | [Español](#) | [Français](#) | [ελληνικά](#) | [italiano](#) | [Deutsch](#) | [Česky](#)

bitaddress.org
Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet | Paper Wallet | Bulk Wallet | Brain Wallet | Vanity Wallet | Wallet Details


Generate New Address | Print

Bitcoin Address

 **SHARE**

1HFZ721RtuEMko4kevCTsLx1m5TDN19J7r

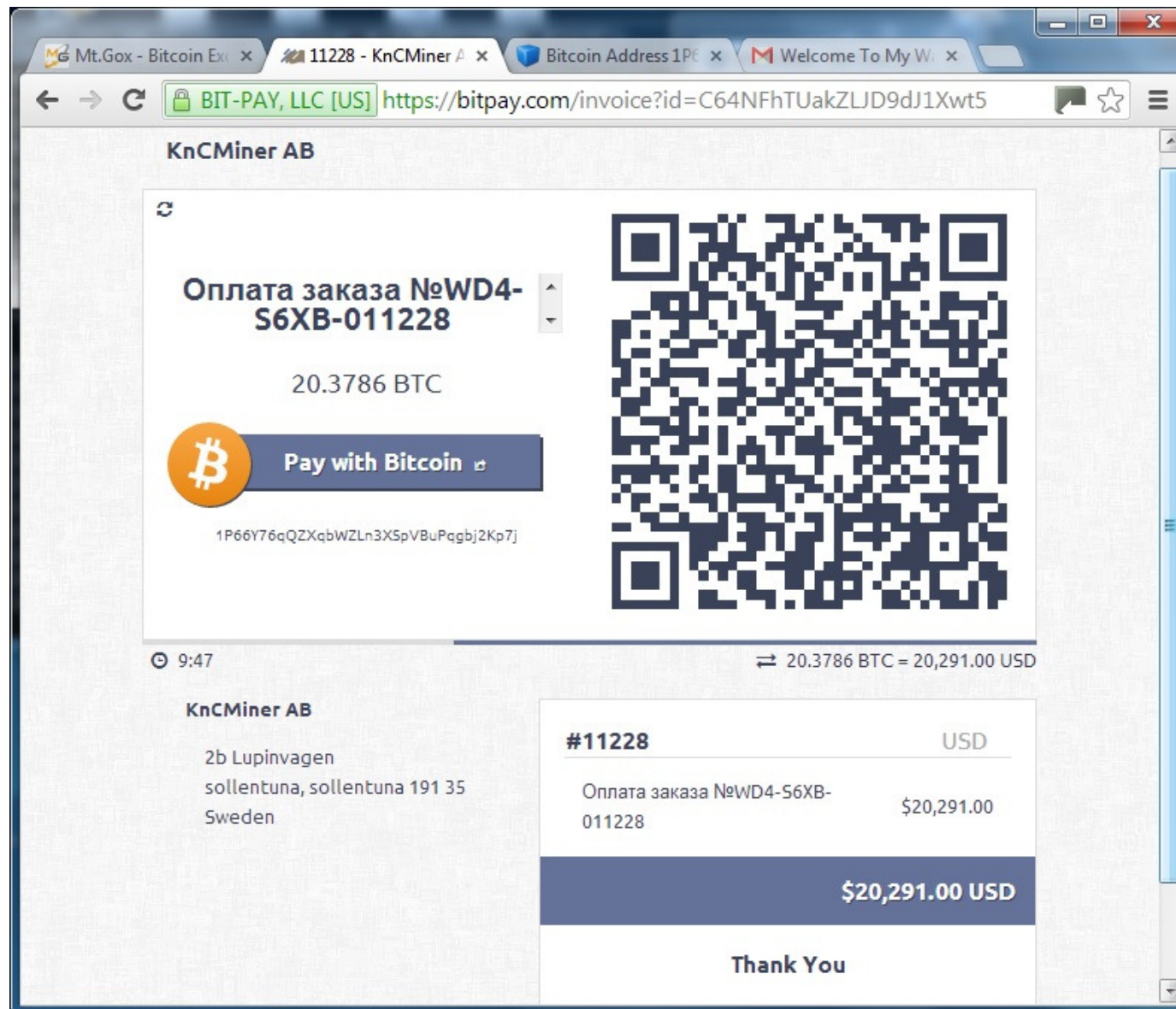
Private Key (Wallet Import Format)

