Blockchain and the Real Challenges of Building IT Systems

Martin Walker
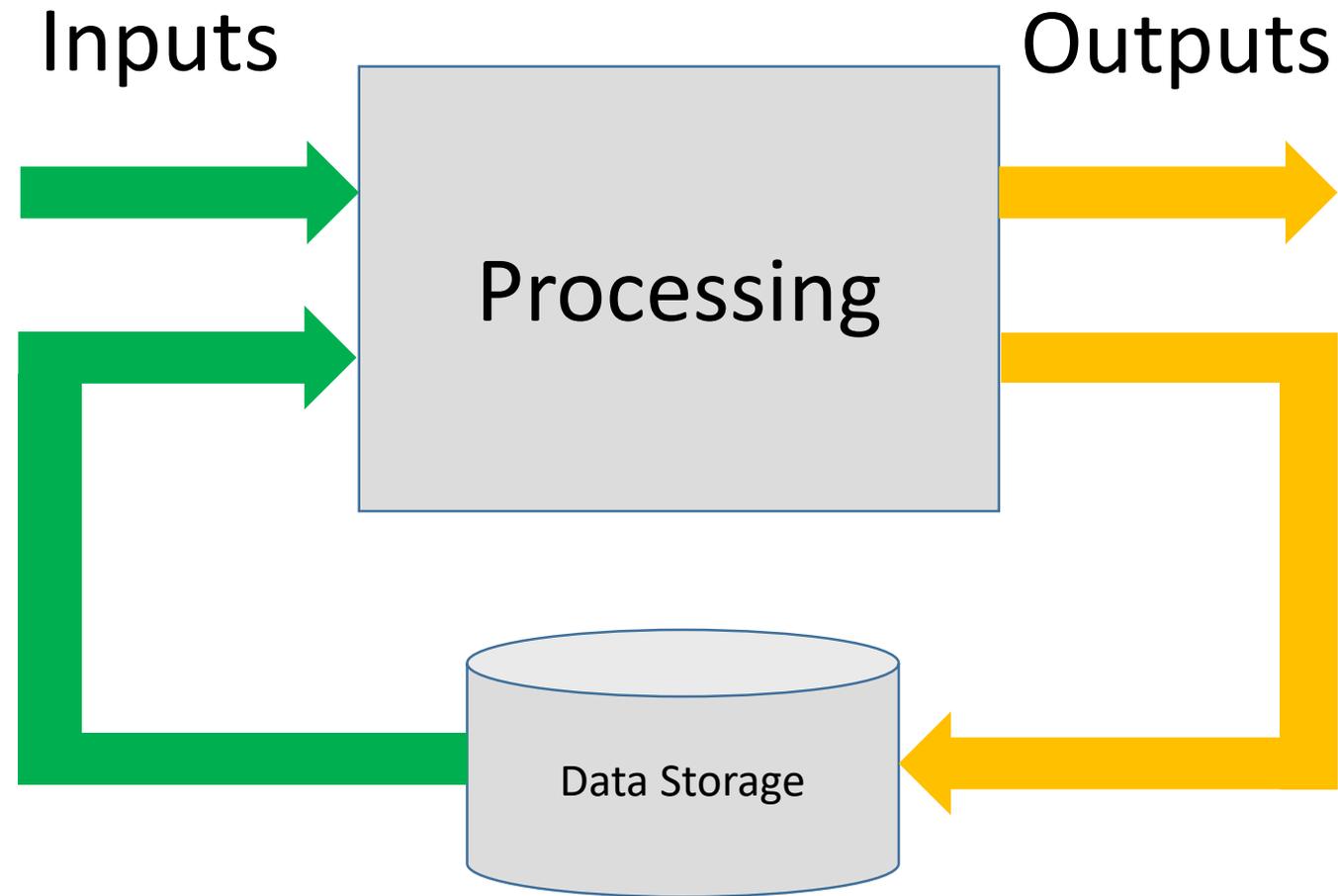
Amelia Island, Florida

May 20th 2019

IT Systems – Made Simple

Inputs

Outputs

Processing

Data Storage

www.cebma.org

Making Pancakes – Same Principles

Inputs

Processing

Outputs

Garbage In – Garbage Out

Put garbage into a system and you are likely to get garbage out. Worse case the garbage (or bad inputs) in combination with lack of programming logic can cause the whole system to crash. Where does the "garbage" come from?