 **SECRET**

5JV6b6Vq9hR5bGXpF9ZtjQn6zSbV84fdYyHEREAs4e5bDFNsSTf

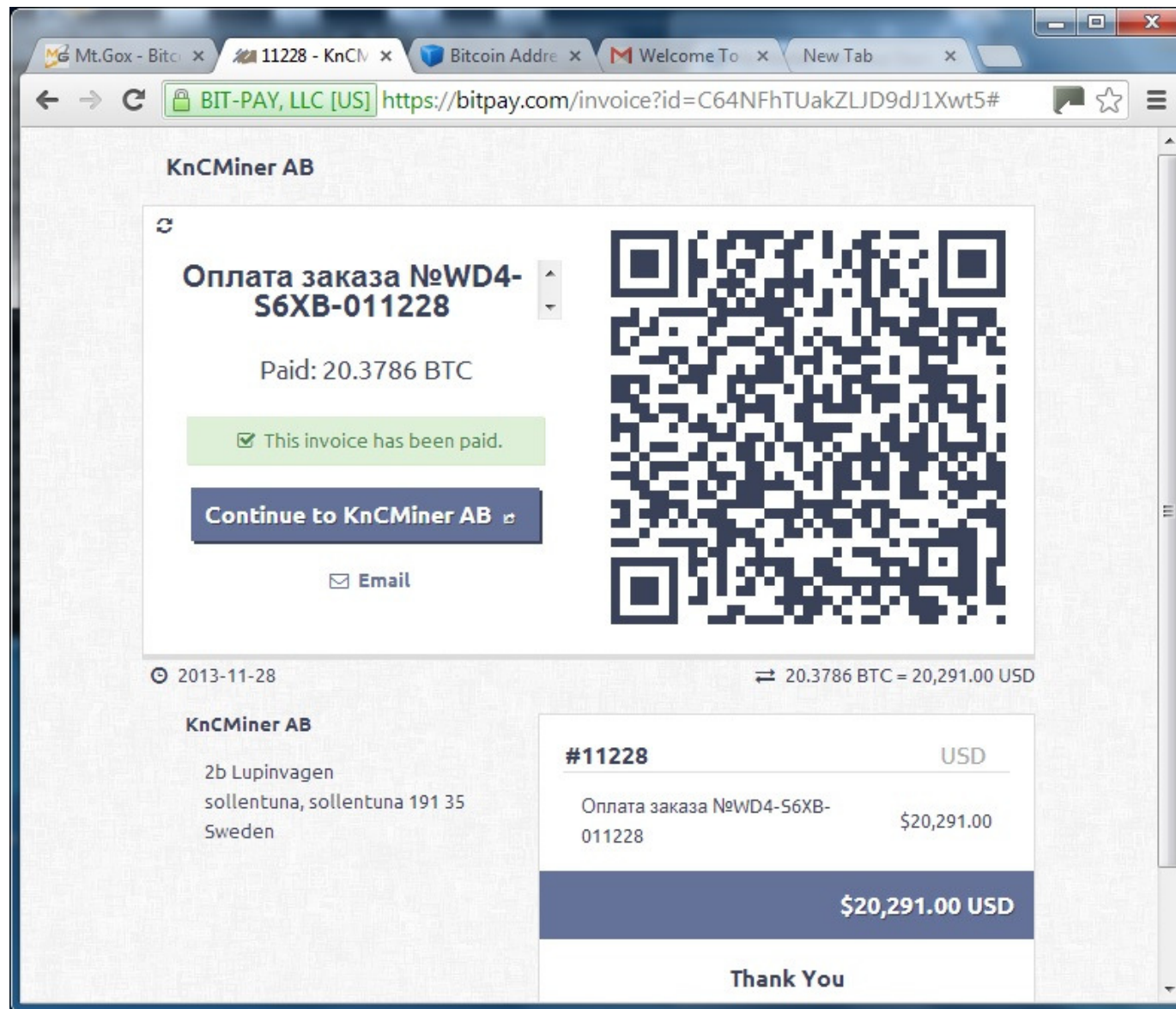
Example: Transacting online

22



Example: Transacting online

23



The blockchain is a disruptive innovation

- **Question:** What is so innovative about it?
- **Answer:** It is a distributed ledger... and we never had such a thing before
 - No central ledger (like NHS or HMRC or Central Bank or corporate)
 - Hence no need to trust that the bookkeeper or middleman to put the correct data into the ledger
 - No need to trust that the bookkeeper is not fudging the data (like discarding statistical 'outliers' or inconvenient truths)
 - No need to trust that your data might disappear from the bookkeeper's records
 - Could displace property registries, could change accounting systems (i.e. Reduce Enron like fraudulent behaviour), could help with smart property
 - At the extreme this technology can reduce and remove the need for certain kinds of expertise (e.g. middle management, notary, accounting), because said expertise is captured by the algorithm
- **Question:** What is so disruptive about this innovation?
- **Answer:** Read on to the next slide.

Blockchain services – important distinctions

25

- The blockchain is a service (and a **disruptive innovation**)
 - Distributed ledger/data-store
 - Distributed consensus
 - Solves the double-spending problem or Byzantine generals dilemma
- There are services around the blockchain
 - Bitcoin processing, bitcoin by SMS/e-mail/Twitter
 - Exchanges
 - ATM's
 - Off-chain messages (blockchain.info)
 - Outsourced bitcoin storage (hot wallets, deep-cold storage)
 - Wallets, block explorers, API's
 - Training courses (UCL, University of Nicosia)
- Services on the blockchain (**the actual disruption**)
 - Distributed Organizations (a.k.a. DAO, DAC)

Bitcoin chip and pin

26



<https://coinkite.com/>

Nikola Tchouparov, April 2014, Sofia & London



**The World's only
Bitcoin Debit Card!**



BITCOIN DEBIT CARD