- Human error

- Another system feeding in incorrect data

- Previously generated data stored incorrectly within the system

- Criminal activity

IT Systems – Bugs

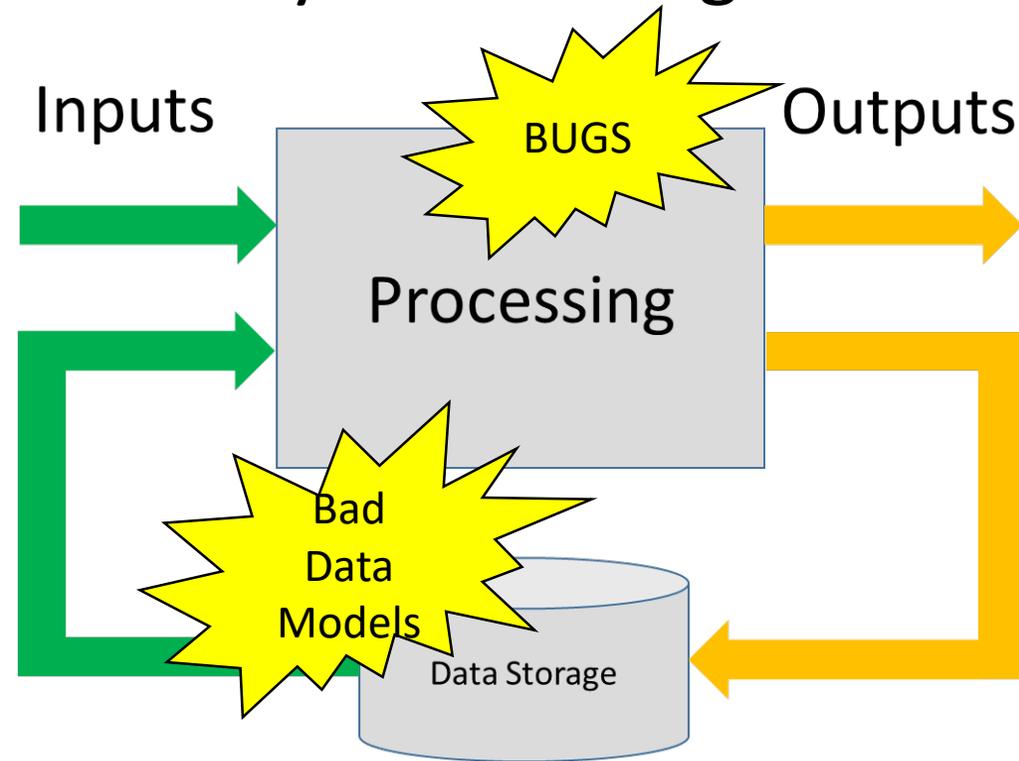- Having the wrong logic implemented in a program, more commonly known as a "bug" can be due to both implementing programming logic incorrectly, functional gaps or failing to deal appropriately with bad or missing data
- Data that is stored in a system needs a structure so the system or anyone querying the system can understand what it represents. This is not always done correctly. People often force data into systems that does not fit

Consistency Between Systems
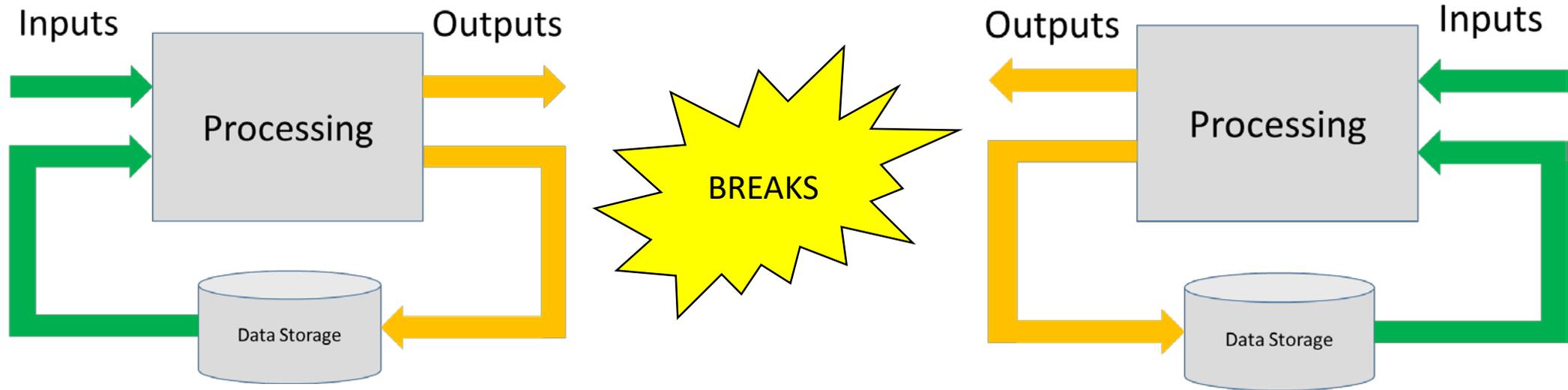
Different parties to a transaction (or even different systems belonging to the same party) can easily end up with different views of the truth. This results from some basic problems