Withdraw Bitcoin in CASH in your local currency at most ATMs around the world. Also works for online purchases and point-of-sale at stores.



ANONYMOUS CASH

Withdraw money safely and anonymously in cash with your Bitcoin ATM card. You can use your Bitcoin Visa to shop online anonymously and securely.

<https://bitplastic.com/>

- Transfer of unique value – Hello bitcoin!
- Multisignature – escrow or voting on the blockchain
- Blockchain advertisement (soon to be released on bitcoin)
- Financial derivatives and pass-through arrangements – blockchain derivatives
- Insurance – pay your premium to the blockchain
- Smart property – your car, fridge and oven on the blockchain
- Bank on the blockchain (improved account auditability)
- Data services
 - Data feed – sending data by blockchain
 - E-mail – crypto@blockchain.block
 - Dropbox / file-sharing – save on the blockchain
 - Law enforcement – parking ticket, building permit on the blockchain
 - Wikileaks on blockchain
- Polling – performance feedback by blockchain
- Gambling – deal me 2 cards blockchain

- **New challenges and business opportunities for privacy and law enforcement!**

Challenges

29

- Bitcoin is a proof of concept of the blockchain technology
- Pretty successful and pretty cool
- Only the very basic on-chain services can be developed and operated on the bitcoin blockchain
- Additional services possible off-chain with touch points to the blockchain, but then you lose the benefits of the blockchain
- Many shortcomings (SHA-256, elliptic curve not so elliptic... ask Nicolas for full list)
- Security and malleability weaknesses
- “Stupid coin” syndrome (dilution)

- Should I start my own blockchain (Unobtanium, Max-coin...)?

- Then someone invented Ethereum – a blockchain on which to develop and run your applications
 - Turing complete – i.e. can run any application (CLL and LLL development)
 - Seems better suited for building blockchain services
 - Scheduled to launch later this year

What does ECB say?