- Inputs for one or both parties can be wrong
- One party may have a more up-to-date view of the truth
- The way data is stored about the truth may be different leading to different results
- The processing logic may be different

Accurate Representation of the Real World

ID	233301223
DataTime	05/05/2019 12:03
InputUser	Martin
Type	Floribunda
Color	Yellow
Origin	UK
Supplier	English Roses Ltd

- Input errors, programming errors or fraud can mean that the real world object is not the same as the data representation
- With complex supply chains there are multiple opportunities/incentives such as switching or forging labels or paperwork

- The record of the existence of almost all financial assets (including funds in a checking account) is digital
- But those records ultimately represent the real world, legally enforceable relationship between "Obligor" and "Obligee"
- This is not the same as infinitely duplicable digital assets such as MP3s

www.cebma.org
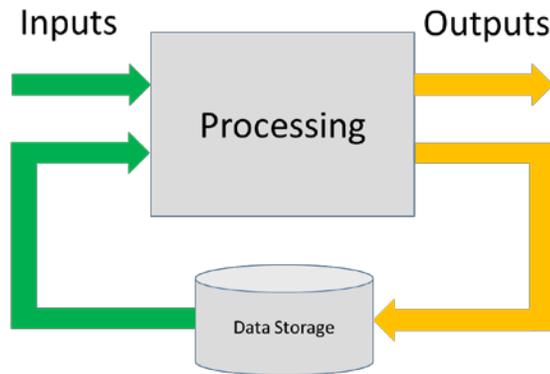
Security

Ability To Use System

Ability to change code

Access to Data

- Need to control who can use systems, who can change the code or data models and who has access to data
- Security is not just about keeping out bad actors it is about protecting people from making accidents

..and Blockchain Adds?

Problem	Real World/Logical Solution	What Blockchain adds?
Processing Logic i.e. Bugs	Train people to program, do analysis to try make sure system is doing and test, test, test.	Smart Contracts are programs, written in programming languages and frequently contain bugs. If a program is running decentralised and goes wrong no one can stop it.
Data Models	Train people to design things, we test the systems that encapsulate data models and we work to agree common standards across systems and the relevant firms	Still need to agree data models and get consistency. The enthusiasm for blockchain can be a catalyst to get people to talk about standards.
GIGO	Have controls around what goes into system, who can use the system (and make sure they are appropriately trained) build in validation of inputs	You have to use same systems and techniques to control what goes in. Blockchain alone does nothing to remove the problem the GIGO problem.
Consistency Between Systems	Agree transactions on a common system and feed other systems from golden record. Alternative attempt to use the same system and/or data models	Everybody essentially uses clones of the same system but you still get timing issues, you still need to feed into other systems. This type of model can work but it is inherently computationally inefficient. It can also be implement using traditional technologies
Accurate Representation of the Real World	Control how data is captured, audit the supply chain, use reputable suppliers.	Same techniques but do it on the blockchain
Security	Only allow appropriate people to have access to system. Keep out everyone else. Periodically validate permissions and test the security checks. Keep vendor provided systems up to date.	Make it evident if someone has tampered with data. Sometimes distribute data to wide group but encrypt it. Inherent problems come if all data is distributed to all parties. The irreversibility of transactions on a de-centralised blockchain is one of the fundamental causes of cryptocurrency thefts.

Conclusion

- Blockchain type technologies do not fundamentally change or remove the key challenges faced in building an IT system

- Blockchain based/influenced systems can be used to implement new and innovative ideas but so can existing technologies

- Anyone faced with building, buying or integrating a new system cannot simply assume they should use a blockchain based system because it is new, better or in some way magical

- People still have to think, to define the problems they face and critically evaluate the evidence about the effectiveness of their technology options