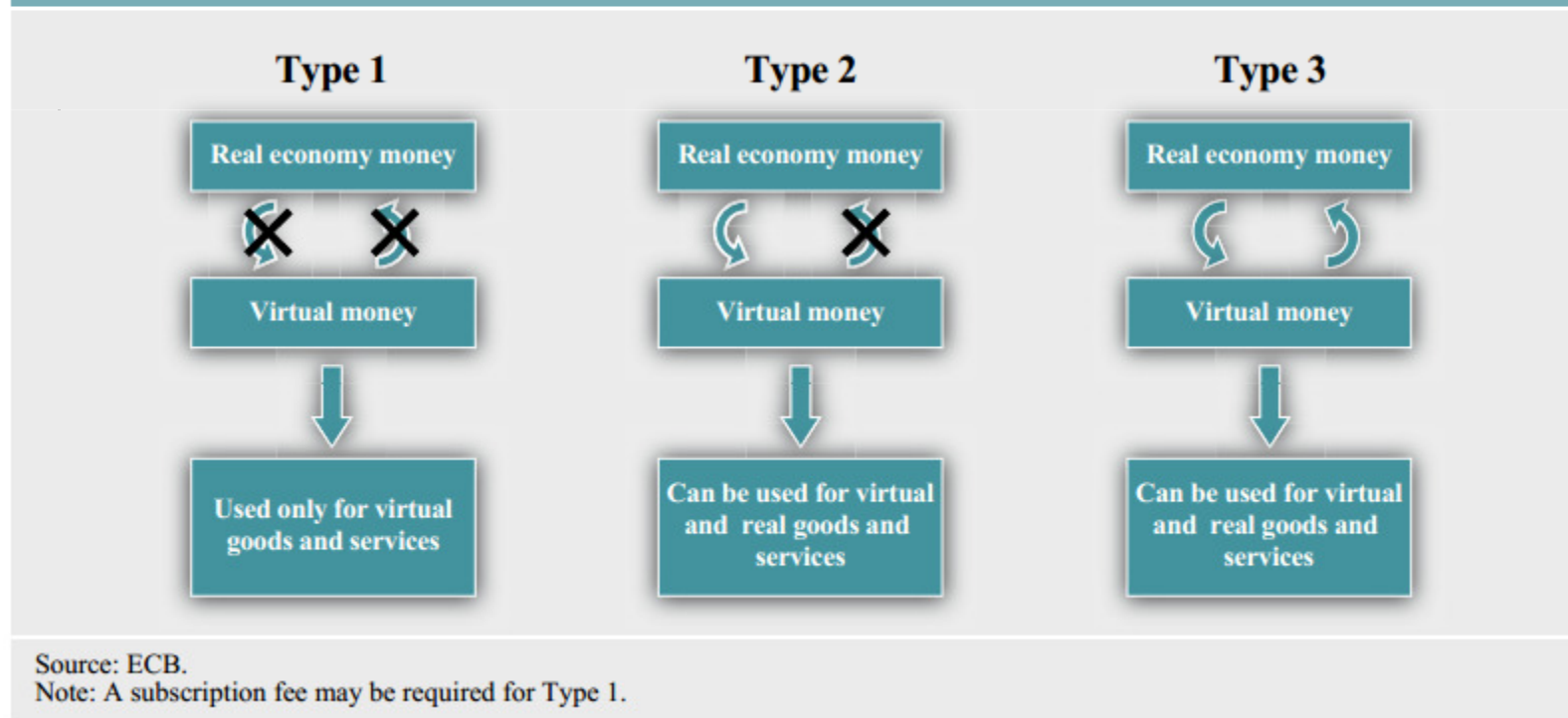
- ECB Report:
- VIRTUAL CURRENCY SYSTEMS
- OCTOBER 2012

Table 1 A money matrix

<i>Legal status</i>	<i>Unregulated</i>	– Certain types of local currencies	– Virtual currency
	<i>Regulated</i>	– Banknotes and coins	– E-money – Commercial bank money (deposits)
		<i>Physical</i>	<i>Digital</i>
<i>Money format</i>			

30

Chart 2 Types of virtual currency scheme



<http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

Under IFRS An asset is defined as:

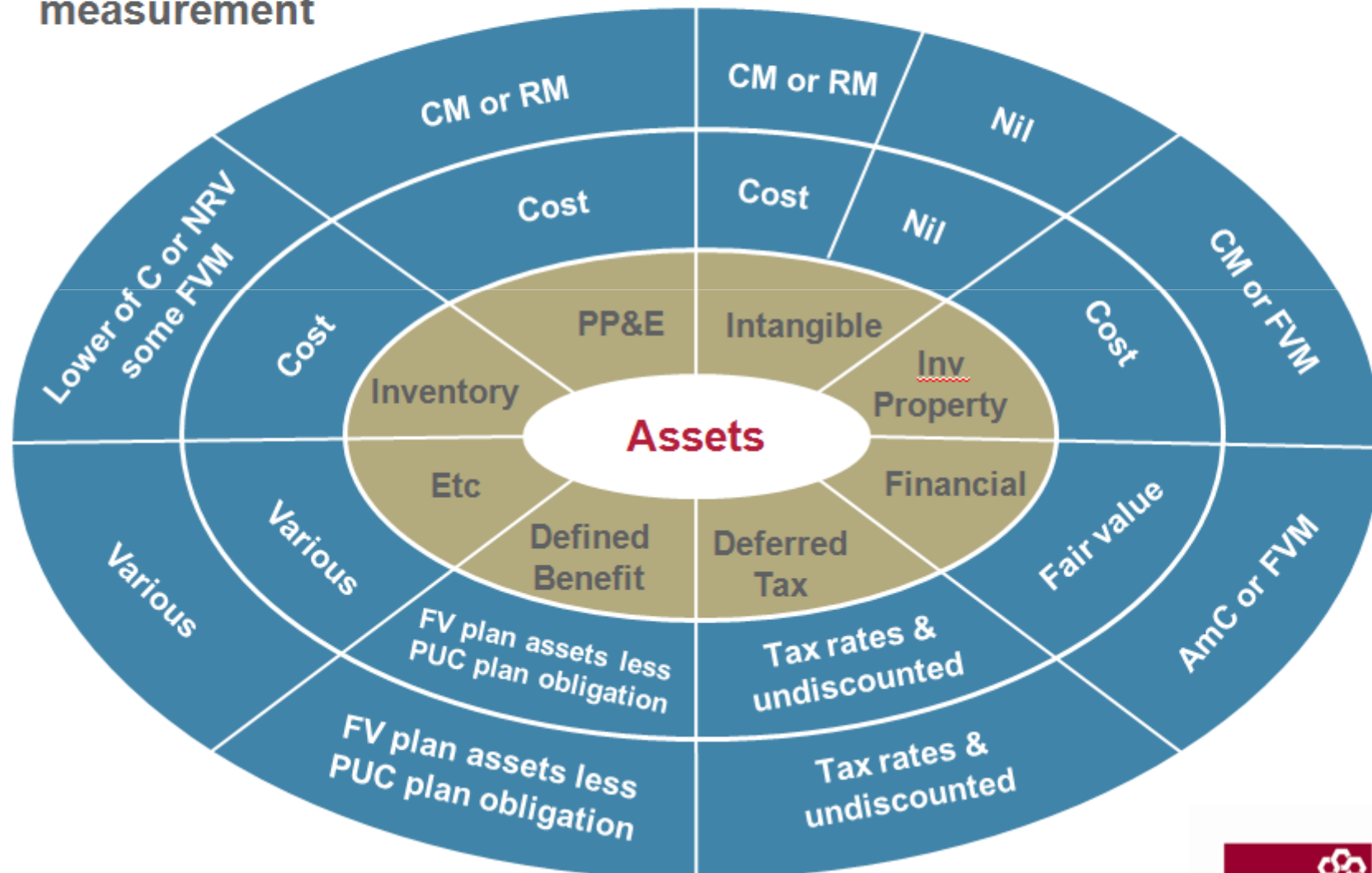
- a resource controlled by the entity
- as a result of a past event
- from which future economic benefits are expected to flow to the entity.

Source: <http://www.ifrs.org/Use-around-the-world/Education/Documents/Framework-based%20teaching%20presentations/1.%20Classification%20of%20assets.pptx>

Assets overview

10

Classification, recognition and measurement



A liability is defined as a:

- present obligation
- arising from a past event
- the settlement of which is expected to lead to an outflow of future economic benefits from the entity

Source: <http://www.ifrs.org/Use-around-the-world/Education/Documents/Framework-based%20teaching%20presentations/1.%20Classification%20of%20liabilities.pptx>

Liability

19

Classification, recognition and measurement

